

STANDARDS RESEARCH

Assessment of AI Applications in Manufacturing and Associated Risks

March 2026

Authors

Denaige McDonnell, PhD, MBA, CRSP, CSP, EIHQ Inc.

Tom McCaffery, MBA, Two River Advisory Inc.

Rajbir Bhatti, Ph.D., chAIntrixQ

Keith McDonnell, MBA, Two River Advisory Inc.

Project Advisory Panel

Kai Lin, Rockwell Automation

Mohammed Tauhiduzzaman, NRC

Nicholas Poirier, Independent

Victoria Hailey, CMC

Olga L. Arevalo Quintero, CSA Group

Christina Hou, CSA Group (Project Manager)

Acknowledgements

The authors extend their sincere gratitude to the many interview participants and subject matter experts who generously shared their time, insight, and expertise in support of this study.

Disclaimer

This work has been produced by Two River Advisory Inc. and is owned by Canadian Standards Association. It is designed to provide general information in regard to the subject matter covered. The views expressed in this publication are those of the authors and interviewees. Two River Advisory Inc. and Canadian Standards Association are not responsible for any loss or damage which might occur as a result of your reliance or use of the content in this publication.

Table of Contents

Executive Summary 5

1 Introduction 7

1.1 Key Terms: High-level Explanations 8

2 Methods 10

2.1 Literature Review 10

2.2 Review of AI Standards and Guidelines 10

2.3 Environmental Scan of AI Adoption 10

2.4 Manufacturing Sector Interviews 10

2.5 Case Study Selection and Analysis 11

2.6 Risk Assessment Framework 11

3 Results and Discussion 12

3.1 AI in Manufacturing: Systems and Applications 12

3.1.1 AI Technology and Use in Manufacturing 12

3.1.2 AI Integration Within Evolving Manufacturing Paradigms 13

3.2 AI in Manufacturing: Functional Deployment 14

3.2.1 AI Deployment by Manufacturing Function 14

3.2.2 Typical Deployments by Function 15

3.2.3 Emerging Applications: Generative AI and LLMs 16

3.2.4 Cross-Cutting Challenges to Adoption 16

3.2.5 Agentic AI 16

3.2.6 Protocols and Interconnected Systems 17

3.3 Mapping the AI Landscape in Canadian Manufacturing 17

3.3.1 AI Adoption Patterns 17

3.3.2 Institutional and Policy Landscape 18

3.3.3 Infrastructure and Enabling Conditions 19

3.3.4 Human Capital and Ethical Barriers 20

3.3.5 Organizational Readiness and Structural Barriers 21

3.3.6 Canada's Global Position and Strategic Outlook 23

3.3.7 Summary of the Canadian AI Landscape in Manufacturing 25

3.4 Regulations, Standards, and Frameworks 25

3.4.1 Regulations 26

3.4.2 Standards 31

3.4.3 Strategic Policies and Initiatives 34

3.4.4 Lifecycle and Risk Governance Analysis 37

3.5 Interview Findings and Analysis 38
3.5.1 Use of AI Applications and Technologies in Canada 40
3.5.2 Lessons Learned 40
3.5.3 Risks and Challenges 41
3.5.4 Broader Ethical and Societal Impacts 43
3.5.5 Legislation, Standards, and Frameworks for AI Adoption 44
3.6 Case Studies of AI Adoption 45
3.6.1 Overview of Case Studies 45
3.6.2 Risks and Challenges Encountered 47
3.6.3 Lessons to Learn and Practices to Replicate 51
3.7 Risks Associated with AI Adoption 53
3.7.1 Risks Identification and Classification 53
3.7.2 Assessment of Key Risks by Category 56
3.7.3 Interconnection of Risks Across Domains 62
3.8 Discussion of Integrated Thematic Findings 63
3.8.1 Core Findings and Challenges for Manufacturers 63
3.8.2 Challenges Related to Standardization 65
3.8.3 Gaps and Opportunities for Standardization 66
3.8.4 Bridging Gaps Through Integrated Mitigation 68

4 Recommended Strategies for Strengthening Standardization 68
4.1 Mitigation Strategy Framework 68
4.2 Recommendations 69
4.2.1 Develop Implementation-Focused Guidance for Standards 69
4.2.2 Improve Data and Infrastructure Foundations 70
4.2.3 Integrate Psychosocial and Human Factors 71
4.2.4 Strengthen Lifecycle Governance with Co-Created Guidance Tools 72
4.2.5 Build Governance Maturity 72
4.3 Insight for Addressing Standards Gaps 73

5 Conclusions 73

References 75

Appendix A—Interview Protocol 86

Executive Summary

This research report presents a comprehensive assessment of artificial intelligence (AI) applications in the Canadian manufacturing sector, with a focus on identifying associated risks and developing practical strategies for safe and sustainable adoption. Grounded in evidence from peer-reviewed literature, international standards, 14 case studies, and 20 interviews with manufacturers, technologists, and policy experts, the findings reveal that AI adoption in Canadian manufacturing is both promising and precarious.

While AI is increasingly being applied to improve quality control, predictive maintenance, process optimization, and supply chain management, its adoption remains uneven. Many firms, especially small and medium-sized enterprises (SMEs), overestimate their readiness and underestimate the organizational, technical, and human requirements to make AI succeed at scale. Common barriers include weak data infrastructure, legacy industrial systems, fragmented use of standards, and limited post-deployment monitoring.

The research identified the following eight interrelated categories of risk pertaining to AI deployment in manufacturing:

- Technical
- Data
- Cybersecurity
- Operational
- Human-machine interaction
- Ethical/legal
- Organizational/strategic
- Psychosocial

Among these, psychosocial risks emerged as the most underrecognized but highly consequential. Workers described stress, trust erosion, cognitive overload, and the loss of tacit expertise when AI displaced manual judgment. The literature review and case study findings confirmed that these are foreseeable and preventable risks, yet they remain largely absent from existing standardization and policy frameworks.

The research also identified the following five systemic gaps in Canada's approach to AI adoption in manufacturing:

- Implementation readiness gap (firms mistaking pilot projects for maturity);
- Interpretability and translation gap (limited accessibility and sector-specific guidance, creating challenges in translating requirements into real-world implementation);
- Human and psychosocial gap (lack of psychosocial integration);
- Feedback and learning gap (weak learning loops between practice and policy), and
- Strategic alignment gap (fragmented, voluntary approaches vs. enforceable global regimes).

Left unaddressed, these gaps could threaten both competitiveness and worker well-being.

To address the identified risks and gaps, this report proposes a multidimensional set of mitigation strategies and recommendations. For manufacturers, recommendations include conducting robust readiness assessments, embedding risk evaluation into AI planning, forming cross-functional groups, and prioritizing workforce education in both AI literacy and emotional resilience. For standards bodies, recommendations include developing sector-specific templates, codifying usability and psychosocial protections, and establishing structured feedback loops that connect frontline practice with evolving requirements.

Preferred solutions emphasize moving from fragmented ambition to coordinated action, investing in readiness, data infrastructure, interpretability supports, and workforce well-being.

Canada could position itself as a leader in responsible AI for manufacturing, but doing so may require addressing the structural and relational barriers identified in this report. With deliberate action, the sector can work toward building AI systems that are technically reliable, socially sustainable, and globally competitive.



"The global manufacturing landscape is undergoing profound transformation, driven by disruptive technologies that are redefining how goods are designed, produced, and delivered."

1 Introduction

The global manufacturing landscape is undergoing profound transformation, driven by disruptive technologies that are redefining how goods are designed, produced, and delivered. Among these innovations, artificial intelligence (AI) is poised to play a foundational role in the next phase of industrial evolution, commonly referred to as Industry 4.0 or smart manufacturing. AI, combined with data analytics, automation, and interconnected systems, holds the potential to significantly enhance productivity, product quality, responsiveness, and resilience across manufacturing sectors [1], [2], [3].

Smart manufacturing represents the convergence of these technologies, integrating AI with machine learning, digital twin technology, and the industrial internet of things (IoT) to facilitate more intelligent, adaptive, and efficient production environments [4], [5]. This shift has implications for the entire product lifecycle, from conceptual design and prototyping to production, distribution, maintenance, and end-of-life management. Globally, jurisdictions that have embraced AI as a pillar of industrial modernization, such as Germany and China, are accelerating their competitiveness through strategic policy alignment, workforce investment, and infrastructure development [6], [7].

In Canada, AI adoption in manufacturing is often exploratory. While there are compelling examples of AI integration, particularly in the automotive, and high tech sectors [8], most firms remain in pilot or limited-use phases. Small and medium-sized enterprises (SMEs), which comprise over 98% of Canadian manufacturers [9], face disproportionately high barriers related to capital access, workforce readiness, data infrastructure, and regulatory clarity [10], [11].

To remain competitive in this rapidly evolving context, Canadian manufacturing must not only adopt AI-enabled technologies but must also do so in a way that is inclusive, coordinated, and externally-informed [12]. Achieving this requires a nuanced understanding of where Canada currently stands, the structural and operational constraints shaping adoption, and the specific governance tools, such as standards and policy frameworks, that can support secure, responsible, and scalable implementation.

This report assesses the current state of AI in Canadian manufacturing, benchmarks its trajectory against international peers, and identifies strategic opportunities for standards development. It examines AI applications across a variety of manufacturing domains, evaluates enabling and constraining factors, and explores how standardization and public policy can facilitate safer, more effective deployment. It also presents case-based evidence from across Canada and draws on international models to highlight practices that could inform future efforts. Finally, the report provides practical insights and recommendations to accelerate the responsible adoption of AI across the Canadian manufacturing sector.

1.1 Key Terms: High-level Explanations

As AI continues to evolve, the need for clear definitions and a structured approach to its applications, risks, and governance is essential. This section provides definitions of key terms, core AI technologies, and security considerations that are central to understanding AI's role in the manufacturing sector.

Advanced manufacturing technology (AMT): Integrated hardware and software systems that improve manufacturing performance through enhanced precision, flexibility, automation, and intelligence. It includes technologies such as robotics, digital twins, additive manufacturing, computer-integrated manufacturing, and AI-based control systems.

Advisory AI applications: AI tools that generate insights, forecasts, or recommendations to support human decision-making. These systems do not act autonomously but rely on human intervention to execute decisions. Often referred to as open-loop AI systems in practice.

Anomaly detection: A machine learning application that identifies deviations from expected behaviour in data patterns. In manufacturing, it is used to detect equipment faults, cybersecurity threats, or abnormal production events before they escalate into failures.

Artificial intelligence (AI): A field of computer science focused on creating systems capable of performing tasks that typically require human intelligence, such as reasoning, learning, pattern recognition, and decision-making. In manufacturing, AI is used for optimizing product design, operations, forecasting, automation, and complex problem-solving.

Closed-loop AI applications: AI systems integrated into automated control loops that monitor real-time inputs and autonomously adjust system behaviour or processes. These applications execute decisions without direct human intervention and are central to AI-based control systems in advanced manufacturing.

Computer vision: A field of AI that enables machines to interpret and analyze visual inputs (e.g., images or videos) for tasks such as identification, classification, or tracking. It is often used in quality control, surveillance, or diagnostics.

Deep learning: A subset of machine learning using neural networks with multiple layers to learn hierarchical data representations. It is commonly used in image recognition, defect classification, and complex pattern analysis.

DeepSORT (Simple online and real-time tracking with a deep association metric): A deep learning-based object tracking algorithm for tracking movement across frames.

Digital twin technology (DTT): A dynamic digital representation of a real-world system, asset, or process that enables real-time simulation, analysis, and optimization through continuous data synchronization.

Generative design: A design process in which users define parameters and constraints and an AI system automatically generates optimized design options, often using machine learning.

Edge AI: AI computing that occurs locally on devices rather than in centralized data centres, minimizing latency and dependency on cloud infrastructure. Edge AI is deployed in real-time defect detection and mobile robotics.

Evolutionary algorithms: These algorithms iteratively evolve optimal solutions to complex problems. In manufacturing, they are applied to product design, material selection, and production resource optimization.

Explainable AI (XAI): Relates to techniques that make AI models and their decisions transparent and understandable to humans, fostering trust and enabling better scrutiny of AI systems.

Federated learning: A decentralized machine learning method where models are trained across multiple local datasets without transferring data to a central server. This enhances data privacy and is valuable in multi-site manufacturing operations.

Generative AI: AI systems that create new content or data based on learned patterns. In manufacturing, generative AI supports computer-aided design, documentation drafting, and virtual prototyping.

Graph neural networks: A form of neural network architecture tailored to data structured as graphs. They are used to model relational complexity in supply chains, material flows, and process networks.

Human-in-the-loop: A system or process in which a human actively participates in the operation, supervision, or decision-making of an automated system.

Human-machine teaming: Pairing humans and AI together to streamline workflows and improve efficiency, quality, and accuracy.

Hybrid AI systems: Systems that combine rule-based logic (symbolic reasoning) with statistical learning (machine learning). These systems offer greater flexibility and are often found in predictive diagnostics and dynamic control systems.

Industrial IoT: A network of interconnected sensors, devices, and systems in industrial settings that collect, analyze, and share data to improve operational efficiency and decision-making.

Knowledge graphs: Structured networks of entities and relationships used to model manufacturing processes, component hierarchies, or product lifecycles. Knowledge graphs support traceability, maintenance, and compliance tracking.

Large language models (LLMs): Deep learning models trained on vast amounts of text data that understand and generate human language. LLMs are increasingly used to automate technical documentation, customer support, and standard operating procedures.

Machine learning: A subset of AI that enables systems to learn from data patterns and improve their performance without explicit programming.

Natural language processing: An AI domain focused on enabling machines to understand, interpret, and generate human language. Applications include chatbots, document parsing, and operator voice interfaces.

Predictive analytics: The application of statistical algorithms and machine learning techniques to forecast future outcomes based on historical data. Manufacturing uses include predicting downtime, customer and inventory needs, and energy consumption.

Reinforcement learning: An approach where AI agents learn optimal behaviours by interacting with an environment and receiving feedback. It is used in robotics, warehouse automation, and dynamic system optimization.

Robotic process automation: Software that automates routine, rule-based digital tasks such as data entry, report generation, and administrative workflows. It is common in manufacturing back-office functions.

Sentiment analysis: A text analysis technique that determines the emotional tone behind written inputs. It is increasingly used to evaluate operator feedback or detect cultural and psychological trends within organizations.

Speech recognition: Enables machines to process and act on spoken input. Used in hands-free controls, safety and security applications, and maintenance reporting.

Swarm intelligence: A decentralized AI technique modelled after collective behaviour in nature (e.g., flocks or colonies). It is applied to logistics coordination, mobile robot fleets, and resource allocation problems.

Time series forecasting: AI methods that predict values over time, such as machine wear, energy usage, or demand fluctuations. These models rely on chronological data patterns and are vital for proactive maintenance and planning.

Vision transformers: A state-of-the-art model architecture in computer vision that excels at interpreting complex visual scenes. Vision transformers are used in defect detection, product sorting, and quality assurance.

You Only Look Once, version 3 (YOLOv3): A real-time object detection model capable of identifying and classifying multiple objects within images or video streams simultaneously. Originally developed for general object recognition but has been adapted for specialized use cases.

2 Methods

This report uses a multi-method research design, which included a literature review, standards review, environmental scan of AI adoption, semi-structured manufacturing sector interviews, detailed case study analysis, and application of risk assessment frameworks. Together, these methods provide a robust foundation for understanding the current landscape of AI adoption in Canadian manufacturing and the standards-related opportunities that could support its responsible scaling.

2.1 Literature Review

The literature review used structured search strategies across academic databases, such as IEEE Xplore, SpringerLink, Elsevier, ScienceDirect, and Google Scholar, as well as industry publications and government reports. Sources were screened based on publication date (2015–2025), empirical grounding, methodological transparency, and relevance to industrial applications of AI. Excluded sources included outdated, non-empirical, or overly speculative or unverifiable content.

2.2 Review of AI Standards and Guidelines

A focused review of global and national AI-related standards and regulatory frameworks was conducted to assess their relevance to manufacturing. This review included documents from the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the Institute of Electrical and Electronics Engineers (IEEE), the Canadian Standards Association (CSA Group), and key guidance from the Pan-Canadian AI Strategy [13]. The analysis concentrated on five core governance areas:

- AI risk management
- System explainability
- Cybersecurity
- Data lifecycle integrity
- Interoperability

The review identified areas of alignment and divergence across frameworks, highlighted fragmentation in regulatory coverage, and identified specific guidance gaps, particularly those affecting SMEs or high-value industrial use cases, such as predictive maintenance, quality assurance, robotics, and AI-enabled supply chain operations.

2.3 Environmental Scan of AI Adoption

To complement the literature and standards review, an environmental scan was undertaken to assess real-world AI adoption trends in manufacturing. The scan examined AI-driven applications across predictive maintenance, process automation, quality control, supply chain optimization, and robotics. Sources included industry reports, corporate white papers, trade association publications, and government studies. These materials provided insight into workflow integration, efficiency improvements, and cost implications, while also surfacing challenges related to interoperability, data quality, and workforce readiness.

2.4 Manufacturing Sector Interviews

Primary data was collected through 20 semi-structured interviews with relevant manufacturing sector participants, who were selected via purposive and snowball sampling. Participants included manufacturers, AI developers, standards experts, policy advisors, and researchers. Interviewees were invited to share their perspectives on AI adoption enablers, barriers, risk perceptions, and standardization needs. A flexible interview guide was used to promote open-ended discussion while covering consistent thematic areas (see Appendix A). Interviews were conducted via online platforms, recorded with consent, and transcribed for analysis.

The participant pool reflects a diverse yet executive-heavy cross-section of professionals from Canada's AI in manufacturing ecosystem. Most interviewees held senior leadership roles and brought extensive manufacturing experience, although their AI expertise ranged from novice to advanced. Representation spanned SMEs and large firms, with a balance between traditional and advanced manufacturing sectors. The key demographic insights include:

Professional roles and seniority: The majority (85%) of participants held senior or executive roles, such as CEO, vice president, or director. Approximately one-third were in executive leadership, while 20% served as consultants or former executives. Only a small fraction (two participants) occupied supervisor or manager roles.

Experience: Most participants had over 15 years of experience in manufacturing. Their AI-specific experience was more varied: 35% had 4 to 7 years, 30% had 8 or more years, and 15% had fewer than 3 years of experience in AI.

AI decision-making involvement: A significant portion (70%) of participants were actively leading or co-leading AI-related decisions, and 20% contributed strategically or through advisory roles, ensuring high relevance to organizational AI governance.

Domains of expertise: Participant expertise spanned technology development (60%), business strategy (50%), research and policy (35%), security and risk (15%), manufacturing systems (10%), and supply chain optimization (20%). Many participants demonstrated interdisciplinary skills.

Organizational types and industry sectors: Participants came from manufacturing firms (45%), AI development companies (20%), standards and policy bodies (35%), and support services (20%). Sector alignment included traditional manufacturing (65%), advanced manufacturing (45%), agriculture/food industries (25%), and supply chain services (20%).

Geographic presence: Almost all participants (95%) were employed by organizations that operate in Canada, although some have international reach.

Organizational size: Participant representation spanned micro firms (30%), small businesses (50%), and large organizations (15%), indicating a balance between SME and enterprise perspectives.

AI adoption stage: Half of the participants were in early-stage exploration or pilot phases, 25% reported partial implementation, and 15% had achieved full deployment. One organization remained in a theoretical exploration phase.

AI applications and integration: Common applications included predictive analytics (100%), quality optimization (70%), robotics (50%), generative systems (35%), enterprise tools (25%), and experimental tools (20%). AI integration varied: 35% had fully embedded systems, 30% reported partial integration, and 30% used experimental tools.

As these demographics demonstrate, the interview participants reflected a dynamic mix of experience levels, organizational sizes, and sectors, highlighting Canada's evolving landscape in manufacturing and AI adoption.

2.5 Case Study Selection and Analysis

To further ground the analysis, case studies were selected and analyzed to illustrate real-world AI implementation scenarios across different manufacturing subsectors. Case inclusion was based on criteria such as technology type (e.g., advisory vs. closed-loop AI), sector diversity, stage of adoption, operational impact, and geographical representation. Cases were drawn from both Canadian and international sources. Each case was evaluated using a consistent framework that examined the technologies used, organizational objectives, risk challenges, performance outcomes, governance measures, and lessons learned.

2.6 Risk Assessment Framework

To synthesize insights across sources, a hybrid risk assessment approach was applied, guided by ISO 31000 and ISO/IEC 23894. Risks were evaluated based on core factors of severity and likelihood, categorized across technical, operational, psychosocial, and organizational domains. This framework supported comparative analysis across the research, enabling

the prioritization of key vulnerabilities and informing the development of standards-aligned mitigation strategies for AI deployment in manufacturing.

3 Results and Discussion

3.1 AI in Manufacturing: Systems and Applications

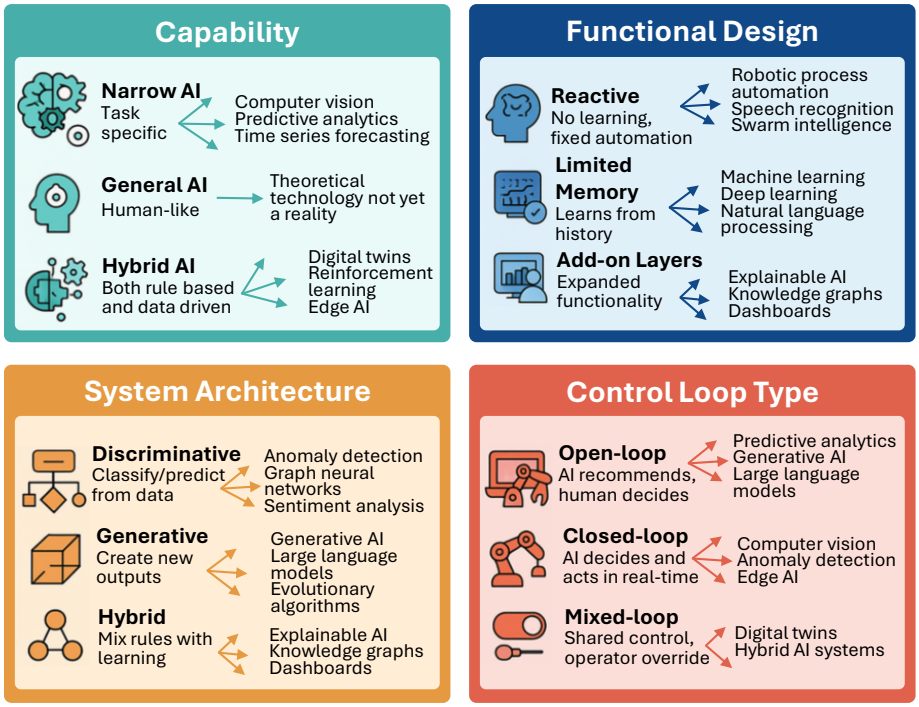
AI is playing an increasingly central role in transforming modern manufacturing, not only as a component of automation systems but as an enabler of data-driven decision-making, adaptive process control, and performance optimization. While AI is often associated with smart manufacturing initiatives, its applications span a variety of industrial environments, from legacy systems to highly digitized operations. This section outlines key technical dimensions of AI in manufacturing, including capability classifications, system architectures, and underlying technologies that support its integration into both advisory and autonomous workflows.

3.1.1 AI Technology and Use in Manufacturing

AI in manufacturing can be understood along four overlapping dimensions: capability, functional design, system architecture, and control loop type. Each dimension highlights a different way of classifying how AI operates in industrial settings, from narrow task-specific tools (e.g., visual inspection, predictive maintenance) to closed-loop systems that make and act on decisions in real-time.

Figure 1 illustrates these four dimensions with examples of core technologies. Narrow AI dominates current practice, with tools such as computer vision, predictive analytics, and anomaly detection embedded in limited-memory or open-loop systems. More advanced generative models (e.g., LLMs, evolutionary algorithms) and hybrid approaches (e.g., digital twin technology, reinforcement learning) are beginning to emerge, particularly in robotics, real-time process optimization, and adaptive production planning [14].

Figure 1: Four overlapping dimensions of AI and core technologies in manufacturing.



3.1.2 AI Integration Within Evolving Manufacturing Paradigms

As industries transition from rigid automation to adaptive, human-centric ecosystems, the integration of both open-loop and closed-loop AI systems requires careful alignment with the values, constraints, and ambitions of each manufacturing paradigm. Industry 4.0 focuses on automating and digitizing manufacturing through smart technologies such as AI, IoT, and robotics, while Industry 5.0 builds on this by re-centring people, emphasizing human-machine teaming, sustainability, and resilience.

In Industry 4.0, AI is foundational to the development of cyber-physical systems, industrial IoT, and connected factory networks [14]. Within this framework, closed-loop AI systems drive real-time monitoring and autonomous adjustments by processing sensor data and implementing feedback loops to optimize performance and reduce waste [15], [16]. AI-supported digital twins further enhance control systems by enabling simulation, defect detection, and predictive optimization prior to deployment [17], [18].

AI integration in Industry 4.0 offers tangible operational benefits, including improved process stability, minimized human error, and enhanced throughput. For example, predictive maintenance models can forecast equipment failures and reduce downtime, while quality control systems use AI to identify product defects faster and more accurately than traditional inspection methods [11], [19]. Research suggests that open-loop AI systems can improve decision accuracy by up to 25%, while reducing response times [11]. These benefits are particularly valuable in high-precision industries such as additive manufacturing and semiconductor production [11].

However, the effective deployment of AI systems in Industry 4.0 is often constrained by data quality, infrastructure demands, and cybersecurity vulnerabilities. In closed-loop environments, the need for real-time data integrity makes systems more susceptible to attacks and errors if protective protocols are lacking [20], [21], [22]. Trust also remains a critical issue. If AI-generated outputs are not transparent or interpretable (e.g., black box models), operators may resist implementation, limiting the technology's impact [20]. For example, if an AI system tells a factory worker to shut down a machine because it predicts a potential failure, but the worker does not understand how the AI made that prediction, and the system does not explain its reasoning, the worker might not trust the AI system and might choose to ignore the advice. This lack of transparency can reduce the effectiveness of AI technology.

The transition to Industry 5.0 shifts the integration narrative from efficiency to collaboration, customization, and sustainability [23]. While still reliant on automation, this paradigm repositions AI as a tool for augmenting human skill, enhancing workplace safety, and advancing social and environmental responsibility.

Industry 5.0 also provides space for open-loop AI systems to support decision-making without displacing human agency. These tools generate insights on energy usage, material efficiency, and risk exposure that enhance strategic control while preserving ethical oversight. For example, AI-powered sustainability models classify recyclable materials and reduce waste, while carbon footprint monitoring tools adjust energy usage to align with environmental targets [11], [24].

However, integration of Industry 5.0 demands reskilling and cross-disciplinary competence, particularly in SMEs that lack robust internal AI capacity. Balancing operational efficiency with customization is another friction point, as real-time responsiveness and personalization can strain legacy systems. Moreover, ethical governance becomes increasingly important as AI systems participate in decisions with social, safety, or labour implications [24].

Ultimately, successful AI integration is contingent not only on technical feasibility but also on contextual fit. Open-loop systems are powerful tools in strategic decision-making, while closed-loop systems excel in environments demanding speed and precision. But neither can function in isolation from the human, cultural, and regulatory contexts in which they are deployed. As the industry navigates between the automation-first approach of Industry 4.0 and the human-aligned priorities of Industry 5.0, AI systems must evolve not only in sophistication—but also in purpose, transparency, and trustworthiness.

3.2 AI in Manufacturing: Functional Deployment

This section explores how AI is actively used across the manufacturing value chain. Rather than a siloed innovation, AI is increasingly embedded into domain-specific systems, driving improvements in speed, accuracy, and adaptability. From generative design tools to closed-loop production control, AI technologies support both upstream innovation and downstream execution.

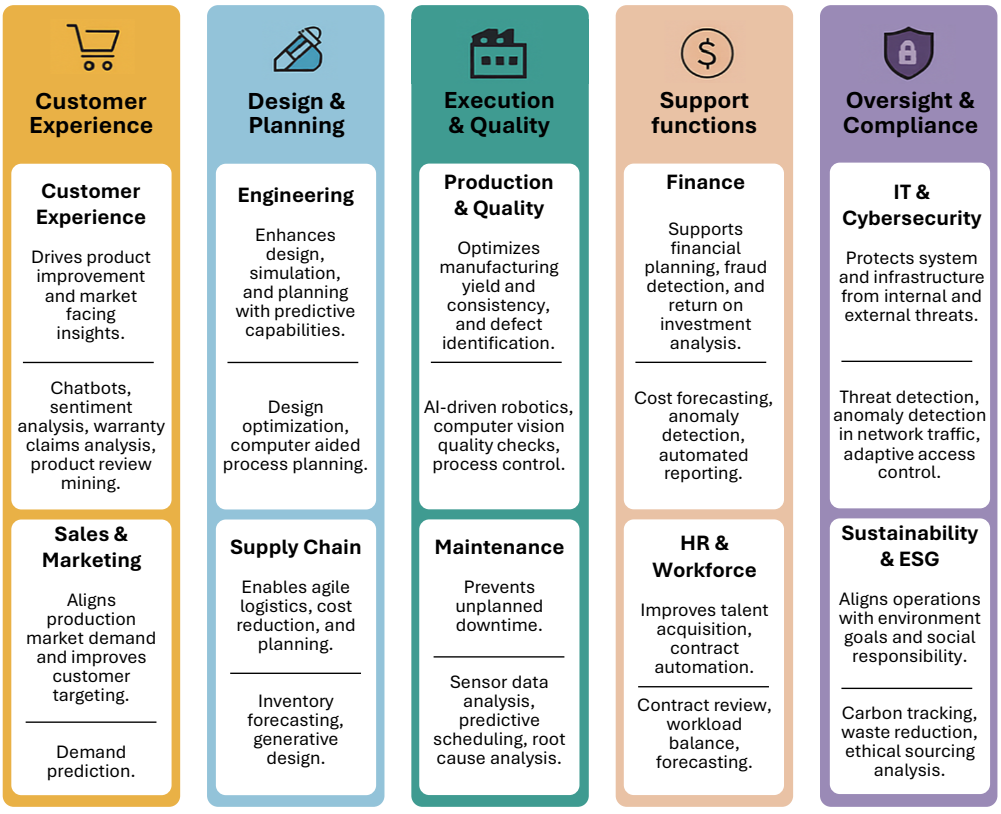
This section categorizes AI applications by domain, emphasizing how core technologies (e.g., machine learning, computer vision, LLMs) are adapted to solve real operational problems. It also highlights emerging trends, capability gaps, and barriers to adoption that shape the readiness and scalability of AI in industrial contexts.

3.2.1 AI Deployment by Manufacturing Function

AI is increasingly embedded across manufacturing domains, supporting everything from product design to customer experience. These domains are not isolated silos, instead they reflect areas where AI enhances decision-making, automates routine tasks, or enables predictive foresight.

Figure 2 illustrates this functional deployment, grouping domains into primary operations (e.g., production, engineering), support functions (e.g., human resources [HR], finance), and strategic overlays (e.g., environmental, social, and governance [ESG] training). Common use cases include predictive maintenance, design optimization, anomaly detection, dynamic pricing, and knowledge capture. While many tools span multiple functions, deployment tends to cluster around tasks with structured data and measurable performance.

Figure 2: Functional deployment of AI in manufacturing.



3.2.2 Typical Deployments by Function

AI deployment in manufacturing follows distinct patterns based on domain-specific priorities, data types, and operational goals. While applications vary by sector and scale, the areas discussed in this section have demonstrated strong early-stage traction or measurable return on investment. Sections 3.2.2.1 through 3.2.2.3 provide a functional overview of how AI is applied across key stages of the manufacturing value chain.

3.2.2.1 Engineering and Maintenance Applications

AI's earliest and most mature manufacturing deployments are in engineering and asset management. These domains benefit from consistent data streams and measurable performance metrics, making them ideal for early-stage adoption. Common applications include:

- **AI-driven process planning:** Feature-based design tools and expert systems use computer-aided process planning to enhance efficiency and reduce human error [25].
- **Evolutionary AI:** Techniques such as genetic algorithms are used in structural optimization and stress analysis to simulate millions of configurations rapidly [26].
- **Predictive maintenance:** Machine learning models and sensor data forecast wear and prevent equipment failures in assets such as turbines and semiconductors [17], [27]. Studies show predictive maintenance can reduce unplanned downtime and increase asset availability [4].
- **Digital twin integration:** Real-time digital replicas enable simulation of manufacturing assets, improving diagnostics and dynamic adjustments [17].
- **Industrial IoT-enabled data infrastructure:** The connection of data-producing devices (e.g., sensors, radio frequency identification tags) enable continuous data capture of factors such as temperature, vibration, load, and energy usage, which fuels AI models for both predictive maintenance and dynamic simulation updates [17], [27].

These tools form a feedback-rich environment where AI adds both tactical efficiency and strategic foresight. Yet many firms remain at early maturity stages due to challenges related to infrastructure, data quality, talent, and regulatory complexity [28].

3.2.2.2 Production, Automation and Quality Control

In the areas of production, automation and quality control, AI powers intelligent manufacturing systems capable of real-time decision-making. Applications include:

- **Closed-loop AI control:** Uses feedback loops to optimize process parameters in real-time [4].
- **AI-augmented robotics:** Enables flexible assembly and defect reduction [29].
- **Computer vision and deep learning:** Detect micro-defects in high-precision parts [11], [30].
- **Edge AI:** Allows rapid, on-device defect detection to reduce latency [31].
- **Explainable AI:** Improves operator trust in AI-driven quality assessments [32].

While these tools improve first-pass yield and reduce material waste, their implementation must balance automation with interpretability to avoid over-reliance and cognitive offloading.

3.2.2.3 Supply Chain and Logistics Optimization

In the area of supply chain and logistics, AI enhances responsiveness, cost-efficiency, and resilience across supply networks. Applications include:

- **Machine learning-driven forecasting:** Aligns inventory with demand [33].
- **Autonomous warehousing:** Uses robotics for real-time coordination.
- **Disruption prediction:** Models supplier risk and flag delays.

In addition, AI-enhanced supply chains can lower costs and improve forecast accuracy [33], [34]. However, increased efficiency can introduce risk through centralization, over-optimization, and cascading failures, which is discussed in the risk analysis presented in Section 3.7.



3.2.3 Emerging Applications: Generative AI and LLMs

Although most industrial applications still focus on traditional AI, the use of generative AI and LLMs is growing. Generative AI supports design iterations in computer automated design systems, process simulations in digital twin technology environments, and novel material formulations or layout testing. While LLMs are used to support natural language querying of maintenance logs or supplier records, chatbots for workforce troubleshooting, and documentation automation. These tools raise concerns around intellectual property, data privacy, and explainability, which are discussed in the risk analysis in Section 3.7.

3.2.4 Cross-Cutting Challenges to Adoption

Despite momentum, AI implementation in manufacturing faces significant hurdles, including:

- **Technical barriers:** Integration with legacy systems and lack of data standardization [2], [7], [14].
- **Human capital:** Shortage of skilled AI practitioners, limited digital literacy, and reskilling needs [4], [14], [35].
- **Strategic:** High cost of experimentation versus a fear of being left behind [11], [36].
- **Security and ethics:** Risks of cyberattacks, unexplainable AI behaviour, and decision accountability [11], [35].
- **Cost and scalability:** High upfront investments and difficulty generalizing AI models across different contexts [4], [14].

For SMEs in particular, adoption depends on scalable modular systems, vendor transparency, and access to trusted AI literacy tools.

3.2.5 Agentic AI

A growing category of agentic AI systems is emerging—applications capable of autonomous, goal-directed actions within defined operational boundaries. Unlike traditional assistive tools that rely on human prompts or oversight, agentic systems can make limited decisions and adapt behaviours in pursuit of performance objectives. In manufacturing, this includes adaptive scheduling agents, self-optimizing process controllers, and predictive maintenance systems that adjust operational parameters in real-time. While these systems improve responsiveness and efficiency, they also introduce governance issues, including how to ensure human-in-the-loop control, trace decision pathways, and assign accountability when AI acts semi-independently.

3.2.6 Protocols and Interconnected Systems

AI deployment in manufacturing is also shifting toward interconnected, multi-agent environments. Emerging frameworks, such as the model context protocol, enable AI systems, tools, and platforms to exchange context dynamically and coordinate decisions across design, production, logistics, and supplier networks. While these integrations hold promise for improving efficiency and visibility across the value chain, they can also expand uncertainty by introducing unknown issues where system interactions or data exchanges create unintended consequences. Furthermore, unwanted bias may also be embedded early in system or model design, then amplified as interconnected systems reinforce each other's assumptions. Governance and assurance frameworks must therefore evolve to evaluate not only individual AI performance but also system-of-systems interactions.

3.3 Mapping the AI Landscape in Canadian Manufacturing

AI adoption in manufacturing is shaped by differences in technological readiness, regulatory environments, and workforce capabilities. While some nations have advanced large-scale AI deployment through technologies such as digital twins, autonomous robotics, and real-time optimization, Canada demonstrates pockets of excellence amid systemic constraints. This section maps the Canadian AI manufacturing landscape across six thematic domains: (a) adoption patterns, (b) institutional and policy landscape, (c) enabling infrastructure, (d) human capital readiness, (e) structural and ethical barriers, and (f) global positioning. Together, these themes provide a comprehensive overview of where Canadian industry stands and what is required to remain competitive in an AI-driven global market.

3.3.1 AI Adoption Patterns

AI uptake in Canadian manufacturing remains modest but shows promising developments in specific sectors and use cases. As of 2023, only 4.6% of Canadian manufacturers reported using AI [37]. Adoption is concentrated in large firms with digital maturity and capital-intensive operations [38], [39], while SMEs lag behind due to cost, expertise, and infrastructure constraints.

Success stories illustrate AI's potential to decrease costs through AI-driven predictive maintenance. For example, Magna International reduced unplanned downtime by 35%, Bombardier saved $2.3M, and Harbour Air reduced parts replacement costs by 25% [40]. These gains reflect core deployment areas in predictive maintenance, computer vision for quality control, and intelligent supply chains [41].

Predictive maintenance is one of the most impactful applications of AI in Canadian manufacturing. Automotive suppliers, aerospace firms, and steel producers have deployed AI-powered sensor networks to monitor equipment in real-time, reporting reductions of up to 40% in unplanned downtime and significant maintenance cost savings [40].

AI is also driving efficiencies in supply chain management. Companies such as Atlas Manufacturing and Magna International are using AI for demand forecasting and vendor performance analysis, resulting in up to 30% improvements in inventory accuracy and supply chain resilience [40]. AI-based visual inspection systems are transforming quality assurance by detecting defects with higher accuracy and consistency than human inspectors. At AutoParts Canada, defect rates dropped from 2.3% to 0.4% after implementing machine vision systems, while Thomson Precision Manufacturing reported a 42% improvement in product consistency [40]. These tools enable Canadian manufacturers to improve quality, reduce waste, and enhance customer satisfaction [41]. These tools help manufacturers respond more effectively to volatile markets, a trend mirrored in global research showing increased agility and responsiveness as key AI benefits [1].

AI also has the potential to enhance workplace safety and augment human performance, particularly in high-risk or complex environments [36]. Maxwell Manufacturing in Toronto reported a 45% reduction in workplace incidents after implementing AI-enabled safety monitoring systems [40]. Wearables and computer vision tools are increasingly used to support task automation and proactive risk detection, aligning with international trends in human-machine collaboration that prioritize safer, more inclusive workplaces [22]. While early benefits

are promising, the long-term implications of AI for occupational health and safety (OH&S) remain under-researched and warrant further study.

In addition to predictive maintenance and intelligent supply chains, other emerging applications include digital twins for production efficiency, AI-powered decision systems for real-time planning, and computer vision for quality and waste reduction [40], [41], [42]. Early-stage use in mining, oil, and gas focuses on improving safety through remote operations [43]. Knowledge retention is also gaining attention amid workforce turnover [41].

Environmental performance is another emerging AI application domain in Canadian manufacturing. AI-powered energy management systems at Thomson Industries and Ecosystems Group reduced their energy consumption by 29% and 40%, respectively, through real-time monitoring and intelligent control of production processes [40]. While still in early adoption stages, these applications align with broader decarbonization goals [39].

3.3.1.1 Regional AI Adoption Patterns

Historically, southwestern Ontario has lead AI deployment due to its dense manufacturing base, strong integration with the United States (US), and active innovation corridor from Windsor to Waterloo. The region hosts a concentration of automotive original equipment manufacturers, aerospace firms, and applied research institutions that support AI experimentation at scale [43].

Quebec follows, driven by Montreal's global AI ecosystem and strong aerospace and automotive sectors. Collaborations between academia and industry have produced tangible results. For example, Montreal-based AutoParts Canada reported a drop in defect rates from 2.3% to 0.4% after implementing AI-based visual inspection systems [40].

Alberta's efforts remain narrowly focused on resource extraction industries, with AI mainly deployed for remote safety monitoring and energy-sector automation [43]. The province currently hosts only one Advanced Manufacturing Cluster facility [43].

In the territories (the Yukon, Northwest Territories, and Nunavut), manufacturing-scale AI adoption remains minimal, but there are early instances of AI use in resource and exploration contexts. For example, an initiative in the Northwest Territories is using AI-driven core scanning and historical geological data to identify new areas that may contain critical minerals [44]. The Regional Artificial Intelligence Initiative has also allocated funding to support AI-related projects pertaining to natural resources, logistics, and infrastructure [45]. These efforts could lay groundwork for more manufacturing or industrial AI in the North, contingent on improvements in connectivity, localized technical capacity, and supportive policy.

3.3.2 Institutional and Policy Landscape

Unlike Germany, Japan, or the United Kingdom (UK), Canada lacks a cohesive national strategy to harmonize industrial AI adoption across federal, provincial, and municipal levels. What remains is a fragmented ecosystem of AI-related initiatives by various groups, organizations, and agencies, including:

- **Innovation, Science and Economic Development Canada:** Oversees the Advanced Manufacturing Cluster (led by NGen) [46], the Scale AI Cluster [47], and other Global Innovation Clusters [48].
- **Treasury Board of Canada Secretariat:** Manages AI policy instruments such as the Directive on Automated Decision-Making [49].
- **Canadian Institute for Advanced Research:** Leads the Pan-Canadian AI Strategy [13].
- **National Research Council of Canada:** Supports Canadian policy by providing evidence-based solutions, scientific knowledge, and technological insights to inform government decision-making in priority areas.

Additional contributors include Public Services and Procurement Canada, Global Affairs Canada, Justice Canada, Statistics Canada, Transport Canada, and National Defence, among others.

Investments under the Pan-Canadian AI Strategy and the Global Innovation Clusters are expected to generate $16.5 billion toward Canada's GDP and 16,000

jobs by 2030 [42]. Programs such as Scale AI and the Advanced Manufacturing Cluster have supported applications ranging from machine learning and additive manufacturing to autonomous robotics and digital twin technologies [46], [47], [42]. However, these initiatives often lack cross-jurisdictional coordination. Moreover, at this time, 72% of funding is going to industry, 16% to non-profits and charities, and 13% to academia, which raises concerns about reinforcing industrial hierarchies and limiting community-based innovation [42], [43].

3.3.3 Infrastructure and Enabling Conditions

The successful deployment of AI in manufacturing depends heavily on access to robust digital infrastructure, including computer resources, cloud services, secure data environments, and digital connectivity that enables AI development, testing, deployment, and scaling [42]. Canada has implemented several federal programs to support this process, including the Strategic Response Fund (formerly the Strategic Innovation Fund) [50], the Scale AI Cluster [47], the Industrial Research Assistance Program [51], and the Canada Digital Adoption Program [52]. These initiatives provide funding, training, and partnership opportunities that serve as key enabling mechanisms for AI deployment [36]. However, access to these supports remains uneven. Compared to global peers with coordinated national AI strategies, Canada's approach imposes limitations, particularly for SMEs.

Many Canadian manufacturers lack the foundational technologies needed for intelligent automation, such as sensor networks, edge computing, and interoperable data pipelines. Legacy IT systems remain widespread and often hinder communication between enterprise resource planning, manufacturing execution systems, and machine-level controls, creating friction in the integration of AI technologies [2].

Deployment frequently depends on foreign-owned cloud platforms such as Amazon Web Services and Google Cloud, raising concerns about vendor lock-in, data sovereignty, and limited domestic capacity to scale or innovate [43]. This external dependence compromises national control over intellectual



property, operational data, and cybersecurity resilience, particularly in safety-critical sectors.

While innovation corridors in regions such as Ontario and Quebec provide access to high-performance computing resources, applied research facilities, and industrial testbeds, manufacturers in less industrialized provinces face persistent infrastructure gaps. These include unreliable high-speed internet, limited access to regional data centres, and the absence of locally tailored technical support. Without equal access to enabling conditions, SMEs outside major hubs struggle to participate in AI-driven transformation.

Several national programs have attempted to extend AI capabilities to manufacturers across the country. For example, projects under the Advanced Manufacturing and Scale AI clusters often use cloud-based platforms to deliver supply chain visibility, real-time analytics, and collaborative R&D [46], [47]. However, the distribution of these tools has not been even. This imbalance reflects a broader structural challenge, which is the lack of a cohesive national strategy to develop and distribute AI infrastructure equitably.

3.3.4 Human Capital and Ethical Barriers

AI adoption in manufacturing is constrained not only by technical or financial factors, but also by persistent challenges in human capital and ethics. Shortages of skilled talent, a lack of workforce readiness, psychosocial strain, and ethical uncertainty are consistently identified as barriers to Industry 4.0 deployment, particularly among SMEs [6], [7], [12]. These issues are deeply interdependent. For example, a lack of technical expertise compounds employee resistance, while ethical ambiguity erodes trust in both systems and organizations [1], [11], [20].

For manufacturers, the importance of these challenges depends on their relationship to standards. Frameworks such as ISO/IEC 23894, *Information technology — Artificial intelligence — Guidance on risk management* [53], and ISO/IEC 42001, *Information technology — Artificial intelligence — Management systems* [54], assume a baseline of technical expertise, psychosocial safety, and ethical competence. Without these human and organizational foundations, standards remain aspirational documents rather than operational safeguards. Moreover, the growing integration of AI into workplace decision-making (e.g., processes such as hiring, task assignment, and scheduling) means that psychological health (i.e., workers' mental well-being and sense of safety), autonomy (i.e., the ability to exercise control and agency in one's work), and fairness (i.e., the perception of equitable and unbiased treatment) are no longer peripheral issues but central determinants of adoption outcomes [23], influencing whether AI is accepted and used effectively.

This section examines three interrelated barriers that could directly affect the extent to which manufacturers can translate standards into practice: (a) workforce skill shortages, (b) emotional and psychosocial readiness, and (c) ethical friction and mistrust.

3.3.4.1 Workforce Skill Shortages

Adopting and sustaining AI requires highly specialized human capital [41], yet Canada faces shortages in machine learning, data engineering, and automation systems expertise. While national talent strategies exist, they remain insufficiently scaled to meet current industrial demand. The gap is especially pronounced in SMEs, which often lack internal technical staff and must outsource at high cost [55], [56].

Interviewees reinforced these challenges by pointing to both a shortage of workers and a mismatch of skills. One expert explained that the occupational makeup of manufacturing has shifted, noting that traditional manual labour roles are declining while technical and specialized roles are increasing. As a result, companies are paying higher wages for scarce technical talent but not seeing equivalent gains in productivity because systems and processes have not been upgraded at the same pace.

Others noted that many organizations are still in the early stages of developing true AI competence, meaning that they are increasingly familiar with the language of AI, but their understanding remains surface-level. As a result, some organizations rely on widely used terminology or vendor narratives because they have not developed knowledge of the underlying mathematical models, assumptions, or implications needed to critically assess these systems. While initiatives such as the Pan-Canadian AI Strategy [13] and sector-specific micro-credentials offer a place to start developing such knowledge, most fall short of addressing the hands-on, interdisciplinary nature of AI deployment in manufacturing. Manufacturers require talent that can bridge operations, IT, and compliance [12], [56]. Without these integrated capabilities, projects can stall or fail to scale. As interviewees confirmed, the shortage is not simply a matter of coding skills; it is a systemic readiness gap spanning cognitive problem-solving, communication, and collaboration skills that underpin effective human-AI interaction.

3.3.4.2 Emotional and Psychosocial Readiness

Beyond a need for technical competence, AI introduces psychosocial complexities that shape worker engagement and adoption outcomes. The Government of Canada defines the psychosocial work environment as the interplay of psychological and social factors, such as workload, expectations, deadlines, relationships, and workplace culture, which influence how people experience their jobs and, ultimately, their health and retention [57]. When AI alters how tasks are assigned, monitored, or valued, it inevitably reshapes this psychosocial work environment.

For many employees, working with AI means navigating existential questions about job identity, autonomy, and personal values [36], [56]. These concerns are compounded in manufacturing environments where change is fast-moving, culturally top-down, and often framed in purely economic terms—a sentiment shared by several interviewees. Psychosocial health is a relatively new concern for employers, and organizational systems have not yet caught up with the scale of mental health challenges accelerated by technological disruption [56]. Evidence also shows that psychosocial risk is not only an individual issue but also a systemic one. When workplaces fail to integrate psychological health into organizational governance, risks such as technostress, job insecurity, and erosion of trust spread across teams and reduce overall resilience [58], [59].

Psychosocial stress can manifest as resistance to new systems, disengagement, or even system sabotage. These issues arise not from a lack of awareness, but from legitimate worker concerns about privacy, agency, and future employment [56]. These challenges cannot be addressed through training alone. They require emotionally intelligent leadership, participatory change management, and transparent communication about the intent and limits of AI systems.

The costs of inaction are significant. In 2024, mental health-related absences were estimated to cost Canadian employers $51 billion annually [60], and psychosocial hazards are formally recognized under CAN/CSA-Z1003/BNQ 9700-803, *Psychological health and safety in the workplace* [61]. This emerging evidence underscores the importance of addressing psychosocial risks during AI adoption. Integrating psychosocial readiness into implementation strategies is essential to mitigate potential stress, burnout, and disengagement, while fostering trust, inclusion, and workforce stability, which are key factors for successful digital transformation.

3.3.4.3 Ethical Friction and Mistrust

Ethical concerns related to fairness, bias, explainability, and accountability complicate AI deployment in manufacturing. Employees are increasingly subject to algorithmic tools, such as automated scheduling, productivity tracking, and workplace surveillance, without adequate explanation or meaningful channels for appeal [11], [56]. These practices create power imbalances that erode trust not only in the technology but also in organizational decision-making [36].

The risks are amplified by the absence of inclusive design practices. When datasets fail to represent all groups, underrepresented workers may face disproportionate harms, such as misclassification, exclusion from opportunity, or intensified monitoring [11], [56]. Despite these risks, most manufacturers do not embed ethical principles into procurement, deployment, or oversight.

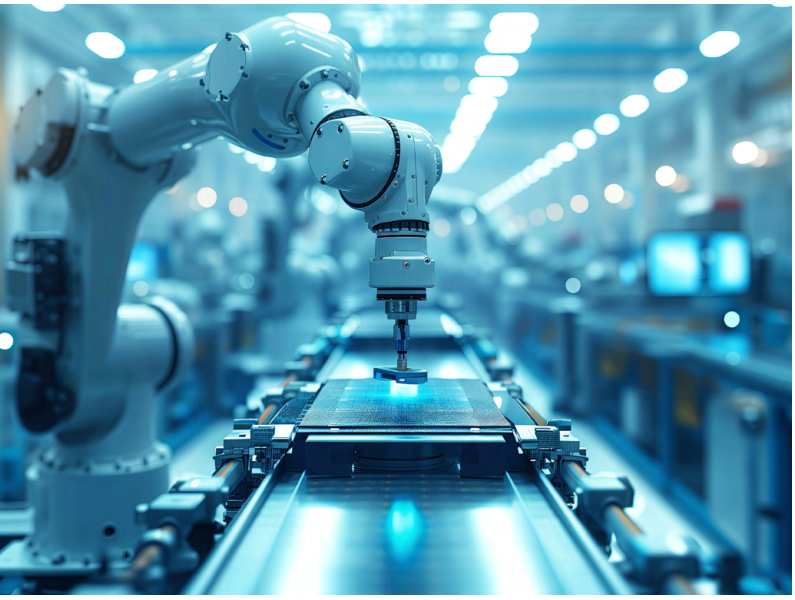
ISO/IEC 23894 and ISO/IEC 42001 provide high-level guidance on fairness and accountability, but their provisions remain abstract unless organizations already maintain mechanisms for engagement, grievance handling, and internal accountability [53], [54]. In practice, ethical ambiguity compounds other human capital gaps, making it difficult for firms to embed AI in ways that are both operationally reliable and socially acceptable [1], [20]. Addressing this challenge requires more than technical upskilling; it demands a systemic approach that integrates emotional readiness, psychological safety, and inclusive workplace ethics as preconditions for AI adoption [11], [23].

3.3.5 Organizational Readiness and Structural Barriers

Most Canadian manufacturers remain in the exploratory or pilot phase of AI adoption, with successful implementations concentrated to a handful of large firms in central Canada [37]. Adoption continues to be challenging due to various structural, financial, technical, and sociopolitical factors, which are outlined in sections 3.3.5.1 through 3.3.5.6.

3.3.5.1 High Costs and Uncertain Return on Investment

Canadian SMEs often cite the high cost of AI implementation as a primary barrier. Expenses related to advanced sensors, cloud services, systems integration, and ongoing maintenance are substantial.



"Most Canadian manufacturers remain in the exploratory or pilot phase of AI adoption, with successful implementations concentrated to a handful of large firms in central Canada."

For smaller firms operating on narrow margins, the expected return on investment is difficult to quantify and often too delayed to justify action [37]. Although large firms such as Bombardier and Harbour Air have achieved meaningful savings through AI-driven predictive systems [40], these examples remain exceptions rather than norms.

3.3.5.2 Infrastructure Gaps and Legacy Systems

Traditional manufacturers often rely on aging machinery and legacy IT systems that are incompatible with modern AI technologies. Many lack the foundational infrastructure required for intelligent automation, including sensor networks for real-time data collection, edge computing capacity, and unified data pipelines capable of streaming high-frequency operational data into centralized or cloud-based systems [2]. In many cases, software environments remain siloed or outdated, with limited interoperability between enterprise resource planning, manufacturing execution systems, and machine-level controls, which makes it difficult to support AI-driven predictive models, anomaly detection, or closed-loop feedback systems [2].

3.3.5.3 Governance Burden and Regulatory Uncertainty

Manufacturers face significant regulatory complexity when considering AI implementation, particularly in safety-critical sectors such as pharmaceuticals, food processing, and chemicals. The absence of clear, cohesive guidance on auditability, liability, explainability, and AI ethics creates hesitancy around scaling past pilot phases [36]. Overlapping federal and provincial jurisdictions further complicate compliance for firms operating across multiple regions [39], and disproportionate public funding continues to broaden the gap between SMEs and large firms and academic institutions [42], [43]. This governance gap has the potential to impact investment by discouraging risk-taking and inhibiting broader participation in industrial transformation.

3.3.5.4 Data Quality, Interoperability, and Systemic Bias

High-quality, interoperable data is a cornerstone of effective AI deployment, but many Canadian manufacturers face challenges due to poor data management and oversight, legacy systems, and siloed information flows [2]. Without consistent formatting, metadata standards, or centralized repositories, AI systems cannot be effectively trained or operate with real-time precision [2], [36]. These technical gaps increase the cost and complexity of implementation, particularly for organizations with limited access to resources. Even when infrastructure is in place, the quality and representativeness of training data are critical. AI systems built on incomplete, outdated, or non-diverse datasets risk perpetuating algorithmic bias, which is an acute issue in hiring, procurement, and safety systems where biased outputs can have economic and ethical repercussions [56].

3.3.5.5 Privacy, Cybersecurity, and Data Governance Risks

AI adoption also raises concerns about data privacy, cybersecurity, and governance, particularly in the absence of comprehensive legal protection for industrial data [59]. Firms are hesitant to share sensitive operational, design, or supply chain information with third-party platforms without clear assurances regarding data ownership, security protocols, and cross-border data transfer.

Canada also relies heavily on foreign cloud platforms, such as Amazon Web Services and Google Cloud, to support AI integration, and this intensifies concerns around digital sovereignty and vendor dependency [43]. In practice, some organizations also look to non-regulatory frameworks—such as the ISA/IEC 62443 series, *Security for industrial automation and control systems* [62]—along with guides from the Association of International Certified Professional Accountants System and Organization Controls (SOC 2) Type 2, to help strengthen security practices, manage cyber-physical risks, and promote more consistent governance across industrial environments.

3.3.5.6 Equity, Inclusion, and Disproportionate Access

Beyond infrastructure, deeper systemic inequalities influence who benefits from AI adoption [37]. Firms owned by women, Indigenous entrepreneurs, and individuals with disabilities are significantly less likely to implement AI tools [37], [55]. This disparity stems from intersecting factors, including constrained access to capital, limited culturally relevant training opportunities, and different risk environments that penalize experimentation [37], [55].

In manufacturing environments, equity challenges are further compounded by data bias and systemic exclusion. When AI systems are trained on datasets that lack diversity or fail to represent minority perspectives, outputs tend to reinforce structural inequities [36], [63]. Fairness in machine learning research repeatedly demonstrates how biased training data can entrench existing hierarchies, disproportionately affecting groups already underrepresented in leadership and technical roles [63].

Advances in AI have also raised concerns about large scale job displacement, workplace well being, and widening inequality, even as evidence suggests that AI can also enhance productivity, create new tasks, and complement human work [64]. Its overall impact on employment may depend, among other factors, on how AI technologies are deployed, the extent to which firms invest in worker retraining, and whether new high productivity tasks emerge to offset automation [64].

3.3.6 Canada's Global Position and Strategic Outlook

AI adoption in manufacturing varies significantly across leading global economies, shaped by national priorities, digital infrastructure maturity, and coordinated policy frameworks. The US and China lead AI integration at scale, emphasizing predictive maintenance, logistics, and autonomous robotics [43], [65], [66]. Germany excels in Industry 4.0 precision automation, Japan in adaptive robotics, and the UK in sustainability-focused AI aligned with environmental mandates [34], [43]. These countries not only advance core technologies but also embed AI within their broader industrial strategies.

Canada, by contrast, is widely recognized for its ethical approach to AI and for foundational leadership in research, talent development, and responsible innovation. Government strategies such as the Pan-Canadian AI Strategy and the Digital Charter emphasize principles of inclusion, accountability, and fairness [13], [42]. Canada is also a founding member of the Global Partnership on Artificial Intelligence (GPAI) and plays an active role in shaping international norms through forums such as the Organisation for Economic Co-operation and Development (OECD) and the G7 [67], [68]. However, this leadership in ethics and research has not yet translated into scaled industrial implementation [14], [37], [42]. Most manufacturers in Canada continue to rely on open-loop AI systems that require human oversight, while global leaders increasingly deploy closed-loop systems with real-time optimization and minimal intervention [17], [18].

A review of global trends also reveals key industry-specific patterns. Automotive, aerospace, and electronics sectors dominate AI adoption, capitalizing

on robotics, digital twins, and AI-powered predictive maintenance for measurable performance gains [17], [18]. Traditional industries such as textiles, heavy machinery, and primary metals remain constrained by legacy systems, high integration costs, and limited AI expertise, often depending on manual oversight of AI tools [7], [14]. Table 1 presents a nation-by-nation comparison of AI adoption focus areas, technologies, implementation mechanisms, and challenges.

Further analysis reveals three key dimensions that distinguish Canada from global leaders: (a) industrial strategy and coordination, (b) infrastructure and scaling capability, and (c) workforce/standards integration.

First, in terms of industrial strategy and coordination, global leaders such as Germany, Japan, China and the US not only invest in AI, but they also integrate AI into their national industrial strategies [43], [44], [66]. For example, Germany's Industrie 4.0, Japan's Society 5.0, and China's Made in China 2025 initiatives align government policy, industry, workforce development, and infrastructure around a unified mission. In contrast, Canada has world-leading AI research and strong ethical principles, but industrial adoption remains fragmented, driven by isolated firms, regional clusters, or pilot projects rather than a coordinated national roadmap.

Second, in terms of infrastructure and scaling capacity, countries such as the US and China pair AI with major investments in digital infrastructure, including high-performance computing, factory testbeds, cloud platforms, and robotics manufacturing zones [66]. Germany and Japan help smaller enterprises to adopt AI through subsidized testing centres, advisory hubs, and national funding mechanisms [44]. In Canada, SMEs face, among other challenges, high costs of the technologies, limited digital infrastructure, and skills gaps in the work force [37], [43].

Third, in terms of workforce capability and standards, global leaders approach these as core to AI readiness and not as an afterthought [43]. In Canada, interviewees described a gap in which many firms use AI terminology but lack the mathematical, technical, or ethical literacy to critically assess the systems they purchase. Without strong foundations in OH&S, labour standards, equity, and AI literacy, adoption of AI may increase stress, mistrust, and inequality rather than improve productivity.

This analysis reveals both structural and cultural distinctions. Canada shares many of the same focus areas as peer economies, particularly predictive maintenance, digital twins, and logistics optimization, but diverges in its scale of implementation and policy coordination. In Germany, Japan, and the US, industrial AI integration is reinforced by strong public–private coordination, dedicated manufacturing testbeds, and incentive programs that link research directly to production.

Countries that are more successful in integrating AI into manufacturing tend to combine three reinforcing elements:

- A coordinated national industrial strategy that positions AI as essential infrastructure;
- Applied mechanisms for scaling, such as subsidized testing facilities, shared data platforms, and SME-specific advisory programs; and
- A workforce model that treats safety, ethics, and productivity as inseparable.

Canada can draw several lessons from the approaches used by these global leaders, including aligning research investments with industrial deployment goals, developing shared testbeds and funding models that de-risk SME adoption, and embedding AI readiness into vocational training and occupational safety systems.

While Canada's AI landscape in the manufacturing sector demonstrates clear strengths in high tech sectors, cleantech, and pilot-scale innovation, particularly in Ontario, Quebec, and British Columbia, national deployment remains fragmented, constrained by digital infrastructure gaps, underdeveloped human capital pipelines, and limited coordination across jurisdictions. The development of a cohesive and inclusive AI strategy, anchored in ethical governance and backed by investment in infrastructure and workforce development, is essential to convert Canada's isolated successes into a broad industrial transformation.

Table 1: Global Comparison of AI Adoption in Manufacturing.

Country	Key Focus Areas	Leading AI Technologies	Policy and Support Mechanisms	Challenges
Canada	Aerospace, automotive, cleantech, supply chains [40], [42]	Predictive maintenance, digital twins, AI logistics, computer vision [40]	Pan-Canadian AI Strategy, Scale AI, Digital Charter, federal R&D funding [13], [42], [47]	Low SME adoption, legacy infrastructure, regional disparities [37], [38], [43]
China	High tech, electronics, logistics [66]	AI robotics, smart logistics, visual inspection [66]	State-funded industrial automation zones, Made in China 2025 initiative [66]	Data security, regulatory opacity [66]
Germany	Automotive, logistics, precision engineering [34]	Industry 4.0, cobots, predictive analytics [34]	Industrie 4.0 strategy, government R&D subsidies, SME digitization programs [34]	SME digital divide, integration challenges [34]
Japan	Automotive, robotics, electronics [43]	Adaptive robotics, real-time control, smart sensors [43]	Strategic AI robotics initiatives, automation modernization grants [43]	High costs [43]
United States	Aerospace, automotive, pharmaceuticals [43], [65]	Predictive analytics, robotics, digital twins, supply chain AI, [43], [65]	National AI Initiative, strong private R&D ecosystem, NIST Artificial Intelligence Risk Management Framework	SME adoption barriers fragmented implementation landscape [43]

3.3.7 Summary of the Canadian AI Landscape in Manufacturing

The landscape of AI adoption in Canadian manufacturing is defined by a combination of localized excellence and systemic constraint. While select high tech firms and regions (Ontario, Quebec, and British Columbia) have demonstrated strong use cases for predictive maintenance, intelligent quality control, and sustainable operations, broader uptake across the sector remains fragmented. Canada lags behind global leaders not due to a lack of research expertise or investment potential, but due to structural limitations in digital infrastructure, workforce capacity, regulatory coordination, and support for SMEs.

As global competitors advance closed-loop AI systems and integrated automation at scale, Canadian manufacturing continues to rely heavily on open-loop models and pilot stage implementations. The divide between digitally mature firms and the majority of SMEs reflects deeper economic and institutional imbalances, including limited capital access, data fragmentation, and dependency on foreign cloud providers. These barriers are not solely technical and are embedded in Canada's policy architecture, investment patterns, and inconsistent regional development.

However, the opportunities remain substantial. Successful Canadian pilots have illustrated that AI can significantly reduce downtime, enhance product quality, optimize energy use, and improve workplace safety. If supported by targeted policy intervention, expanded training infrastructure, and a cohesive national AI strategy, these outcomes could be scaled more widely.

3.4 Regulations, Standards, and Frameworks

While no unified system currently governs AI use in industrial contexts, a growing patchwork of voluntary standards, enforceable regulations, and strategic policy frameworks is beginning to shape expectations around safety, accountability, and innovation. However, these are still emerging and are inconsistently applied across jurisdictions.

In the absence of a unified governance framework, manufacturers are often left to assemble their own compliance strategies from a mosaic of federal regulations, national and international standards, and emerging best practices. This approach demands not only technical acumen but also a foundational understanding of hazard identification and risk management. Without a systems-level perspective, organizations may overemphasize familiar or visible risks, such as equipment failure or cybersecurity, while overlooking less tangible but equally critical domains, such as data governance, ethical AI use, or psychosocial harm.

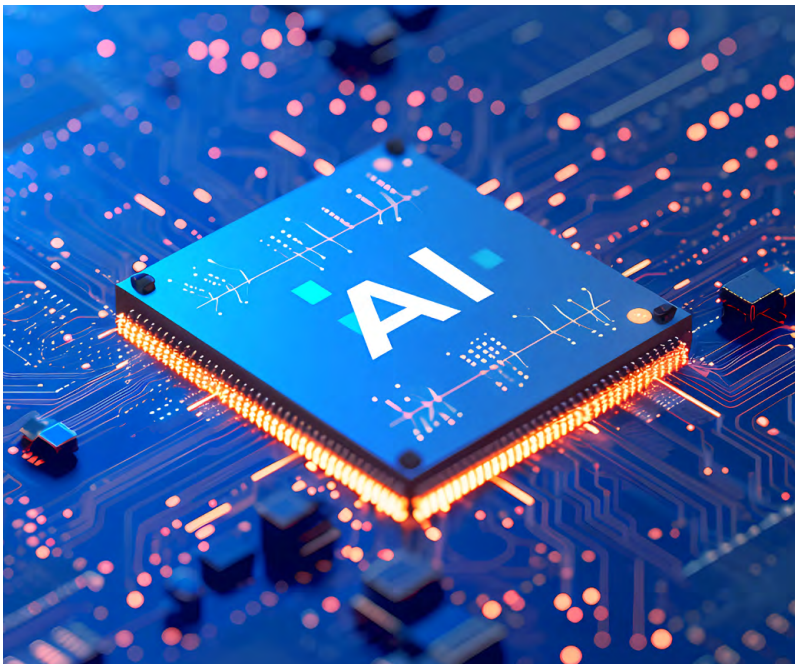
As AI systems become increasingly embedded in decision-making and workplace processes, the ability to anticipate and mitigate a full spectrum of risks, including those that affect worker mental health, job control, and organizational fairness will be essential for safe and sustainable implementation. This section examines the current governance landscape across three key categories:

1. **Regulations:** Both national and international, which define legal obligations but often lag behind technological development.
2. **Standards:** Including those from CSA Group, ISO, IEEE, and others, which offer guidance on risk management, system design, and ethical deployment.
3. **Strategic frameworks and policy initiatives:** Which support innovation and ethical use but lack binding authority.

Each category is assessed for its scope, applicability, and relevance to AI deployment in the manufacturing sector. The section concludes with a synthesis of the strengths and limitations of the current governance landscape, highlighting key gaps and coordination challenges that may affect Canada's long-term competitiveness and AI readiness.

3.4.1 Regulations

This section provides an overview of the current regulatory environment for AI in manufacturing, beginning with Canada's proposed and existing enforceable tools, then expanding to discuss



international regulations that influence or intersect with industrial AI governance. Finally, the section considers these instruments through the dual lens of the AI system lifecycle and risk theory, evaluating how well they identify, mitigate, and enforce protections against emerging risks in real-world deployment. This approach aligns with ISO/IEC 22989, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology* [69]. The analysis also considers concepts from ISO/IEC 23053, *Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)* [70], and from the NIST *Artificial Intelligence Risk Management Framework* (AI RMF 1.0) [71].

3.4.1.1 Canadian Regulations

Canada currently lacks a unified regulatory regime for AI. The country's most ambitious attempt to introduce such legislation was the *Artificial Intelligence and Data Act,* which was introduced as part of Bill C-27 but died on the order paper when Parliament was prorogued in January 2025 [72], [73], [74]. The proposed Act aimed to establish a risk-based compliance regime for "high-impact" AI systems, but was widely criticized for its constitutional fragility, lack of alignment with international norms, and inadequate engagement with relevant interested parties [72], [73], [74]. Analysts also

noted that its exclusion of public sector systems and lack of independent oversight further weakened the Act's credibility and viability [72], [73].

In the absence of AI-specific law, Canadian manufacturers must navigate a patchwork of existing legislation and other instruments, many of which were designed for broader purposes but carry implications for AI deployment, including:

- **Personal Information Protection and Electronic Documents Act (PIPEDA):** Applies to AI systems that process personal data in HR, marketing, or surveillance [75].
- **Provincial OH&S Acts:** Increasingly used to address psychosocial risks linked to algorithmic scheduling or digital monitoring (e.g., CNESST in Quebec) [76]–[88].
- **Canadian Human Rights Act and Canada Labour Code:** Protect against algorithmic discrimination and unfair labour automation practices [89], [90].
- **Directive on Automated Decision-Making:** Applies primarily to public sector AI [49].
- **Export Controls and Industrial Security Protocols:** Affect AI deployment in sensitive sectors such as defence and aerospace [91].
- **Net-Zero Emissions Accountability Act:** Although not AI-specific, it incentivizes AI for emissions tracking and sustainability compliance [92].

While these offer some indirect protections, none are tailored to the nuances of AI-enabled systems in industrial environments, so they do not provide a coherent compliance pathway.

3.4.1.1.1 Lifecycle and Risk Governance Gaps

Mapping Canada's legislation and other instruments across the AI system lifecycle (design, development, deployment, decommissioning) reveals significant gaps across the lifecycle phases [36], [69], as shown in Table 2.

Canada's governance strategy has not yet embraced multidimensional risk frameworks that go beyond physical safety to include psychological, systemic, and ethical dimensions [42], [69]. The following hazards are currently unregulated, despite their relevance in high-trust industrial environments (i.e., workplaces that foster strong relationships between human workers and AI systems, enabling seamless and effective cooperation) where human-AI collaboration is common:

- Cognitive overload due to alert-fatigued monitoring systems;
- Autonomy erosion due to opaque AI decision-making; and
- Bias propagation due to historical training datasets.

Table 2: Observed AI System Lifecycle Coverage and Gaps.

Lifecycle Phase	Existing Coverage	Observed Gaps
Design and Development	PIPEDA; Export controls	No mandatory impact assessments, third-party validation, or safety documentation
Testing and Validation	Directive on Automated Decision-Making (public sector)	No AI-specific safety or fairness testing proto-cols; OH&S requires general hazard assessment but does not address algorithmic bias or dynamic AI risks
Deployment and Operation	OH&S Acts; *Canadian Human Rights Act; Canada Labour Code;* Net-Zero Emissions Accountability	Limited oversight of dynamic AI behaviour, psychosocial harms
Decommissioning	None	No regulation of sunset protocols, data disposal, or accountability post-use

3.4.1.1.2 Practical Challenges for Manufacturers

For manufacturers, regulatory fragmentation poses serious challenges, including:

- **Access to expertise:** Few SMEs have in-house legal or AI audit capabilities, meaning they lack the ability to assess and verify AI systems for compliance, bias, safety, and accountability. This increases both the cost and uncertainty of adoption [6], [37], [93].
- **Limited legal clarity:** Many legal tools (e.g., PIPEDA, OH&S) were not written with AI in mind, leaving room for interpretation [94].
- **Unclear enforcement:** Most instruments are reactive and complaint-driven, with no proactive oversight mechanisms [73], [94].
- **Barrier to innovation:** Without tailored pathways or regulatory sandboxes, cautious firms may delay adoption [42], [72], [95].

Together, these issues compound the perception of legal ambiguity and regulatory burden, making responsible AI implementation feel more like a liability than an opportunity. These barriers are further examined in the lifecycle and risk governance analysis in Section 3.4.4.

3.4.1.2 International Regulations

As global AI adoption accelerates, countries have taken varied approaches to regulating its development and deployment. While some jurisdictions have introduced enforceable legal regimes, others rely on voluntary frameworks, ethical guidelines, or sectoral oversight. These differences directly shape the conditions under which manufacturers operate, especially in cross-border contexts involving automation, data processing, and AI-enabled decision-making.

To assess the relevance and impact of international regulation on Canadian manufacturing, this section provides an overview of major regulatory models in five key regions, followed by an evaluation of their lifecycle coverage and practical implications.

3.4.1.2.1 International Regions Overview

European Union

The European Union (EU) has emerged as a global leader in prescriptive AI regulation. The *EU Artificial Intelligence Act,* 2024 *(AI Act)* was passed in 2024 and will enter into force in stages between 2025 and 2027. It introduces a mandatory risk-based classification for AI systems with four tiers: unacceptable, high, limited, and minimal [96]. Unacceptable risk systems (e.g., social scoring, emotion recognition in workplaces, or untargeted facial recognition scraping) are prohibited entirely under the *AI Act* [96]. High-risk AI systems, particularly those used in manufacturing automation, predictive maintenance, worker evaluation, or biometric access control, are subject to conformity assessments, technical documentation, and ongoing post-market monitoring. Developers of such systems must maintain a risk management system, ensure human oversight, and meet accuracy, robustness, and cybersecurity requirements across the system lifecycle [96], [97].

The *AI Act* also applies extraterritorially, so non-EU providers and users must comply if their AI systems impact individuals in the EU. This positions the AI Act as part of the so-called Brussels Effect, in which European regulatory norms are exported globally [98]. The AI Act also complements the EU's General *Data Protection Regulation* (GDPR), particularly where AI systems involve the processing of personal data (e.g., in HR analytics or customer segmentation) [99].

Importantly, the *AI Act* introduces obligations for general purpose AI models, including transparency requirements, copyright compliance, and, in the case of systemic risk models, mandatory adversarial testing and incident reporting.

United States

The US follows a decentralized, sector-specific approach to AI governance that is managed state by state, rather than at the federal level. Where it exists, federal regulatory responsibility is fragmented across agencies such as the Food and Drug Administration for health technologies and the Federal Trade Commission for consumer protection, which results in inconsistent



enforcement. NIST has also developed the Artificial Intelligence Risk Management Framework as a voluntary guideline for promoting safe and trustworthy AI [71]. While this innovation-first model promotes flexibility and market responsiveness, it lacks cohesive oversight for AI applications in industrial manufacturing. Recent federal action, including the *Executive Order Ensuring a National Policy Framework for Artificial Intelligence,* highlights growing concern that a fragmented landscape of state level AI laws creates compliance burdens, ideological inconsistencies, and barriers to innovation; in response, the Order calls for a unified "national standard" that limits conflicting state regulations and safeguards children, communities, copyrights, and interstate commerce [100]. In parallel, manufacturers emphasize the need for sector-specific rules, workforce upskilling, and improved data governance to reduce confusion and regulatory gaps [101].

China

China's regulatory approach is state-centric and aligned with national strategic priorities. Its Data Security Law and Personal Information Protection Law impose strict data localization and cybersecurity obligations on AI developers and users, with penalties for non-compliance [102]. China's New Generation Artificial Intelligence Development Plan promotes the rapid integration of AI into key industries, including manufacturing, logistics, and energy infrastructure [103]. State funding and centralized planning ensure scalability and deployment speed, but raise concerns around civil liberties, algorithmic transparency, and international interoperability. China's model prioritizes data sovereignty, industrial growth, and geopolitical competitiveness over procedural accountability [103], [104].

Japan

Japan emphasizes ethical AI through voluntary compliance frameworks. As part of its AI strategy, Japan published the Social Principles of Human-Centric AI in 2019, which advocate for fairness, transparency, explainability, and human dignity as guiding tenets for AI development [105]. National AI standards developed under the Japanese Industrial Standards Committee support smart factory integration and robotics. This approach has yielded high uptake in Japan's precision manufacturing and automation sectors. However, the absence of binding legal instruments limits consistency and enforceability across organizations. The effectiveness of Japan's model relies on corporate culture and social trust rather than regulatory compulsion.

United Kingdom

The UK has adopted a hybrid governance model that combines centralized ethical oversight with sectoral flexibility. Institutions such as the Office for Artificial Intelligence and the Department for Science, Innovation and Technology shape national policy on AI development and deployment [106]. In manufacturing, the UK emphasizes sustainable AI applications, such as emissions tracking, predictive maintenance, and energy efficiency optimization. While the UK promotes innovation through a light regulatory framework, its reliance on voluntary compliance and self-assessment mechanisms contributes to overall uptake and variable levels of risk mitigation across industrial sectors.

3.4.1.2.2 Lifecycle and Risk Governance Gaps

Mapping international regulatory regimes across the AI system reveals uneven coverage and jurisdiction-specific gaps, as shown in Table 3. While some countries have codified oversight mechanisms in key lifecycle stages, most frameworks remain incomplete, particularly in addressing downstream risks such as psychosocial harm, human-machine teaming, and post-deployment accountability.

Across jurisdictions, AI standards and practices remain focused predominantly on front-end design and pre-deployment assurance, while downstream risks are insufficiently addressed. Few countries offer enforceable tools for managing adaptive behaviour, unintended consequences, or cumulative harms, especially in complex environments such as manufacturing. Specific gaps include:

- **Psychosocial and human factors:** No jurisdiction mandates protections against over-surveillance, decision fatigue, or erosion of worker autonomy from AI-enabled scheduling, monitoring, or evaluation systems.

Table 3: Lifecycle and Risk Governance Gaps in Select International Regulations.

Lifecycle Phase	Coverage Across Jurisdictions	Observed Gaps
Design and Development	EU AI Act mandates risk management, bias mitigation, and data governance for high-risk systems [96]. China requires security reviews under its *Data Security Law* [102], [103]. Japan and UK promote ethical-by-design principles [105], [106].	US lacks enforceable design-stage requirements. Japan and UK have no mandatory pre-market documentation or independent review.
Testing and Validation	EU requires conformity assessments for high-risk applications [97]. China uses internal auditing [103]. US relies on voluntary frameworks (e.g., NIST Risk Management Framework) [71]. Japan and UK encourage internal testing [105], [106].	No global framework for third-party validation. Lack of enforceable protocols in US, Japan, UK, and China (outside select sectors).
Deployment and Operation	China enforces data localization and usage audits [103]. EU mandates post-market monitoring [96], [97]. UK offers sector guidance on sustainability [106]. US oversight is agency specific [101].	Limited regulation of dynamic system behaviour (e.g., learning systems). Little attention to psychosocial risks or explainability.
Decommissioning	No jurisdiction mandates enforceable rules for AI system sunset, data destruction, or ac-countability at end-of-life [96], [103], [105], [106].	Decommissioning protocols are absent across all reviewed countries. No legal safeguards for legacy system impacts or misuse.

- **System adaptivity and drift:** Even in the EU, where conformity assessments exist, adaptive systems that evolve post-deployment (e.g., reinforcement learning) pose enforcement challenges that are not addressed in current mechanisms.
- **Post-market surveillance:** While the *EU AI Act* includes obligations for high-risk system monitoring, no country has established sector-specific reporting regimes for AI system failures, near misses, or safety deviations in manufacturing.
- **Transparency and auditability:** Several models (e.g., US NIST Artificial Intelligence Risk Management Framework, Japan's Social Principles of Human-Centric AI) emphasize transparency, but none require structured algorithmic audits or standardized documentation accessible to end-users or workers.
- **Global alignment gaps:** Despite common reference to ethical AI principles (e.g., OECD, GPAI), cross-border interoperability remains weak, particularly between state-centric models (e.g., China) and voluntary industry-led approaches (e.g., US and Japan).

Ultimately, most regulatory regimes fail to fully operationalize lifecycle accountability. Canada's manufacturing sector, which relies on global suppliers and markets, will need to account for these governance gaps when integrating imported systems or exporting AI-enabled products to jurisdictions with divergent rules. This underscores the value of adopting AI lifecycle management standards (e.g., ISO/IEC 5338) to bridge international inconsistency and internal readiness gaps. These gaps are further examined in the lifecycle and risk-based analysis in Section 3.4.4.

3.4.2 Standards

The adoption of AI in manufacturing is shaped by a growing ecosystem of standards and management system frameworks issued by organizations such as the CSA Group, ISO/IEC, IEEE, and others. However, their structure, scope, and accessibility vary significantly.

This section reviews national and international standards through the dual lens of lifecycle alignment and risk governance gaps.

The section concludes with a critical analysis of standards uptake, alignment gaps, and the need for coordinated national strategies to translate voluntary frameworks into meaningful governance practice across the Canadian manufacturing sector.

3.4.2.1 Canadian Standards

In Canada, at the time of writing, there is no overarching legislation guiding the adoption of AI. In the absence of such legislation, standards can provide important guidance for manufacturers. This section focuses on key standards in AI governance and lifecycle management that have been adopted by CSA Group, including:

- ISO/IEC 22989, *Information technology — Artificial intelligence — Artificial intelligence concepts and terminology* [69];
- ISO/IEC 23053, *Framework for artificial intelligence (AI) systems using machine learning (ML)* [70];
- ISO/IEC 23894, *Information technology — Artificial intelligence — Guidance on risk management* [53];
- ISO/IEC 42001, *Information technology — Artificial intelligence — Management systems* [54];
- ISO/IEC 5338, *Information technology — Artificial intelligence — AI system life cycle processes* [107]; and
- ISO/IEC 5339, *Information technology — Artificial intelligence — Guidance for AI applications* [108].

While a subset of standards references AI, they do not exist in isolation. In manufacturing, AI-enabled systems are deployed within environments already governed by physical safety, occupational health, and cybersecurity requirements. These standards form the foundation upon which AI-specific standards are built and interpreted, and include:

- **Physical safety:** CSA Z432, *Safeguarding of machinery* [109]; and CSA Z460, *Control of hazardous energy — Lockout and other methods* [110].
- **Occupational health:** CSA Z1002, *Occupational health and safety – Hazard identification and elimination and risk assessment and control* [111]; and CAN/CSA-Z1003/BNQ 9700-803, *Psychological health and safety in the workplace* [61]. ISO 45003. Occupational health and safety management — Psychological health and safety at work — Guidelines for managing psychosocial risks [112] is an international guideline that aligns closely with the principles of Canada's CAN/CSA Z1003/BNQ 9700 803 standard.
- **Cybersecurity and data governance:** ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements* [113]; and ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors* [114].

This standards ecosystem enables alignment with internationally recognized best practices while addressing topics such as human-machine teaming, algorithmic surveillance, and AI-driven productivity monitoring [107], [53], [115], [116].

In response to emerging needs, the following technical reports that address novel risk dimensions have been published:

- ISO/IEC TR 5469, *Artificial intelligence — Functional safety and AI systems* [117]; and
- ISO/IEC TR 24027, *Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making* [118].

These reports provide valuable reference material for manufacturers seeking to integrate fairness, transparency, or functional safety practices into their AI programs through the lens of bias identification, assessment, and mitigation across the AI lifecycle. However, several systemic limitations remain that constrain standards implementation in manufacturing contexts.

3.4.2.1.1 Systemic Limitations to Adoption and Implementation

Interviewees noted that many standards provide high-level frameworks with few operational tools or examples for manufacturers to follow. Manufacturers frequently report difficulty with applying these standards to real-world processes, particularly when integrating AI into complex, legacy industrial environments. Practitioners expressed a need for more accessible implementation supports, such as annotated checklists, sector-specific use cases, and hands-on playbooks.

While ISO/IEC 5338 [107], ISO/IEC 5339 [108], and ISO/IEC 23894 [53] are designed to be complementary, manufacturers often report difficulty with applying them in a coordinated way. Manufacturers inexperienced with implementing standards may be uncertain about the sequence, integration points, or practical distinctions between the different standards. A lack of lifecycle-aligned tools, contextual examples, or guidance on how to use the standards together in a manufacturing setting could lead to confusion.

While CSA's alignment with ISO/IEC frameworks enables interoperability across borders and supply chains, the benefits are not automatic. Manufacturers would benefit from having the internal capacity to map these standards to real-world systems, especially in cases where AI introduces new forms of risk (e.g., autonomous control loops or algorithmic management).

Canada's standards ecosystem for AI in manufacturing offers a valuable foundation to manufacturers, but without tailored support, contextualization, and improved sequencing across documents, the practical benefits may remain unrealized in many industrial settings. These risks are further examined in the lifecycle and risk-based analysis in Section 3.4.4.

3.4.2.2 International Standards

Internationally, AI standardization efforts have intensified across organizations, including ISO, IEC, IEEE, and the International Society of Automation (ISA), who have developed a growing suite of instruments that

address core themes, such as lifecycle consistency, cybersecurity, human-system interaction, data infrastructure, and workplace safety and ethics. International standards of particular relevance to manufacturing include:

- ISO/IEC 42001, *Information technology — Artificial intelligence — Management systems* [54];
- ISO/IEC 5338, *Information technology — Artificial intelligence — AI system life cycle processes* [107];
- ISO/IEC 23894, *Information technology — Artificial intelligence — Guidance on risk management* [53];
- ISO/IEC 38507, *Information technology — Governance of IT — Governance implications of the use of artificial intelligence by organizations* [115];
- IEEE 2671, *General requirements of online detection based on machine vision in intelligent manufacturing* [116];
- ISA/IEC 62443 *Series, Security for industrial automation and control systems* [62]; and
- ISO 45003, *Occupational health and safety management — Psychological health and safety at work — Guidelines for managing psychosocial risks* [112].

These instruments offer technical rigour, lifecycle alignment, and cross-sector adaptability. As AI becomes more embedded in production environments, these standards will serve as crucial scaffolds for managing safety, lifecycle consistency, data integrity, and ethical oversight [1], [3], [14]. However, their adoption across the manufacturing sector remains inconsistent.

Research has noted that while these standards are well-developed, their voluntary nature means they function more as a list of options rather than a structured approach for universal application [36]. This is reflected in a lack of coordinated integration across organizational functions, such as IT, safety, compliance, and operations. As a result, certain high-impact domains, such as explainability, psychosocial risk, and human-AI teaming, may be underemphasized, despite the availability of standards and technical reports, such as ISO 45003 and ISO/IEC TR 24027 [112], [118].



In the Canadian context, international standards are critical for ensuring interoperability across global supply chains. AI tools developed abroad often adhere to ISO/IEC lifecycle and cybersecurity requirements, and Canadian firms must adapt their systems to integrate those components [37]. Similarly, Canadian exporters must often meet standards such as the ISA/IEC 62443 series [62] or ISO/IEC 27001 [113], regardless of domestic mandates. This strategic dependence on international frameworks underscores the need for greater policy coherence and practical adoption pathways in Canadian manufacturing settings [4], [94].

3.4.2.2.1 Limitations and Gaps in International Standards

Although international standards provide essential scaffolding for lifecycle alignment, interoperability, and ethical oversight, several limitations constrain their practical utility for manufacturers. First, adoption remains fragmented and reactive.

Second, while the instruments are technically rigorous, their voluntary nature limits enforceability and creates variability in application [36]. In the absence of mandatory obligations, firms may selectively implement elements of standards, leading to inconsistent practices both within and across jurisdictions. This inconsistency is compounded by the lack of coordinated integration across organizational domains, where standards often overlap without clear harmonization.

Third, certain key domains remain underemphasized in manufacturing practice, despite the existence of relevant standards. Psychosocial risks, bias and fairness, and human-machine teaming are formally addressed in instruments such as ISO 45003 [112] and ISO/IEC TR 24027 [118], but their uptake in industrial contexts to date has been limited [20], [96]. The prevailing focus remains on technical robustness and cybersecurity, leaving other critical domains underdeveloped.

Finally, Canadian manufacturers face a dependency challenge. Because international standards frequently establish the baseline for global supply chain participation, Canadian firms must adapt to them regardless of domestic mandates [94]. Without complementary national supports to contextualize these frameworks, reliance on international standards can create additional resource burdens and reinforce adoption challenges across firm sizes [56].

Taken together, these gaps suggest that while international standards establish a strong technical and ethical foundation, their voluntary status, slow uptake, and limited sectoral contextualization prevent them from fully realizing their governance potential in manufacturing settings. These limitations and gaps are further examined in the lifecycle and risk-based analysis in Section 3.4.4.

3.4.3 Strategic Policies and Initiatives

The governance of AI in manufacturing extends beyond enforceable legislation and voluntary standards to include a range of strategic policies, funding initiatives, and public–private programs that promote ethical AI development, drive innovation, and enhance economic competitiveness. These mechanisms do not carry the force of law, nor do they necessarily provide clear operational or compliance guidance for industrial organizations. Instead, they shape priorities, enable experimentation, and signal preferred directions for AI adoption and governance.

This section provides an overview of relevant policy frameworks and initiatives, organized in three parts: (a) Canadian policies and initiatives, (b) international frameworks and strategic efforts, and (c) practical implementation challenges experienced by manufacturers in engaging with these instruments.

3.4.3.1 Canadian Policies and Initiatives

Canada's approach to AI policy has emphasized ethical leadership, research excellence, and ecosystem development. Some major initiatives include the world's first national AI strategy [13], an AI-focused innovation cluster [47], SME adoption programs [52], and provincial innovation agendas. While these initiatives reflect a strong public commitment to responsible AI, their effectiveness for industrial deployment is uneven. Sections 3.4.3.1.1 through 3.4.3.1.6 review six major policy instruments, highlighting their contributions, limitations, and relevance to the manufacturing sector.

3.4.3.1.1 Pan-Canadian AI Strategy

Launched in 2017 and led by the Canadian Institute for Advanced Research, the Pan-Canadian AI Strategy was the first national AI strategy in the world [13]. It supports three major research hubs (Mila, Amii, and the Vector Institute) and emphasizes ethical AI, international collaboration, and academic excellence. While the strategy has bolstered Canada's AI research reputation, it has been critiqued for its concentration of funding in elite institutions and limited translation into applied industrial or regulatory tools, particularly for sectors such as manufacturing [42], [63].

3.4.3.1.2 Scale AI Cluster

Scale AI is Canada's AI-focused innovation cluster, investing in AI adoption projects across supply chain, logistics, and predictive maintenance. It connects startups, researchers, and enterprises, including those in adjacent manufacturing domains [47]. While its

co-investment model has enabled innovation at scale, several reports note that smaller firms often face difficulty participating due to high match funding requirements, technical capacity expectations, and the complexity of proposal processes [37].

3.4.3.1.3 Canada Digital Adoption Program

The Canada Digital Adoption Program supports digital onboarding for Canadian SMEs through grants and advisory services [52]. It is effective in helping businesses adopt foundational tools such as e-commerce platforms and customer relationship management tools. However, it lacks depth in supporting advanced AI applications that involve real-time control, machine vision, or ethical governance. Consequently, it offers limited value for manufacturers navigating AI complexity.

3.4.3.1.4 Quebec Research and Innovation Investment Strategy

Quebec's research and innovation investment strategy (SQRI^2) [119] represents one of Canada's most ambitious provincial innovation agendas, with a $7.5 billion investment across AI, aerospace, advanced manufacturing, and green technologies [120]. It promotes public–private partnerships, talent development, and applied research, positioning AI as a core driver of Quebec's regional competitiveness. The strategy's integration with sector-specific initiatives, such as the Consortium for Research and Innovation in Aerospace in Quebec, facilitates alignment with industrial use cases and strengthens cross-sectoral collaboration.

While SQRI^2 offers a well-funded and forward-looking investment into AI and innovation, expert commentary has noted several areas for improvement, including the need for more participatory governance mechanisms, clearer role definitions across research sectors, and greater transparency in leadership appointments [120]. Furthermore, concerns have been raised about the balance between interdisciplinary ambitions and support for foundational or sector-specific research capacity. Finally, although the SQRI^2 is well-aligned with provincial priorities, coordination with federal policy and national scalability remains an ongoing challenge [119].

3.4.3.1.5 Canada's Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems

Canada's Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems (Code of Conduct on Generative AI) outlines foundational principles for the ethical use of generative technologies, including safety, transparency, fairness, and accountability [121]. However, adoption has been largely symbolic, with uncertain uptake across industrial contexts.

3.4.3.1.6 Other Federal and Provincial Grant Mechanisms

Programs such as the Strategic Response Fund (formerly the Strategic Innovation Fund) [50], the Industrial Research Assistance Program [51], Mitacs [122], and regional economic development grants support AI experimentation in Canada. These funding streams are typically competitive, time-limited, and focused on research or prototyping. Few provide structured pathways for long-term operational adoption, compliance alignment, or lifecycle governance [37].

The policies and initiatives discussed in sections 3.4.3.1.1 through 3.4.3.1.6 demonstrate Canada's sustained investment in responsible AI, but they also reveal systemic limitations for manufacturers. Common challenges include a dominant focus on academic and ethical discourse over applied industrial tools [42], [63], persistent barriers for SMEs in accessing programs [37], weak linkage to lifecycle risk and compliance frameworks [111], and fragmented coordination between federal and provincial levels. These factors constrain the ability of Canada's policy portfolio to support AI adoption at scale in manufacturing.

3.4.3.2 International Policies and Initiatives

International policies and initiatives shape Canada's AI governance indirectly through trade relationships, interoperability pressures, and global norm-setting. While these mechanisms are not enforceable laws in Canada, they influence national strategies, vendor obligations, and industrial expectations. In the manufacturing sector, alignment with international

frameworks can affect procurement decisions, supply chain requirements, and integration of foreign-developed AI tools. Sections 3.4.3.2.1 through 3.4.3.2.6 review six key international policy instruments and cooperative frameworks that are most relevant to Canadian manufacturers.

3.4.3.2.1 OECD AI Principles

Adopted in 2019, the OECD AI Principles represent one of the first globally endorsed frameworks for responsible AI, promoting inclusive growth, human-centred values, transparency, robustness, and accountability [68]. Canada was an early signatory and has modelled several domestic initiatives on these principles, such as the Pan-Canadian AI Strategy and the Code of Conduct on Generative AI [13], [121]. However, the OECD AI Principles are non-binding and lack implementation mechanisms specific to industrial sectors such as manufacturing.

3.4.3.2.2 European Union Apply AI Strategy and *AI Act*

The EU's Apply AI Strategy [123] is built around a horizontal governance model, combining ethics-driven frameworks, digital rights legislation, and enforceable instruments, such as the *EU AI Act.* The Horizon Europe program and other R&D initiatives also support AI experimentation and deployment [124]. Furthermore, the *EU AI Act* introduces a risk-based classification system and compliance obligations that are expected to become global benchmarks as the act is fully implemented, which means Canadian manufacturers participating in European supply chains may face indirect pressure to conform [94], [96].

3.4.3.2.3 Canada–European Union Digital Partnership

The Canada–EU Digital Partnership is a bilateral policy framework aimed at enhancing coordination on digital governance, data protection, and AI ethics [125]. While it has potential to harmonize approaches between Canada's voluntary, principle-based model and the EU's more prescriptive regulatory system, uptake has been limited and mechanisms for industrial application remain underdeveloped [64].

3.4.3.2.4 United States Executive Orders and Sectoral Guidance

The US has not adopted a centralized AI law but has issued several Executive Orders on AI development and deployment, alongside voluntary frameworks such as the NIST Artificial Intelligence Risk Management Framework [71]. These efforts influence international expectations and vendor practices, particularly in areas such as cybersecurity, data integrity, and lifecycle assurance.

3.4.3.2.5 Global Partnership on AI

The GPAI is a multilateral initiative launched in 2020 to promote responsible AI development through applied research, policy coordination, and international cooperation [67]. Canada is a founding member and hosts one of GPAI's Expert Support Centres.

3.4.3.2.6 UNESCO Recommendation on the Ethics of AI

Published in 2021 and adopted by 193 countries, including Canada, the United Nations Educational, Scientific and Cultural Organization (UNESCO) Recommendation on the Ethics of AI emphasizes human rights, sustainability, cultural diversity, and global solidarity [126]. It provides a moral framework for AI policy but is not enforceable and does not contain industry-specific provisions. Nonetheless, it contributes to the broader normative environment shaping expectations around AI accountability, fairness, and societal impact [126].

The international policies and initiatives discussed in sections 3.4.3.2.1 through 3.4.3.2.6 reinforce Canada's positioning in global AI governance but provide limited direct support for manufacturers. For Canadian manufacturers, the practical effect is a patchwork of external pressures that demand interoperability and ethical alignment but stop short of offering clear, sector-specific implementation tools.

3.4.3.3 Gaps and Challenges for Manufacturers

While Canada's strategic AI policies and initiatives, and its participation in global frameworks, reflect a clear ambition to lead in responsible AI, these efforts do not



fully meet the operational needs of the manufacturing sector. The policies and partnerships discussed in sections 3.4.3.1 and 3.4.3.2 signal important commitments, but they do not provide actionable pathways for implementation, particularly for SMEs or manufacturers seeking lifecycle-based guidance.

Although international policy frameworks may seem peripheral to the Canadian context, they exert significant influence over national governance strategies and procurement ecosystems. For example, the *EU AI Act* and the OECD AI Principles set de facto standards for risk classification and lifecycle oversight [68]. However, the absence of clear integration between these international frameworks and Canada's domestic programs means manufacturers are caught in a policy gap, where they are expected to comply with global expectations but lack the tools to do so.

Key challenges include:

- **Lack of operational linkages:** Strategic initiatives emphasize research funding, talent development, or ethical leadership but stop short of offering clear tools for deployment across lifecycle phases [6], [37], [63].
- **Fragmented policy coordination:** Overlaps between federal and provincial programs create administrative burdens and dilute effectiveness [42].
- **SME access constraints:** Match funding, readiness requirements, and complex applications limit participation by smaller firms [6].
- **Weak international interoperability mechanisms:** Global frameworks are not well integrated with Canada's domestic supports, leaving firms unprepared for emerging compliance expectations [94].
- **Absence of accountability infrastructure:** Voluntary guidelines [114], [107] and partnerships remain non-binding and lack sector-specific technical guidance.

Canada's strategic policy ecosystem is rich in vision but underdeveloped in execution. For AI adoption to scale in manufacturing, these instruments must evolve beyond ethical signalling and research investment toward practical supports that enable lifecycle-based governance, interoperability, and equitable access for SMEs. These limitations, along with those identified in the regulatory and standards landscapes, will be further examined in the cross-cutting lifecycle and risk governance analysis presented in Section 3.4.4.

3.4.4 Lifecycle and Risk Governance Analysis

Across Canada's evolving AI regulatory and standards landscape, the interplay between enforceable regulations, voluntary standards, and strategic policy initiatives reveals a disjointed foundation for industrial adoption. Each layer offers support for responsible AI use in manufacturing, but none provides comprehensive lifecycle coverage or operational maturity on its own. To evaluate their combined effectiveness, this section draws on ISO/IEC 42001 [54] and ISO 31000 [127], integrating findings across national and international sources.

ISO/IEC 42001 defines key domains of organizational AI system management, including context awareness, leadership accountability, planning, operational controls, performance evaluation, and continual improvement [54]. ISO 31000 offers an organizational risk management framework centred on integrated, structured, and responsive action [127]. When applied together, these frameworks provide a robust lens for assessing whether Canada's regulations, standards, and policies enable manufacturers to manage AI system-related risks across the full system lifecycle from design to decommissioning.

Table 4 summarizes how these issues surface differently across the three domains of regulations, standards, and policies/initiatives, using the five core governance areas (AI risk management, system explainability, cybersecurity, data lifecycle integrity, and interoperability) as the organizing frame.

The comparative analysis identified several recurring issues:

- **Limited coverage of post-deployment risk:** Across both Canadian and international frameworks, few instruments address system behaviour over time, including AI adaptivity, drift, or psychosocial impacts. This leaves manufacturers without the appropriate tools to monitor or mitigate risks once AI systems are in production [95], [104].
- **Poor integration across oversight layers:** Regulations often operate in isolation from voluntary standards or strategic initiatives. Manufacturers receive little guidance on how to align grant-funded pilots, internal risk controls, and external compliance requirements into a coherent management approach [37], [72].
- **Absence of interoperability pathways:** As global compliance regimes mature (e.g., EU AI Act, OECD AI Principles), Canadian manufacturers will face growing pressure to align. However, few domestic tools explicitly bridge national initiatives with international requirements, leaving exporters at a disadvantage [74], [94].
- **Implementation gaps in risk culture:** While ethical commitments and responsible AI principles are embedded across policies and standards, Canada lacks an enforcement and audit infrastructure capable of transforming these high-level ideals into industry-wide norms, especially in high-risk or complex manufacturing sectors [42].

Overall, Canada's current mix of regulations, standards, and policy initiatives provides a foundation for responsible AI in manufacturing but lacks full lifecycle coherence. Gaps in interoperability, integration across oversight layers, and practical enforcement mechanisms limit the translation of ethical intent into operational maturity. To advance lifecycle-based risk governance, Canada will need to forge stronger links between regulatory instruments, standardization efforts, and policy supports that enable consistent monitoring, accountability, and continuous improvement.

3.5 Interview Findings and Analysis

This section synthesizes insights from 20 semi-structured interviews with experts across manufacturing, AI development, policy, and standards ecosystems. Participants provided a ground-level view of how AI is currently being applied, what constrains or enables its adoption, and how standards and governance frameworks translate—or fail to translate—into practice. Interviews confirmed that AI adoption is not just a technical upgrade but a sociotechnical transformation that reshapes workflows, accountability, and workforce dynamics.

A recurring theme was the need for translation supports. Intermediaries such as Ngen [46], Scale AI, [47] and provincial innovation hubs could play an important role in helping translate standards into more practical tools through training, readiness assessments, and subsidized advisory services. Without these types of supports, adoption could remain fragmented and uneven, particularly for SMEs.

Table 4: Lifecycle and Risk Governance Gaps Across Domains

Core Governance Area	Regulations	Standards	Policies/Initiatives
AI Risk Management	Canadian federal and provincial regulations (e.g., OH&S and human rights acts) provide indirect coverage but lack AI-specific risk protocols [76]–[90]. Internationally, the *EU AI Act* mandates conformity assessments for high-risk systems, while the US relies on voluntary NIST guidance [96], [71].	ISO/IEC 23894 establishes risk management processes for AI [53]. ISO/IEC 5338 provides lifecycle processes, but uptake is uneven and often reactive [107].	Pan-Canadian AI Strategy and Scale AI fund pilot projects but do not provide structured lifecycle-based risk management supports for manufacturers [13], [42], [45], [47].
System Explainability	Regulations rarely address explainability directly. The *EU AI Act* introduces documentation and transparency obligations for high-risk AI, while Canadian privacy laws (e.g., PIPEDA) offer only general data rights and transparency obligations [96], [75].	ISO/IEC TR 24027 provides approaches to bias and explainability, but its use in manufacturing is limited [118]. ISO/IEC 42001 requires oversight processes but leaves interpretive burden on firms [54].	Canada's Code of Conduct on Generative AI promotes transparency, but adoption is symbolic and non-binding [121].
Cybersecurity	Enforcement is fragmented. Canada's cybersecurity obligations stem from general instruments such as PIPEDA and Export Controls, while China mandates strict data localization and audits [75], [103].	ISA/IEC 62443 series is widely recognized for industrial cybersecurity [62]. ISO/IEC 27001 and ISO/IEC 27018 are baseline standards for information security and cloud privacy [113], [114].	Initiatives such as the Canada–EU Digital Partnership aim to align cybersecurity approaches, but industrial implementation remains underdeveloped [94], [125].
Data Lifecycle Integrity	Regulations provide partial protection. The GDPR governs EU data processing [99]; China's Data Security Law restricts cross-border transfer [102], [103]; Canada has no AI-specific regime.	ISO/IEC 5339 offers guidance for AI applications [108], but manufacturers struggle with sequencing alongside ISO/IEC 5338 and ISO/IEC 23894 [107], [53].	Programs such as the Canada Digital Adoption Program support basic digital adoption but do not address complex AI data lifecycle needs (e.g., continuous model retraining, industrial traceability) [52].
Interoperability	International regimes remain misa-ligned. Canadian exporters must meet *EU AI Act* or US procurement expec-tations without domestic harmonization [95], [98].	Standards such as ISO/IEC 42001 and ISO/IEC 38507 enable technical alignment across jurisdictions, but voluntary uptake limits consistency [54], [115].	Multilateral frameworks (e.g., OECD AI Principles, GPAI) promote high-level values, but integration into Canadian manufacturing practice is limited [95].

3.5.1 Use of AI Applications and Technologies in Canada

Interview findings confirmed that Canadian manufacturers engage with AI mainly through narrow, task-specific applications, such as predictive analytics, computer vision, and process optimization for maintenance, quality, and scheduling [3], [28]. Several participants also highlighted applications in energy optimization and agricultural nutrient monitoring, reinforcing global trends linking AI to sustainability and resource efficiency [24], [26].

Many firms operate open-loop AI systems, reflecting the broader hesitancy to transition into autonomous, closed-loop control in high-risk production settings [14], [22]. Only a minority of interview participants described experiments with closed-loop AI, typically in robotic welding, microstructure classification, or digital twin simulations, applications that were also emphasized in advanced international case studies [17], [18]. This corroborates earlier findings (see Section 3.3) that Canada's adoption curve remains shallow, with advanced deployments clustered in specialized or capital-intensive sectors.

Interviews also confirmed that generative AI and LLMs are entering the landscape, but remain supportive rather than operational, and are used mostly for training material generation, document summarization, or marketing content. This matches global assessments that such tools remain experimental and advisory in manufacturing due to concerns about reliability, explainability, and integration into regulated environments [20], [23]. Here, interviews revealed a clear gap between enthusiasm and implementation; while awareness is high, few manufacturers have pathways for integrating generative tools into standards-based workflows or production controls.

Integration maturity remains fragmented [12], [43]. Some firms reported fully embedded AI systems, but most remain in pilot or partial deployment phases. Interviewees stressed the decisive role of data infrastructure, executive sponsorship, and organizational alignment, echoing barriers described in Section 3.3. Without clean data pipelines or internal champions, even technically promising pilots fail to scale.

From a systems perspective, interviews underscored the dominance of discriminative models (e.g., forecasting, anomaly detection), while generative and hybrid architectures are slowly emerging in simulation, control, and collaborative design [26]. Integration into enterprise resource planning and material requirements planning systems and dashboards is growing but often in modular, vendor-driven ways. This is in keeping with the interoperability challenge noted in Section 3.4.4.

Overall, the interviews depicted an ecosystem in transition, characterized by:

- **Broad exploration and shallow integration:** Predictive and assistive tools dominate.
- **Limited closed-loop autonomy:** Advanced deployments are rare and sector-specific.
- **Generative AI at the margins:** Used for support, not production.
- **Fragmented maturity:** Integration depends on infrastructure and leadership, not standards alignment.

The interviews reinforce the findings from the literature review that Canada has been uneven in its approach to AI adoption, and highlight how that uneven readiness amplifies technical and organizational risk [12].

3.5.2 Lessons Learned

Findings from the interviews highlighted five recurring lessons that span the AI lifecycle:

1. **Data readiness is the first bottleneck.** Poor-quality or fragmented data stalls most projects before deployment [1], [14]. SMEs, in particular, often remain uncertain about whether existing infrastructure satisfies lifecycle requirements [12], such as those outlined in ISO/IEC 23894 [53] or related standards.
2. **Explainability defines trust.** Consistent with broader concerns about explainability [20], participants described discomfort with black box systems whose recommendations could not be validated in safety-critical contexts. Several projects were abandoned because leadership could not justify opaque outputs.

3. **Integration fails without governance alignment.** Even technically promising models stalled when developed in IT silos or disconnected from operations, HR, and compliance [12], [28]. The lack of cross-functional ownership led to "pilot purgatory," echoing patterns identified in Industry 4.0 literature [3], [26].
4. **Human factors amplify risk.** Employees expressed anxiety about monitoring, job loss, and digital literacy gaps, confirming that psychosocial and ethical barriers are central—not peripheral—to adoption outcomes [11], [23], [56].
5. **Oversight and accountability gaps persist.** Long-term risks cluster around cybersecurity, data protection, and intellectual property exposure [95]. Few firms maintained internal protocols for bias, transparency, or explainability, illustrating that high-level standards have yet to translate into operational safeguards.

Collectively, these lessons underscore that governance maturity, not algorithmic sophistication, determines success in AI adoption.

3.5.3 Risks and Challenges

Interviewees emphasized that risks and challenges associated with AI in manufacturing cut across the entire value chain, from data capture and model development to deployment, supply chain integration, and long-term oversight. These risks, which are discussed and summarized in sections 3.5.3.1 through 3.5.3.8, are interdependent and weaknesses in one domain often amplify vulnerabilities in others.

3.5.3.1 Cybersecurity and Information Protection

As AI increasingly interfaces with industrial control systems, cloud platforms, and third-party application programming interfaces (APIs), cybersecurity emerged as a foundational concern in the interviews. Every AI system represents a potential attack surface, with data exfiltration, adversarial attacks, and proprietary exposure identified as critical risks. Risks are especially acute in closed-loop environments, where AI outputs directly influence operations.

Standards such as the ISA/IEC 62443 series and ISO/IEC 27001 provide baseline industrial cybersecurity controls, but adoption challenges persist among SMEs [62], [113]. Participants also noted growing pressure from external regimes, such as the *EU AI Act,* which embeds obligations for data integrity and security assurance [94], [96].

3.5.3.2 Safety and Human Factors

Safety risks extend across physical and psychological domains. Physically, AI-enabled robotics, vision systems, and quality controls raise concerns about reliability, fail-safes, and explainability in real-time [42], [63], [53]. These risks intensify in closed-loop systems where autonomous responses may outpace human correction.

Equally significant are psychosocial risks. Participants reported worker anxiety about monitoring, job insecurity, and loss of control, which reflects emerging hazards such as technostress and silent displacement [6], [12], [56]. Standards such as CAN/CSA-Z1003/BNQ 9700-803 [61] and ISO 45003 [112] provide solid frameworks for psychological and occupational health but have not yet been updated to cover AI-specific risks, such as algorithmic opacity or cognitive overload [96].

In terms of safety and psychosocial risks, the issue is not necessarily a lack of standards, but a lack of standards translated into AI contexts. Without deliberate integration of psychosocial and ethical safety provisions into OH&S systems, AI may inadvertently amplify risk rather than mitigate it.

3.5.3.3 Operational Risk and Workflow Disruption

Operational risk surfaced wherever AI tools failed to align with existing workflows. Participants described duplicated systems, inconsistent outputs from generative tools, and pilots that stalled when models could not integrate with legacy software [37], [42], [56]. These findings echo challenges reported in Industry 4.0, where projects remained siloed and failed to scale [6], [12].

Lifecycle frameworks such as ISO/IEC 5338 [107] and ISO/IEC 42001 [54] emphasize planning and continual improvement, but firms struggle to apply them in



complex environments. Again, the issue is not necessarily a lack of standards, but a lack of translation tools such as checklists, templates, and practical examples that bridge lifecycle theory with day-to-day operations.

3.5.3.4 Supply Chain and Ecosystem Complexity

AI deployment across supply chains adds layers of complexity, particularly where models must operate across vendors and data systems. Interviewees described context loss (i.e., models trained in one facility that fail in another) and vendor lock-in as factors that limit flexibility and oversight [37], [42], [56].

While standards such as ISO/IEC 42001 [54] and ISO/IEC 38507 [115] promote accountability and interoperability, their application to supply chain ecosystems remains limited. Few mechanisms exist to ensure AI systems remain portable, auditable, and resilient across vendors. The result is increased brittleness and dependency. Without consistent interoperability standards, AI could amplify systemic fragility [93].

3.5.3.5 Usability and Explainability

Participants repeatedly emphasized that usability and explainability determine adoption success. Poorly designed interfaces or opaque models undermine operator trust, causing reversion to manual processes [42], [63]. In precision environments, lack of interpretability directly compromises safety and accountability [20], [95].

ISO/IEC TR 24027 [118] and ISO/IEC 42001 [54] provide methods and oversight guidance but remain high-level. Interviewees called for sector-specific templates and examples to translate explainability principles into concrete safeguards that non-specialists can use, ensuring tools are not only transparent but also practical.

3.5.3.6 Ethical Risk and Workforce Impact

Interviewees described ethical risks through stories of biased hiring systems, opaque scoring algorithms, and intrusive productivity tracking. Participants described psychological strain from perceived surveillance and unfair metrics, especially for underrepresented or digitally less fluent workers [20], [63].

Displacement fears were widespread, with many describing gradual deskilling rather than layoffs [6], [12], [23]. While standards such as ISO/IEC 23894 [53] and ISO/IEC 42001 [54] outline accountability and bias mitigation, they remain too generic for manufacturing contexts. Ethical implementation still depends on leadership choices, culture, and worker participation, areas that standards have yet to fully operationalize.

3.5.3.7 Governance Gaps and Regulatory Volatility

Interviewees expressed uncertainty over how to manage oversight and accountability amid rapid technological change and slow regulation. Several cited deployments launched before governance mechanisms or approval pathways were in place, creating liability and reputational risks [6], [37], [95].

Concerns also focused on future compliance. Systems implemented today may not meet upcoming obligations under the EU AI Act, potentially requiring costly redesigns or retroactive documentation [94], [96]. At the organizational level, few firms maintain internal governance structures, such as bias audits or cross-functional risk reviews [42], [63].

Standards such as ISO/IEC 42001 [54] and ISO/IEC 23894 [53] provide management frameworks for accountability and continual improvement, but without regulatory harmonization or sectoral implementation tools, uptake remains inconsistent. The result is strategic hesitation as firms risk moving too fast and being penalized or moving too slow and falling behind. Proactive governance clarity and embedded accountability mechanisms are required to stabilize adoption.

3.5.3.8 A Cross-Stream Risk Matrix

As shown in Table 5, participants identified risks across every lifecycle stage, reinforcing that technical, organizational, and human vulnerabilities are tightly connected.

Together, these findings demonstrate that AI is not a discrete tool but an ecosystem-level intervention that reshapes infrastructure, decision-making, and social trust. Meaningful adoption requires staged, human-centred governance that integrates technical validation with psychosocial and organizational safety.

3.5.4 Broader Ethical and Societal Impacts

Participants emphasized that the ethical and social implications of AI are inseparable from technical performance. Many described gradual exclusion of experienced workers through deskilling and loss of tacit expertise, echoing psychosocial risk research [36], [59]. Concerns also centred on algorithmic surveillance and psychological strain when AI tools monitor performance without transparency [20], [23].

Standards such as ISO/IEC 23894 [53] and ISO/IEC 42001 [54] address fairness, accountability, and transparency, while CAN/CSA-Z1003/BNQ 9700-803

Table 5: Risks Identified by Participants Across AI Adoption Domains.

Domain	Key Risks Identified
Cybersecurity	Data breaches, intellectual property theft, adversarial manipulation, cloud vulnerabilities
Safety	Robotic error, failure of quality controls, loss of human oversight, mental health impacts, surveillance stress
Operational	Workflow misalignment, pilot drop-off, over-reliance on untested tools, low interpretability
Supply Chain	Vendor mismatch, system misfit across ecosystems, dependency risk, lack of standards interoperability
Usability	Low explainability, poor user interface, AI illiteracy among staff, trust gaps
Ethical	Bias in decision systems, algorithmic surveillance, silent displacement, lack of informed consent
Governance and Regulatory	Ambiguous accountability, missing internal oversight, regulatory uncertainty, risk of future non-compliance or costly redesign due to evolving standards, deployment–risk misalignment

[61] offers a foundation for psychological safety. However, participants noted that these standards are underused in manufacturing. Without operational tools such as communication protocols, inclusive retraining, ethical audits, and cross-functional oversight, there is a risk that ethical guidance will remain symbolic.

3.5.5 Legislation, Standards, and Frameworks for AI Adoption

Interviews suggested a disconnect between the growing availability of standards and their limited uptake in manufacturing. Participants viewed ISO/IEC 42001 [54] and ISO/IEC 23894 [53] as important but too abstract for direct use. Most SMEs instead rely on vendor frameworks or adjacent-sector practices [6], [12], [43]. Without incentives, certification, or simplified playbooks, there is a risk that standards will remain symbolic rather than operational [95].

3.5.5.1 Regulatory Lag and Strategic Uncertainty

Participants expressed concern that evolving frameworks, including the EU AI Act, could retroactively affect deployed systems, creating redesign and liability risks [94], [95]. For long-lived manufacturing systems, this regulatory lag discourages investment and slows adoption [37], [95].

3.5.5.2 The Usability Gap in Standards Adoption

Despite robust frameworks, interviewees noted that uptake is slow and standards rarely translate into manufacturing contexts. Even well-established OH&S standards, such as CAN/CSA-Z1003/BNQ 9700-803 [61], remain under-adapted to AI-related psychosocial risks. Similarly, ISO/IEC 42001 [54] and ISO/IEC 23894 [53] require interpretation that many SMEs cannot afford without intermediaries.

3.5.5.3 Overcoming Challenges with Practical Solutions

Interviewees proposed several tangible approaches to bridge the usability gap:

- **Start small, prove value, and build confidence.** Early pilots in low-risk domains (e.g., predictive maintenance, document summarization) can generate organizational literacy and provide pathways to later compliance with lifecycle-based standards [6], [12].
- **Build internal champions and cross-functional teams.** Successful adoption often depended on individuals who could bridge technical, operational, and governance domains, translating abstract frameworks into organizational practice [42], [63].
- **Invest in data readiness and interoperability.** Participants consistently linked standards adoption to the precondition of structured, accessible data. Upgrading enterprise resource planning and manufacturing execution systems and implementing data governance practices were seen as essential to aligning with lifecycle frameworks such as ISO/IEC 5338 [107].
- **Leverage intermediaries and partnerships.** Sectoral hubs (e.g., Ngen [46], Scale AI [47], universities, and vendors with transparent practices were identified as key supporters. Shared testbeds or sandboxes were recommended to de-risk experimentation while promoting ecosystem learning.
- **Prioritize usability, transparency, and workforce inclusion.** Embedding interpretability and workforce training into AI adoption was viewed as essential to operationalizing ethical and safety provisions of standards such as ISO/IEC TR 24027 [118] and CAN/CSA-Z1003/BNQ 9700-803 [61].
- **Establish governance early, even in pilots.** Lightweight documentation, review boards, and accountability pathways can ensure that the risk and ethics provisions in ISO/IEC 42001 [54] and ISO/IEC 23894 [53] are incorporated before scaling.
- **Align AI with long-term strategic goals.** Firms that tied adoption to sustainability, resilience, or workforce strategy were seen as better positioned to adapt to evolving compliance obligations, reinforcing findings in the literature on anticipatory governance [37], [95].

3.5.5.4 Synthesis

Overall, interview findings converged on three insights that were consistent with international literature:

1. **The usability gap:** Standards exist but remain too abstract to guide manufacturing adoption without translation into sector-specific tools.
2. **Regulatory lag:** Firms face compliance uncertainty as governance frameworks evolve faster than adoption cycles, especially in capital-intensive manufacturing.
3. **The translation imperative:** Intermediaries, certification schemes, and procurement-linked requirements are necessary to transform high-level frameworks into practical safeguards.

Overall, participants reinforced that standardization will only shape responsible AI adoption in manufacturing if it is practical, anticipatory, and enforceable. Without these conditions, firms risk remaining in pilot purgatory or facing costly compliance shocks as regulatory landscapes mature.

3.6 Case Studies of AI Adoption

This section presents an analysis of 14 selected case studies that illustrate how AI is being implemented across the global manufacturing sector. The cases vary in maturity, geography, industry, and complexity, ranging from real-time defect detection in aerospace and predictive scheduling in Canadian SMEs to fatigue monitoring in visual inspection lines and generative design in pandemic response. A high-level overview of the cases is presented first, followed by a detailed discussion of the risks and challenges, and the section concludes by identifying lessons learned, key success factors, and practices worth replicating.

Collectively, the case studies reflect the breadth of AI adoption in manufacturing, spanning sectors from steel production to automotive to healthcare. Examples include real-time object tracking in steel production [128], worker-led AI development at Toyota [134], fatigue monitoring in European inspection lines [133], and generative design for agile pandemic response [135]. While some emphasize technical integration and sustainability goals, others focus on workforce interaction, ethics, and regulatory adaptation.

3.6.1 Overview of Case Studies

AI implementation in manufacturing is not a once-and-done process. Across the case studies, two variables influenced success more than others: organizational readiness and risk-aligned system design. Firms that matched the complexity of the AI system to their operational maturity, infrastructure, and leadership capacity were more likely to experience successful deployment and sustained value.

Table 6 provides a high-level overview of each case discussed in Section 3.6, categorizing them by region, sector, AI system type (advisory or closed-loop), application focus, and stage of adoption. This overview highlights the breadth of contexts in which AI is being explored and the variations in system maturity and organizational capacity.

With this context, Table 7 examines how stage of adoption correlates with the types of AI used, the key risk domains, and the operational outcomes. Early-stage adopters tend to rely more on advisory AI and human oversight, while mature deployments are more likely to feature autonomous or hybrid systems. However, mature-stage adopters also face greater integration and ethical governance challenges.

This framing provides a structured view of how firms evolve their use of AI over time, and the different risks and capabilities that accompany each phase. Early-stage adopters typically face challenges in data quality, trust, and system alignment. In contrast, while more technically capable, mature users face challenges related to psychosocial, ethical, and strategic governance issues.

As adoption advances, the prioritization of standardization also shifts from establishing basic data quality and interoperability at early stages to embedding lifecycle assurance, transparency, and psychosocial safety in mature deployments. This progression underscores the idea that standardization must evolve alongside system maturity, guiding firms toward increasingly accountable and human-centred AI practices.

Table 6: Summary of Selected AI Adoption Case Studies.

ID	Ref.	Region	Sector	AI System Type	Focus Area	Stage of Adoption
1	[128]	Canada	Steel manufacturing	Closed-loop	Predictive maintenance	Early stage
2	[129]	Canada	SME manufacturing	Advisory	Industry 4.0 tools	Early stage
3	[130]	Canada	Manufacturing	Advisory	Simulation modelling	Early stage
4	[131]	Multinational	Cross-sector	Advisory	Ethics and human rights	Early stage
5	[132]	Multinational	Manufacturing	Advisory	Sustainability	Mature
6	[133]	Europe	Manufacturing	Closed-loop	Fatigue prediction	Early stage
7	[56]	India	Manufacturing	Closed-loop	TAM-TOE framework	Early stage
8	[134]	Multinational	Automotive manufacturing	Closed-loop	Process optimization	Mature
9	[135]	Multinational	Additive manufacturing	Advisory	Generative design	Mature
10	[136]	Multinational	Additive manufacturing	Advisory	Material selection	Mature
11	[137]	Multinational	Aircraft manufacturing	Advisory	Defect detection Predictive maintenance	Mature
12	[138]	Europe	Satellite manufacturing	Closed-loop	Automated design	Mature
13	[139]	Multinational	Pharmaceutical manufacturing	Closed-loop	Machine learning	Early stage
14	[140]	Multinational	Manufacturing	Advisory	Trends in Industry 4.0	Mid-stage

Table 7: Evolution of AI Risk and Outcomes

Stage of Adoption	AI Application Types	Risk Domains Touched	Notable Outcomes
Early	Simulation Predictive analytics Fatigue detection	Workforce adaptation Data quality Strategic alignment	Improved planning Reduced fatigue Foundational AI awareness
Mid	Trend synthesis ESG alignment	Regulatory fragmentation Digital maturity gaps	Identification of cross-cutting gaps and convergence opportunities
Mature	Closed-loop control Generative design AI/machine learning optimization	Psychosocial risk Human-AI symbiosis Ethics-by-design	Scalability Energy/resource gains Enhanced decision-making

Section 3.6.2 analyzes the risks and challenges encountered across the case studies, using a governance-informed lens to identify recurring barriers to AI success in manufacturing environments.

3.6.2 Risks and Challenges Encountered

While the promise of AI in manufacturing is substantial, there are several risks and challenges to successful implementation. The case studies examined in this report revealed a recurring set of risks that are contingent on sectoral context, system complexity, and organizational maturity. These risks span infrastructure, workforce dynamics, leadership alignment, ethical governance, and systemic readiness. They also surface at different phases of the AI system lifecycle, from design and development to deployment and post-implementation monitoring.

This section organizes the identified risks into five primary governance domains: technical, operational, psychosocial, strategic, and ethical. Each domain touches distinct lifecycle stages and offers insight into how specific types of risk can derail adoption or expose deeper gaps in organizational and ecosystem preparedness. Importantly, these risks are not discrete; they often compound one another, making integrated risk governance a necessary condition for responsible AI use in manufacturing.

Table 8 summarizes the five domains and maps each to illustrative case studies, lifecycle phases, and governance insights.

Sections 3.6.2.1 through 3.6.2.6 analyze the five risk domains, along with systemic risks that emerged at the ecosystem level, in the context of the relevant case studies.

Table 8: Case Studies by Primary Risk Domain.

Primary Risk Domain/Cases	AI Applications	Key Sectors	Lifecycle Phases	Risk Governance Insight
Technical [128], [130], [136], [137]	Object tracking Simulation Fuzzy decision systems	Steel Aerospace Additive manufacturing	Model development Validation Integration	Underscores the need for robust test protocols, model assurance, and validation frameworks
Operational [129], [132], [134], [138]	Lean transformation Scheduling Hybrid AI platforms	SMEs Automotive Satellite	Deployment Change management	Highlights misalignment with existing systems, infrastructure strain, and workflow adaptation
Psychosocial [131], [133]	Human-in-the-loop AI Fatigue prediction	Robotics Visual inspection	Deployment Post-Implementation	Brings attention to job stress, cognitive overload, emotional response, and change fatigue
Strategic [56], [139], [140]	Readiness assessment Machine learning for supply chain Policy synthesis	Manufacturing Pharmaceutical Global	System design Strategy alignment	Emphasizes gaps in leadership coherence, long-term planning, and regulatory understanding
Ethical [131], [135]	Ethics-by-design Generative design with human-AI symbiosis	Robotics Cross-sector	Model design Deployment Post-use monitoring	Surfaces concerns about bias, fairness, surveillance, and worker autonomy

3.6.2.1 Technical Risks: Gaps in Validation, Reliability, and Model Fit

Technical risks emerged as some of the most visible and disruptive challenges in AI implementation across manufacturing environments, particularly during the design, development, and early deployment phases. In these stages, issues such as inadequate testing protocols, model drift, and system misalignment frequently resulted in performance degradation or operational setbacks.

In the study from the Canadian steel sector, the use of YOLOv3 and DeepSORT for object tracking within crane operations demonstrated potential for improving material flow and safety [128]. However, the system's accuracy was highly sensitive to misaligned camera feeds and incomplete annotations, revealing that perception systems are only as reliable as their data integration infrastructure. Similarly, Longo et al. [130] reported on the use of simulation-based planning tools in complex production settings, where minor errors in model assumptions or temporal granularity produced misleading recommendations. These cases underline the critical need for robust test environments, sandbox simulations, and model validation protocols as prerequisites for real-time deployment.

The study in aerospace manufacturing found that AI-driven defect detection models struggled to generalize across product batches due to insufficient training diversity and regulatory constraints on data augmentation [137]. This exposed the tension between system robustness and certification requirements, especially in safety-critical environments. Additive manufacturing firms faced similar challenges when fuzzy logic systems for generative material optimization delivered unpredictable outcomes when integrated with legacy firmware, suggesting that black box optimization methods must be grounded in explainable, testable frameworks before being released into production [136].

Together, these four cases highlight a common thread: technical risk in AI is not only a question of algorithmic sophistication but also of lifecycle readiness. Models that perform well in controlled experiments may fail in live environments without lifecycle-aware validation, integration checks, and reliability safeguards.

3.6.2.2 Operational Risks: Infrastructure Misalignment and Change Management Barriers

Operational risks were primarily observed during the deployment and early scaling phases, particularly in contexts where new AI systems had to coexist with legacy workflows, strained infrastructure, or insufficient change management planning. These risks often manifested as integration failures, productivity disruptions, or low system uptake among frontline staff.

In the study on Canadian SMEs, attempts to implement lean scheduling and simulation tools encountered fragmented digital environments with limited interoperability [129]. Production lines lacked centralized data systems, requiring firms to invest in costly middleware to establish basic AI operability, with one case reporting that firms deploying AI-based optimization tools struggled to harmonize data across distributed production cells, leading to inconsistent outputs, worker confusion, and retraining cycles that delayed overall rollout [129], [132].

In the automotive sector, early attempts to introduce hybrid AI platforms at Toyota clashed with linear production planning methods [134]. Successful implementation eventually required the decentralization of model building to the shop floor, a shift that improved adoption but highlights how top-down deployment strategies often overlook operational nuance.

Satellite manufacturers in Europe faced similar challenges. Despite high digital maturity, the introduction of AI-enhanced generative design required extensive retraining of design engineers and a reorganization of product development cycles [138]. Even in well-resourced environments, operational risk persists when AI-driven processes demand new organizational rhythms that conflict with established norms.

These findings reinforce the importance of adaptive infrastructure planning, participatory rollout strategies, and phased deployment architectures. Without these elements, operational risk becomes a limiting factor, not just for implementation but for long-term system evolution and workforce alignment.



"Psychosocial risks were prevalent in the deployment and post-implementation stages, especially when AI altered job roles or monitoring practices."

3.6.2.3 Psychosocial Risks: Human Response and Sociotechnical Misalignment

Psychosocial risks were prevalent in the deployment and post-implementation stages, especially when AI altered job roles or monitoring practices. These risks included job stress, cognitive overload, and emotional fatigue.

Fatigue monitoring systems designed to improve worker safety in European inspection lines were perceived as surveillance tools, generating anxiety and mistrust among employees [133]. Similarly, in robotics deployments, poorly communicated human-in-the-loop designs resulted in confusion over accountability and authority [131].

These cases show that technological functionality does not equate to psychological acceptability. Without clear communication, inclusive design, and ongoing support, AI systems risk undermining the workforce they aim to assist.

3.6.2.4 Strategic Risks: Readiness, Leadership, and Policy Fit

Strategic risks emerged during the system design and strategy alignment phases, particularly in contexts where leadership buy-in, internal coherence, or regulatory foresight were lacking. These risks were especially pronounced in early-stage firms navigating uncertain return on investment, fragmented priorities, or evolving policy landscapes.

In India and Canada, several manufacturers conducting AI readiness assessments reported stalled implementation due to unclear value propositions, competing organizational agendas, and insufficient leadership alignment [56], [139]. Even in cases where AI tools demonstrated technical viability, such as supply chain prediction or pharmaceutical production, deployment was delayed by ambiguity around compliance responsibilities or uncertainty about how AI systems fit within broader operational goals [140].

These examples illustrate that technical feasibility alone is not sufficient for effective AI adoption; it requires leadership commitment, integrated policy interpretation, and clear long-term strategic framing. Without these, AI risks becoming a fragmented or underleveraged initiative rather than a transformative capability embedded across business functions.

3.6.2.5 Ethical Risks: Surveillance, Fairness, and Inclusive Design

Ethical risks were identified throughout the model design, deployment, and post-use monitoring phases, especially in applications that interfaced directly with human roles, decisions, or values. Key issues included lack of stakeholder inclusion, fairness concerns, transparency deficits, and anxiety about surveillance.

In the additive manufacturing sector, engineers initially resisted generative design tools, expressing discomfort with algorithmic outputs that appeared to override professional judgment or creative input [135]. In robotics

and human-in-the-loop systems, transparency and accountability were strained by a lack of ethical co-design, leaving frontline workers unclear about system logic and decision authority [131]. Furthermore, firms that implemented AI in sustainability or governance contexts encountered backlash when models embedded implicit trade-offs or failed to represent the full range of relevant perspectives [131], [135].

These cases emphasize that ethics cannot be retrofitted. Fairness, trust, and legitimacy must be embedded from the outset through participatory design, explainable systems, and governance models that reflect diverse user needs. Without these, AI risks compounding existing power imbalances and value misalignments.

3.6.2.6 Systemic Risks: Fragmentation, Funding, and Infrastructure Gaps

Systemic risks emerged at the ecosystem level, often intersecting with organizational vulnerabilities but extending beyond the control of individual firms. These included structural issues, such as skills shortages, infrastructure fragmentation, inconsistent funding access, and gaps in standards and interoperability frameworks, particularly in early-stage environments.

Canadian SMEs repeatedly cited the lack of internal AI expertise, weak data infrastructure, and difficulty accessing national innovation supports as barriers to experimentation and scale [129], [132], [139]. Even when firms demonstrated initiative, they faced bottlenecks in integrating legacy systems, aligning with external standards, or sustaining cross-departmental implementation. In contrast, firms operating in jurisdictions with stronger national coordination and interoperability protocols reported fewer scaling constraints [134].

These findings point to a layered governance challenge, that is, AI adoption is not simply a firm-level decision, but a function of broader ecosystem health. Without reliable access to funding, shared infrastructure, and standardization pathways, many manufacturers, especially SMEs, remain stuck in pilot phases or abandon AI projects altogether. Closing these systemic gaps will require coordinated policy, testbed platforms, and modular innovation supports that reduce risk and lower the barrier to entry.

Table 9: Summary of Lessons Learned from the Case Studies.

Lesson	Summary	Representative Cases
Phased Deployment	**Start small, learn fast, and scale smart.** Used across all adoption stages for managing risk and enabling learning.	[128], [129], [130], [132], [133], [134], [136], [137], [56]
Data Maturity	**Data is the foundation, not the add-on.** Clean, structured data and interoperable systems differentiate successful from stalled projects.	[128], [129], [130], [132], [136], [137], [56]
Leadership Alignment	**Leadership must go beyond buy-in.** Cross-functional, metrics-aligned leadership is essential for implementation success.	[129], [132], [134], [135], [139]
Design for Flexibility	**Flexibility is an insurance policy for innovation.** Simulation and modular systems enable agility, resilience, and incremental growth.	[129], [130], [132], [135], [137], [138]
Ethical Design	**Ethics is an operational imperative.** Ethical foresight improves adoption, trust, and alignment in human-facing applications.	[131], [133], [135], [56], [140]
Sustainability as Strategy	**Sustainability is a performance benchmark.** AI tied to sustainability delivers both operational and strategic value.	[132], [135], [138], [139], [140]

3.6.3 Lessons to Learn and Practices to Replicate

Across the 14 case studies, several key themes emerged that characterized successful AI adoption in manufacturing environments. These lessons offer strategic and practical insights for firms aiming to integrate AI systems in ways that are effective, scalable, and aligned with broader business and societal goals. The most impactful implementations balanced technical innovation with human integration, organizational readiness, and sustainability consciousness. Notably, several themes exhibited variation based on region, sector, application type, and stage of adoption, reflecting the diverse maturity levels and contextual drivers shaping AI adoption across the global manufacturing landscape. Table 9 summarizes the lessons learned, which are discussed in more detail in sections 3.6.3.1 through 3.6.3.7.

3.6.3.1 Lesson 1: Start Small, Learn Fast, and Scale Smart

Across all sectors, phased deployment emerged as a defining feature of successful AI projects. In early-stage deployments, Canadian SMEs applied simulation modelling and predictive maintenance in narrow contexts, such as crane operations or production scheduling, allowing for quick iteration and organizational buy-in [128], [129], [130]. Other firms continued this modular approach even at maturity, piloting AI components before full-scale deployment [132], [137]. At Toyota, workers were empowered to trial machine learning tools on-site, using small-scale experimentation to accelerate learning and reduce friction [134]. This approach managed operational risks while developing digital skills over time. SMEs in Canada and India used simulation tools to test production adjustments before scaling [129], [130], [56]. Aerospace and automotive firms applied modular deployment to maintain compliance and avoid downtime during system upgrades [133], [136].

Practice to replicate: *Design for iteration, not perfection.*

3.6.3.2 Lesson 2: Data Is the Foundation, Not the Add-On

Projects with poor data quality, inaccessible systems, or fragmented pipelines struggled to get off the ground. In some cases, AI deployments were slowed or paused to allow time for data restructuring and cleaning [128], [130]. Another case demonstrated that scalable success in sustainability and predictive systems required interoperable databases and reliable real-time inputs [132]. Meanwhile, other cases underscored the need for robust metadata and version control to support model accuracy and traceability [136], [137]. Even policy-aligned firms acknowledged that without baseline data governance, AI readiness remained theoretical [56]. Data readiness determined rollout success in steel manufacturing, where real-time visual tracking systems were only possible due to robust, synchronized data streams [128]. Firms with fragmented systems delayed adoption or paused implementation altogether to restructure datasets [129], [56].

Practice to replicate: *Invest in data maturity before model sophistication.*

3.6.3.3 Lesson 3: Leadership Must Go Beyond Buy-In

Technical readiness alone was insufficient when leadership alignment was weak. Several case studies demonstrated that organizational transformation hinged on leadership that understood AI as a cross-functional strategy and not just a tech upgrade [129], [134], [135]. Projects floundered when executives failed to coordinate infrastructure, workforce, and ethical priorities. In contrast, strategic coherence in allowed AI to align with sustainability and efficiency goals [132]. Another case revealed how misalignment between leadership priorities and data maturity can lead to AI stagnation, while successful firms embed AI within organizational decision-making from the outset [139]. Toyota's approach empowered frontline workers to co-develop machine learning tools, demonstrating how aligned leadership and worker empowerment can coexist [134]. Firms that

tied AI to measurable goals, such as emissions reduction or return on investment, secured executive sponsorship and sustained resources [132], [139].

Practice to replicate: *Align AI with organizational strategy and executive ownership.*

3.6.3.4 Lesson 4: Flexibility is an Insurance Policy for Innovation

In volatile environments, adaptability proved to be a core advantage. Several case studies featured modular systems and simulation tools that enabled firms to validate changes, optimize processes, and pivot rapidly without large-scale overhauls [129], [130], [138]. Other cases demonstrated how additive manufacturing systems were reconfigured during pandemic disruptions using AI-driven generative design [137], and how design flexibility supported innovation in health and safety equipment [135]. Additive manufacturing firms used modular tools and generative design to pivot during COVID-19, rapidly producing essential goods [135]. Canadian SMEs leveraged flexible workflows to improve delivery metrics and respond to custom demands [129], [130]. Across all these examples, firms viewed flexibility as a strategic asset embedded into their AI systems.

Practice to replicate: *Design for modularity and simulation.*

3.6.3.5 Lesson 5: Ethics is an Operational Imperative

Ethical risk was present in nearly all human-facing applications, whether acknowledged or not. One case focused on human-robot collaboration and emphasized the need for ethical co-design frameworks [131]. One described how fatigue prediction tools triggered worker anxiety due to perceived surveillance [133], while another found that participatory AI development gave workers a sense of control and dignity [135]. In cross-border governance cases, unresolved questions around fairness, stakeholder inclusion, and interpretability slowed adoption or undermined trust [56], [140]. The clearest successes embedded ethical foresight from the start. For example, worker-centred systems, such as fatigue monitoring with oversight [133] and participatory human-robot collaboration platforms [131], minimized resistance and stress, while Toyota's democratized AI design gave factory workers ownership over machine learning models [134], reinforcing trust and engagement.

Practice to replicate: *Build AI around people, not instead of them.*

3.6.3.6 Lesson 6: Sustainability is a Performance Benchmark

Firms that positioned AI as a tool for environmental and social performance, not just productivity, were better equipped for long-term competitiveness. In several case studies, AI helped optimize resource use, align with ESG targets, and reduce emissions [132], [135], [139]. One case used modular design to support sustainability in satellite manufacturing [138], while another showed how global AI governance is increasingly tied to sustainability benchmarks [140]. AI systems were used to optimize energy, reduce emissions, and align with ESG mandates in pharmaceutical, satellite, and multi-national deployments [132], [138], [140]. Generative design helped to reduce waste and improve product recyclability in additive manufacturing [135]. These examples confirm that sustainability is a primary driver of investment, compliance, and innovation in the next phase of industrial transformation.

Practice to replicate: *Use AI to align operations with ESG and long-term goals.*

3.6.3.7 Summary of Lessons Across Contexts

These six lessons and associated practices illustrate that while AI implementation varies in complexity and context, certain foundations remain universal: start small, lead intentionally, build on quality data, stay flexible, honour ethics, and aim for sustainability. For manufacturers, this means embedding AI into the core of how they operate, not just as a tool but as a strategy for transformation. For policymakers, these lessons underscore the need to support standards, infrastructure, and governance systems that promote safe, inclusive, and future-ready AI adoption across the sector.

3.7 Risks Associated with AI Adoption

This section applies a risk management model to analyze risks associated with AI adoption in the Canadian manufacturing sector. Following ISO 31000 [127], ISO/IEC 22989 [69], and ISO/IEC 23894 [53], risks are classified by both lifecycle phase (e.g., design, training, deployment, post-deployment) and organizational domain (e.g., data governance, safety, leadership). This dual mapping highlights when risks emerge and where they are managed, providing a structured basis for targeted mitigation.

Risks were identified by consolidating the literature review, the 14 case studies, the regulatory and standards analysis, and the 20 interviews with AI developers, manufacturing leaders, and policy specialists.

By aligning risk categories with lifecycle phases and organizational responsibilities, the framework emphasizes that risks are interdependent. For example, technical errors often reflect upstream data gaps, and psychosocial hazards can amplify operational and strategic vulnerabilities. This integrated view provides the foundation for the detailed risk analyses presented in Section 3.7.2 and the mitigation strategies in discussed in Section 4.

3.7.1 Risks Identification and Classification

Risks were classified through a two-step mapping process consistent with ISO/IEC 23894 [53]. First, each risk was situated within the lifecycle stage where it most often emerges, and then it was linked to the governance domain responsible for its management (e.g., system design, operational controls, data governance, psychosocial safety). This approach reflects the need for lifecycle-integrated and cross-functional risk management.

Table 10 presents the identified risks across eight major categories: technical, data, cybersecurity, operational, human-machine interaction, ethical/legal, organizational/strategic, and psychosocial. The table illustrates how vulnerabilities cascade across lifecycle stages and functions, emphasizing the importance of coordinated, multidisciplinary approaches to risk management.



Figures 3 through 5 visualize the distribution of risk observations across sources, lifecycle phases, and governance domains. This evidence-based mapping highlights not only the concentration of risk types but also the gaps in formal standards and regulatory treatment, particularly around relational, psychosocial, and post-deployment risks.

Figure 3 illustrates the strength of the interviews and the literature review in identifying emergent and experiential risks, such as psychosocial hazards and deployment-level operational failures. Regulatory documents and case studies, by contrast, offer clearer insight into structural, legal, and technical controls, although they often overlook subjective or workforce-level impacts.

Figure 4 reveals a concentration of the identified risks during the deployment phase, with substantial contributions across all data sources. This suggests that deployment is the most vulnerable and visible point of failure in AI integration. In contrast, post-deployment risks are significantly underrepresented, indicating a potential blind spot in research and governance around system monitoring, drift, and long-term psychosocial effects. Interviews offered a more even distribution of risks across design, deployment, and operation, emphasizing the complexity of real-world implementation.

Table 10: Functional and Governance Mapping of AI Risk Classes.

Risk Class	Examples	Primary Governance Domain	Functional Area
Technical	Model errors Automation failure Silent failure	System design and testing	Engineering Health, safety and environment Production Maintenance
Data	Training bias Poor metadata Privacy breaches	Data governance IT	Production Supply chain Health, safety and environment Cybersecurity
Cybersecurity	Unauthorized access Adversarial attacks	Information security Vendor risk	Cybersecurity Legal and compliance
Operational	Pilot drop-off Over-engineering Misalignment	Operations Project management	Production Health, safety and environment Supply chain Strategy
Human-Machine Interaction	Misinterpretation Deskilling Loss of agency	Training Human factors User experience	HR & Workforce, Production, Health, safety and environment
Ethical/Legal	Algorithmic bias Surveillance Unclear consent	Legal affairs Compliance Labour relations	HR Legal Customer experience Procurement
Organizational/ Strategic	Skills gaps Vendor lock-in Siloed governance	Leadership Strategic planning	All functions (especially cross-cutting roles)
Psychosocial	Monitoring stress Job ambiguity Relational erosion	Occupational health Corporate responsibility	HR Health, safety and environment Training and knowledge management

Figure 3: Risk observations by category and source. Count represents the number of distinct risk types identified within each source (multiple mentions of the same risk within one source are not double counted).

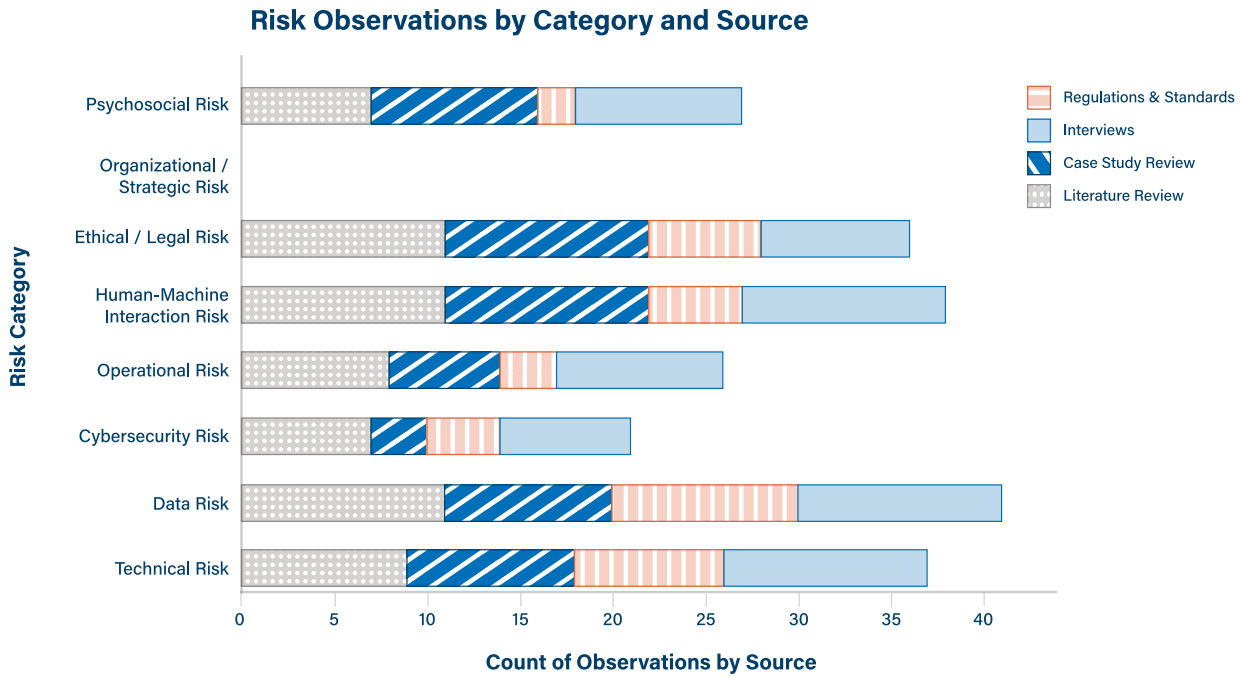


Figure 4: Distribution of AI risks by lifecycle category.

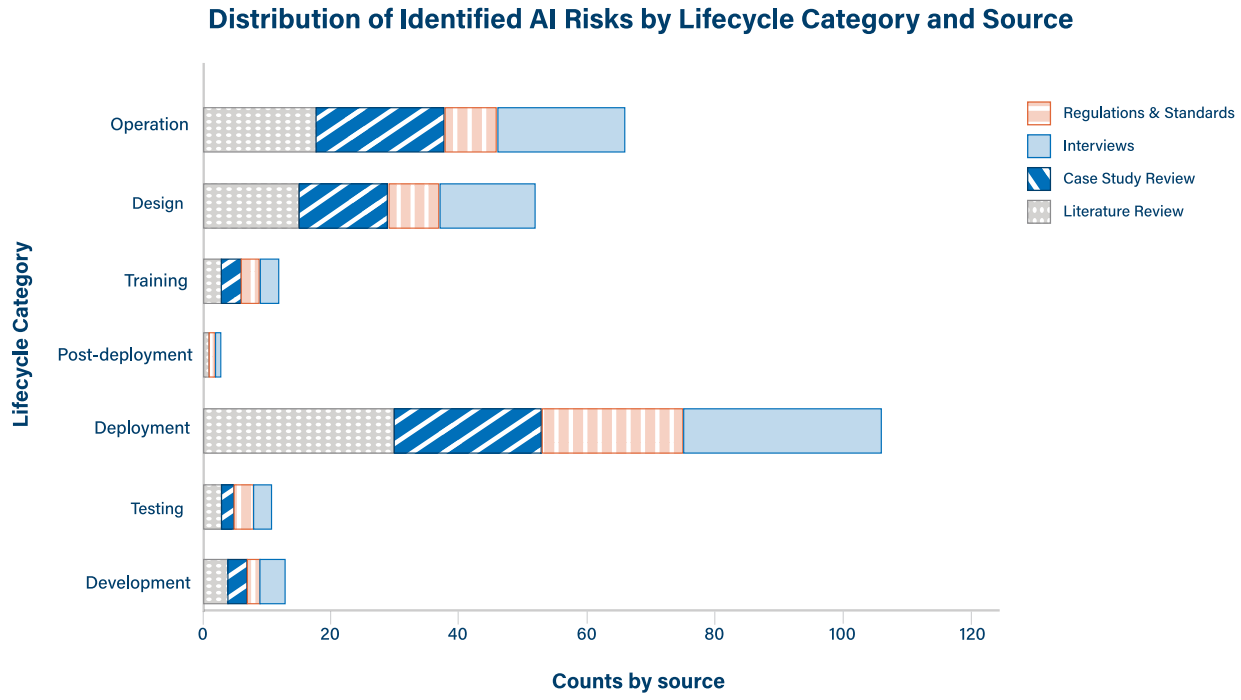


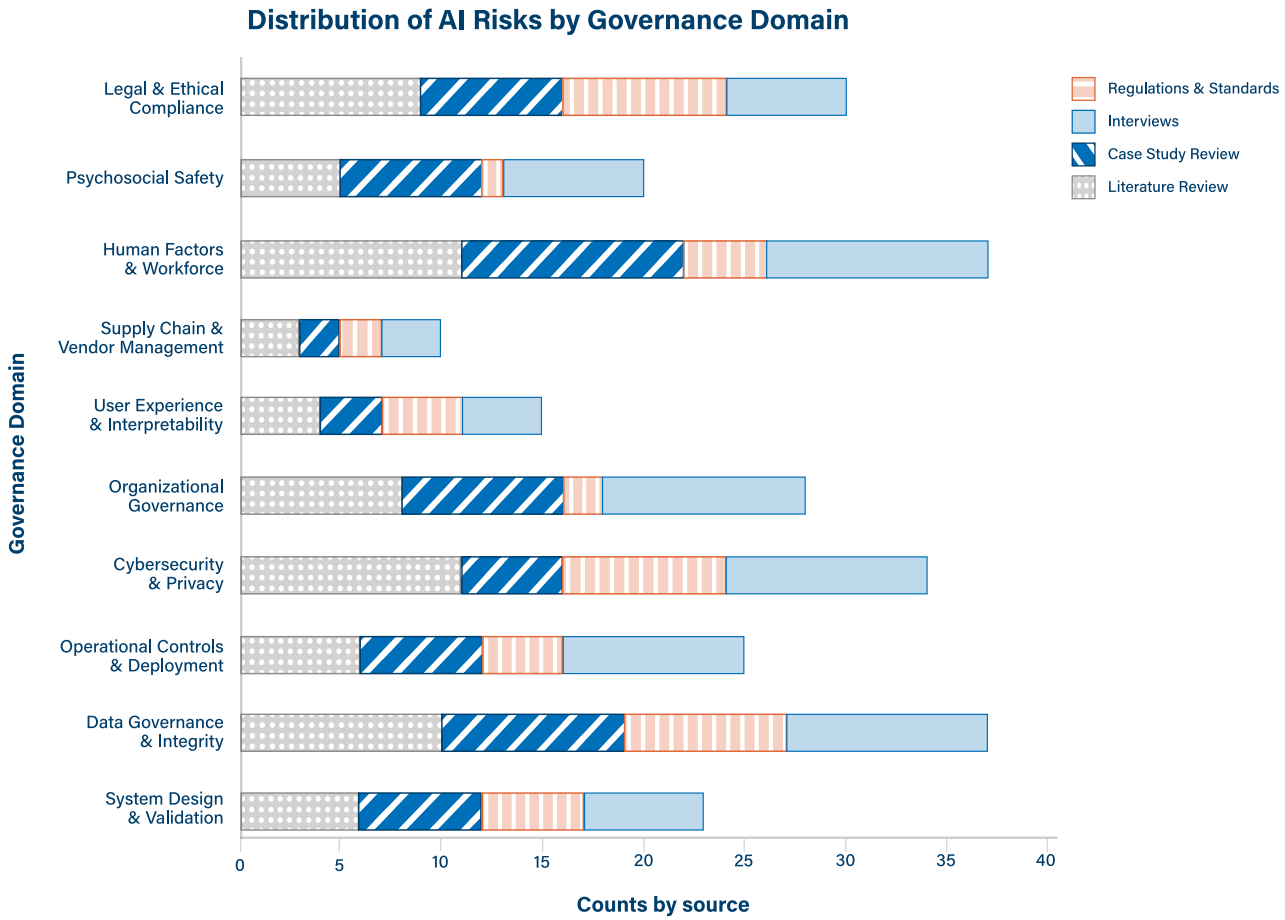
Figure 5 shows that the most frequently cited governance domains were human factors and workforce and data governance and integrity. These categories reflect both the technical dependence of AI systems on quality data and the social complexity of workplace integration. Cybersecurity and privacy, as well as operational controls and deployment, were also strongly represented. However, psychosocial safety emerged almost exclusively in the interviews, revealing a significant governance blind spot in both standards and regulatory frameworks.

This fragmentation across sources reflects a key insight from AI risk guidance: effective governance must include both formal compliance tools and qualitative, workforce-informed indicators. The absence of relational and emotional risks in formal governance structures, despite their frequent appearance in implementation data, underscores the need for more comprehensive, human-centred approaches to AI safety and sustainability.

3.7.2 Assessment of Key Risks by Category

To extend beyond identification, this section applies CSA-aligned methodologies (ISO 31000 [127], ISO/IEC 23894 [53]) to interpret how and where AI-related risks affect Canadian manufacturers. Risks were evaluated for likelihood, severity, lifecycle phase, and governance domain, with triangulation across literature, case

Figure 5: Distribution of AI risks by governance domain.



studies, and interviews. The analysis shows that risks rarely exist in isolation, but instead intersect across technical, organizational, and psychosocial domains.

3.7.2.1 Technical Risks

Technical risks, such as automation failure, false negatives, inadequate validation, and post-deployment drift, were consistently identified across the literature, case studies, and interviews as the most universally recognized hazards [1]. These risks directly disrupt production or safety and are foundational to AI system integrity. Standards such as ISO/IEC 42001 [54] emphasize lifecycle-aligned practices (e.g., validation and monitoring) but evidence shows that they often remain abstract in application. Manufacturers are told what to do but not how to do it, leaving SMEs in particular to interpret requirements without practical roadmaps [36], [56].

Case studies revealed predictive maintenance tools that underperformed, not because the algorithms were inherently flawed but because pre-deployment validation and stress testing were inconsistent across firms [20]. Similarly, interviews described system failures that emerged months after deployment, when monitoring processes failed to detect model drift or data quality issues. While manufacturers attempt to establish monitoring mechanisms, the absence of common indicators or sector-specific benchmarks leads to ad hoc approaches and inconsistent reliability.

Another challenge is that technical risk rarely appears in isolation. Bridging organizational gaps to align safety, data, and technical reliability remains particularly difficult in manufacturing contexts, where functions such as operations, IT, and OH&S often operate in silos [6], [28]. Without integrated approaches, technical failures are frequently symptoms of cross-domain weaknesses, such as poor vendor oversight or fragmented data governance.

These findings confirm that technical risks are both central and interdependent, highlighting that system breakdowns often reflect broader structural and organizational fragilities rather than isolated technical shortcomings.

Evaluation Summary of Technical Risks

- **Severity:** High; failures may directly disrupt production or safety.
- **Likelihood:** Medium to High; particularly in early-stage or poorly integrated deployments.
- **Lifecycle:** Development → Deployment → Post-deployment.
- **Domains:** System Design and Validation; Operational Controls.
- **Priority:** Medium-High; critical for ensuring real-world usability and continuity.

3.7.2.2 Data Risks

Data risks were also pervasive across all sources, underscoring that the reliability of AI systems depends on the quality, structure, and governance of underlying data [26], [28]. Case studies and interviews repeatedly showed that poor data quality, inconsistent metadata, fragmented infrastructure, and training bias were among the most common barriers to adoption. For Canadian SMEs, legacy enterprise resource planning or supervisory control and data acquisition (SCADA) systems often cannot support the interoperability or real-time analytics that AI requires, creating bottlenecks and undermining trust in outputs [12].

While ISO/IEC 23894 [53] and ISO/IEC 42001 [54] emphasize the importance of risk-based data management and lifecycle monitoring, firms still struggle to operationalize these requirements. Manufacturers are given broad expectations but few sector-specific benchmarks or thresholds for what constitutes sufficient data quality in industrial contexts [56]. This leaves SMEs in particular uncertain about whether their datasets are adequate for safe deployment. The result is uneven adoption, with some firms investing heavily in custom solutions while others rely on ad hoc practices that introduce bias or unreliability.

Lifecycle misalignment can compound data risks. Case studies highlighted silent model failure and drift that went undetected because ongoing validation mechanisms were absent. Interviews echoed these

concerns, with participants noting that "bad data in, bad data out" is a daily reality, particularly in supply chain and quality control applications.

Data sharing and vendor relationships add another layer of complication. SMEs often outsource data preparation or rely on third-party platforms but lack clear guidance on contractual obligations for portability, security, and quality [12]. Without standardized accountability mechanisms, firms remain exposed to risks of vendor lock-in or data misuse.

Data risks include not only technical shortcomings but also structural fragmentation, lack of sectoral benchmarks, and absent lifecycle controls. The evidence confirms that data governance is one of the most critical—and most underdeveloped—foundations for trustworthy AI in manufacturing.

Evaluation Summary of Data Risks

- **Severity:** High; poor data undermines model accuracy, safety, and compliance.
- **Likelihood:** High; especially among SMEs with limited infrastructure.
- **Lifecycle:** Design → Training → Deployment.
- **Domains:** Data Governance and Integrity; Cybersecurity.
- **Priority:** High; foundational to system reliability, traceability, and regulatory compliance.

3.7.2.3 Cybersecurity Risks

Cybersecurity emerged as a critical concern across the literature, policy frameworks, and interviews, although the case studies revealed that, in practice, it often receives less operational attention. Risks such as adversarial manipulation, data poisoning, unauthorized access, and unprotected APIs were consistently identified as potential threats [53], [62]. However, many manufacturing firms, particularly SMEs, lack the in-house expertise to fully assess or respond to AI-specific vulnerabilities [12].

While ISO/IEC 27001 and the ISA/IEC 62443 series provide strong foundations for information and operational technology security, they are not tailored to AI-specific attack vectors, such as adversarial machine learning or LLM-enabled leakage [53], [62]. Interviews highlighted how these gaps manifest: firms relying on cloud platforms or vendor APIs reported unease about whether they had adequate visibility into third-party practices, leaving them vulnerable to breaches or intellectual property theft.

Cybersecurity threats in AI are further complicated by their convergence with safety. Closed-loop systems, where AI outputs directly influence physical processes such as robotics or predictive maintenance, create scenarios where security lapses could translate directly into safety hazards [117]. In these cases, traditional separation of IT security and OH&S frameworks proves inadequate.

Supply chain dependence was another consistently identified theme. Manufacturers frequently adopt third-party AI solutions but lack mechanisms to verify or enforce vendor security standards [12]. This dependency creates cascading risks, as vulnerabilities in one link of the supply chain can propagate across multiple firms. Case studies noted how limited cross-vendor security verification left organizations exposed to breaches that originated outside their direct control.

Overall, while strong cybersecurity frameworks exist, their general purpose orientation and lack of AI-specific provisions leave manufacturers underprepared for emerging threats. The evidence suggests that without integrated safety-security protocols and vendor accountability mechanisms, AI adoption in Canadian manufacturing will remain exposed to critical vulnerabilities.

Evaluation Summary of Cybersecurity Risks

- **Severity:** Very High; breaches may expose proprietary intellectual property or trigger safety-critical failures.
- **Likelihood:** Medium; elevated in under-protected or legacy environments.
- **Lifecycle:** Deployment → Post-deployment.
- **Domains:** Cybersecurity and Privacy; Operational Safety.
- **Priority:** High; essential for safeguarding safety, intellectual property, and system trust.



3.7.2.4 Operational Risks

Operational risks were heavily discussed in the interviews and moderately addressed in policy frameworks and the literature. The risks include misaligned pilots, inadequate contingency planning, over-engineered systems, and lack of internal process ownership [6], [56]. In real-world implementations, such risks often materialized when AI tools were introduced without sufficient cross-functional coordination or change management [12]. Case studies revealed how poor alignment between system capabilities and business needs can lead to expensive underperformance [28]. Interviews reinforced this point, with several respondents noting that AI pilots "died quietly" due to a lack of internal ownership or misfit with organizational workflows [56]. While ISO 31000 advises close attention to operational context, the findings suggest that execution gaps remain significant [127].

While ISO/IEC 5338 [107] and ISO/IEC 42001 [54] provide manufacturers with lifecycle guidance, they remain high-level and do not explain how to move from pilot project to scaled deployment in practice Interviews underscored that pilots are often developed in IT silos and fail to integrate with operations, HR, or compliance teams, leaving firms without clear ownership or accountability structures [56]. Few standards address contingency planning, so firms rarely establish human-in-the-loop fallback procedures or continuity protocols for when AI tools fail mid-operation [6].

Change management challenges further amplify operational risks, particularly when workforce readiness and psychosocial safety are overlooked [57], [59], [61]. For SMEs, the absence of accessible implementation pathways exacerbates these issues, as many lack the resources to build formalized cross-functional alignment or detailed scaling roadmaps [12], [37].

Operational risks represent the "messy middle" of AI adoption, where failures occur not because AI systems lack technical capability but because firms lack structured supports for scaling, cross-functional integration, and contingency planning [6], [12], [56]. Without stronger organizational processes that connect technical pilots to operational reality, Canadian manufacturers will continue to experience stalled projects, stranded assets, and unrealized returns on AI investment [37].

Evaluation Summary of Operational Risks:

- **Severity:** Moderate to High; can cause inefficiency, rework, or failure to scale.
- **Likelihood:** High; frequent in pilot settings without integrated change management.

- **Lifecycle:** Deployment → Operation.
- **Domains:** Operational Controls; Organizational Governance.
- **Priority:** Medium-High; critical for ensuring real-world usability and continuity.

3.7.2.5 Human-Machine Interaction Risks

Human-machine interaction risks, including cognitive overload, deskilling, misinterpretation of outputs, and loss of role identity, were underemphasized in the regulations but highly visible in the case studies, literature, and interviews [11], [12]. These risks align closely with ISO 31000 principles, which urge attention to cultural and human factors [127]. The findings indicate that many firms struggle to anticipate or mitigate the emotional and psychological effects of automation on workers [56]. Several interviewees described "silent resistance" among staff when AI systems displaced tacit knowledge or undermined job meaning [12], [56].

Standards such as ISO/IEC 42001 [54] call for attention to human factors, though they provide limited guidance on usability testing methods that are adapted to manufacturing. This leaves firms without clear processes to evaluate operator workload, error pathways, or the interpretability of AI outputs [20]. Case studies highlighted how operators can misinterpret AI-generated predictions, which created downstream inefficiencies and trust issues in production [28]. Interviews further revealed that when AI replaced manual judgment, tacit worker knowledge was often disregarded, eroding workforce confidence and cohesion [56].

The psychosocial dimension of human-machine interaction is also important. Workers reported stress from opaque decision-making, monitoring fatigue, and fears of replacement [57], [59], [60]. Current standards on explainability, such as ISO/IEC TR 24027 [118], remain abstract and are not widely applied in manufacturing contexts. Without sector-specific guidance on transparency and explainability, frontline workers have little recourse to challenge or override AI outputs, intensifying anxiety and undermining trust [20], [56].

Human-machine interaction risks demonstrate that technical success is not sufficient for AI adoption. Without usable interfaces, mechanisms for tacit knowledge preservation, and safeguards for worker agency, AI deployments risk social failure even when they perform well technically [12], [20], [56].

Evaluation Summary of Human-Machine Interaction Risks:

- **Severity:** High; affects worker safety, confidence, and operational interpretation.
- **Likelihood:** High; consistently surfaced in user-facing deployments.
- **Lifecycle:** Deployment → Operation.
- **Domains:** User Experience and Interpretability; Human Factors and Workforce.
- **Priority:** High; systems must function in harmony with human judgment and agency.

3.7.2.6 Ethical and Legal Risks

Ethical and legal risks, such as algorithmic bias, surveillance anxiety, lack of transparency, and inadequate consent protocols, were acknowledged across all data sources, although their prioritization and enforceability varied significantly [11], [56]. In both the literature and the interviews, there was concern that AI systems may unintentionally replicate or reinforce systemic inequities, particularly in areas such as recruitment, scheduling, and performance monitoring [63], [64]. Case studies on human-robot collaboration and generative design highlighted resistance rooted in a lack of ethical foresight, where workers questioned the fairness and legitimacy of AI-driven decisions [12], [56].

Canada's current regulatory landscape on AI remains fragmented. While voluntary guidance, such as the Code of Conduct on Generative AI, promotes principles of transparency and accountability, it lacks enforcement power [121]. Privacy protections under PIPEDA, the *Canadian Human Rights Act,* and the *Canada Labour Code* provide indirect coverage, but they do not specify

how consent, explainability, or accountability should be operationalized in AI-enabled workplaces [75], [89], [90]. This creates uncertainty for manufacturers, particularly SMEs, who lack in-house expertise to interpret high-level ethical principles [6], [28].

While standards such as ISO/IEC TR 24027 [118] provide methods for bias assessment and fairness evaluation, they appear to be underused in manufacturing practice and are not always tailored to shop floor contexts . ISO/IEC 42001 [54] emphasizes accountability and oversight roles but leaves firms to interpret how these should be structured internally, which could potentially lead to inconsistency and ambiguity. Interviews revealed that when AI system errors occurred, responsibility often shifted between vendors and employers, with no clear accountability framework in place [12].

Overall, ethical and legal risks underscore that voluntary principles and fragmented protections are insufficient for AI adoption in manufacturing contexts. Without concrete mechanisms for fairness audits, worker consent, and clear accountability, Canadian manufacturers risk social backlash, reputational harm, and non-compliance in international markets [42], [56], [63].

Evaluation Summary of Ethical and Legal Risks:

- **Severity:** High; impacts compliance, reputation, and equity.
- **Likelihood:** Medium; often dependent on specific use cases.
- **Lifecycle:** Design → Deployment.
- **Domains:** Legal and Ethical Compliance; Organizational Governance.
- **Priority:** Medium-High; emergent area with growing regulatory and social importance.

3.7.2.7 Organizational Risks

Organizational risks, such as policy misalignment, skills gaps, vendor lock-in, and strategic short-sightedness, were primarily identified through the interviews and case studies, highlighting systemic weaknesses that can derail AI projects before technical issues even arise [12], [56]. In several cases, SMEs heavily depended on a single "AI champion" within the firm, which creates vulnerability if that individual were to leave or shift focus [28]. This was compounded by fragmented access to public funding programs, with smaller firms reporting difficulty in navigating application processes or meeting eligibility criteria, leaving them under-resourced compared to larger competitors [42].

Cross-functional integration challenges also emerged as a recurring barrier. Case studies revealed that AI pilots often remained siloed within IT departments, failing to secure buy-in from operations, HR, or compliance functions [12]. This siloed approach led to "quiet project deaths," where pilots stalled not due to technical failure but due to a lack of internal ownership and alignment with organizational workflows [56]. Interviews further underscored that SMEs often lacked the capacity to manage cross-domain coordination or establish structured change management processes, leaving adoption efforts fragmented and prone to collapse under competing priorities [6], [28].

While standards such as ISO/IEC 42001 emphasize senior leadership engagement and lifecycle integration, they provide limited practical tools for embedding oversight into day-to-day manufacturing governance [54]. ISO 31000 [127] highlights the importance of integrating risk management into organizational structures, yet case studies demonstrated that manufacturers often treat risk analysis as a compliance exercise rather than an embedded management practice. This left organizations ill-prepared to adapt AI deployments into broader strategic planning, particularly when confronting vendor dependency or shifting international requirements [20].

Overall, organizational risks highlight that AI adoption is as much a question of leadership and structure as it is of technology. Without stronger mechanisms for cross-functional integration, leadership accountability, and SME-accessible supports, Canadian manufacturers could remain vulnerable to stalled projects, vendor dependency, and fragile implementation capacity [12], [28], [42].

Evaluation Summary of Organizational Risks:

- **Severity:** Moderate to High; affects sustainability and long-term value.

- **Likelihood:** High; especially in SMEs and decentralized firms.
- **Lifecycle:** Design → Deployment.
- **Domains:** Organizational Governance; Strategic Planning.
- **Priority:** High; governance maturity is central to successful AI integration.

3.7.2.8 Psychosocial Risks

Psychosocial risks emerged as one of the most underexplored yet consequential risk categories in this report, encompassing technostress, fear of replacement, reduced autonomy, and stigma linked to performance monitoring [56], [59]. These risks were identified predominantly through the interviews and case studies rather than the literature or regulatory documents, suggesting that they remain underacknowledged in formal risk frameworks despite their real-world impact [57]. Workers described anxiety from opaque AI decision-making, stress from constant digital surveillance, and diminished team cohesion when human judgment was displaced by algorithmic processes [12], [60].

Evidence from Canadian workplaces showed that psychosocial strain is not a marginal issue but a recognized occupational hazard, with CAN/CSA-Z1003/BNQ 9700-803 defining psychological health and safety as integral to workplace well-being [58], [61]. However, current applications of these frameworks rarely account for AI-specific stressors, such as algorithmic pressure or the erosion of tacit expertise [56]. Case studies further illustrated that when AI systems sidelined long-term staff without adequate retraining, morale declined and resistance to adoption increased, underscoring the link between psychosocial safety and workforce trust [12].

The literature supported this view, highlighting that psychosocial challenges are amplified in fast-moving, top-down manufacturing cultures where economic imperatives dominate decision-making [36]. Without proactive attention to worker autonomy and inclusion, AI adoption risks exacerbating burnout and disengagement rather than improving performance [59]. Interviews revealed that psychosocial risks were often treated reactively (i.e., addressed only after stress or dissatisfaction became visible) rather than being anticipated during system design or rollout [28].

Psychosocial risks illustrate the human cost of AI when systems are implemented without safeguards for dignity, autonomy, and psychological health. Failure to integrate psychosocial safety into AI adoption strategies risks amplifying existing mental health strains and undermining trust in organizational change at precisely the moment when engagement and inclusion are most critical [57], [59], [60].

Evaluation Summary of Psychosocial Risks:

- **Severity:** High; may lead to disengagement, mental health challenges, and turnover.
- **Likelihood:** Medium to High; underreported but pervasive.
- **Lifecycle:** Operation → Post-deployment.
- **Domains:** Psychosocial Safety; HR; Organizational Learning.
- **Priority:** High; essential for ethical, sustainable AI adoption and workforce trust.

3.7.3 Interconnection of Risks Across Domains

The assessment of key risks by category confirms that risks associated with AI adoption in manufacturing are not discrete but interdependent, often reinforcing each other across technical, organizational, and human domains. For example, technical and data risks frequently cascade into operational disruptions, which in turn erode worker trust and heighten psychosocial strain [56], [57], [59]. Similarly, gaps in explainability or accountability amplify ethical concerns, intensify worker resistance, and weaken the perceived legitimacy of organizational decisions [11], [20], [63].

This interconnected risk landscape highlights that AI adoption cannot be managed through siloed controls. Instead, effective management requires robust organizational systems grounded in lifecycle processes, cross-functional oversight, and mechanisms for continuous learning [53], [54]. Literature and case evidence show that when firms lack these fundamentals, risks compound. Slow uptake of AI [37],

uncertain returns on investment [12], and hesitancy in risk-related decision-making [11] mirror broader structural uncertainties, including a fragmented policy environment [72], [73], inconsistent international policies [95], shifting trade expectations [94], and newly recognized psychosocial hazards [58], [60], [104].

Taken together, these findings point to a single imperative: manufacturers must invest in building capacity for risk management and organizational resilience. Without this systemic foundation, the interconnection of risks will continue to amplify vulnerabilities, undermining both the reliability of AI systems and the sustainability of their integration into Canadian manufacturing.

The risk analysis presented in this section forms the basis for the discussion of thematic findings presented in Section 3.8.

3.8 Discussion of Integrated Thematic Findings

This section presents the most significant cross-cutting findings from the assessment of AI applications in Canadian manufacturing. It synthesizes patterns across the literature, case studies, interviews, and standards to highlight where risks converge, where governance remains insufficient, and where opportunities for coordinated action exist. It also identifies the systemic issues shaping AI adoption in practice, emphasizing that these are not isolated technical problems but layered and interdependent challenges.

The discussion is presented across three dimensions. First, it explores six core challenges that manufacturers face when adopting AI systems, with attention to recurring issues in data governance, lifecycle oversight, organizational coordination, and psychosocial risk. Second, it examines the limitations of current AI governance standards, highlighting concerns about their accessibility, relevance, and practical usability. Finally, it synthesizes these insights into a set of gaps that cut across policy, practice, and infrastructure. Each of these gaps points to an opportunity for more responsible, inclusive, and scalable AI adoption across the manufacturing sector.

3.8.1 Core Findings and Challenges for Manufacturers

The assessment revealed six interlocking challenges affecting AI adoption in Canadian manufacturing, which are illustrated in Figure 6 and discussed in sections 3.8.1.1 through 3.8.1.6. These findings emphasize systemic risk patterns and governance gaps, and reflect the lived realities of manufacturers navigating technical ambition, organizational readiness, and regulatory uncertainty.

3.8.1.1 Lifecycle Governance is Fragmented and Deployment-Oriented

Manufacturers consistently prioritize deployment and operationalization, with minimal attention to early-phase activities, such as data preparation and model validation, or to post-deployment controls, such as drift detection and ethical impact reviews [36], [56]. Case studies confirmed that most AI pilot projects lacked comprehensive feedback loops or monitoring protocols, with failures often discovered only after costly disruptions [20], [28]. Interviews reinforced this gap, showing that SMEs rarely have the resources or expertise to manage iterative lifecycle governance, and few adopt post-implementation performance assessments unless externally mandated [12], [56]. Although ISO/IEC 42001 and ISO/IEC 22989 emphasize lifecycle integrity, they are rarely operationalized, leaving governance uneven and heavily deployment-centric [54], [69].

Impact: This lifecycle imbalance increases vulnerability to silent system failures, scalability limitations, and risk accumulation. Without continuous processes, when governance is treated as a static checkpoint rather than an ongoing practice, manufacturers risk compliance gaps and systemic brittleness [54].

3.8.1.2 Data Governance is a Structural Weakness

Data governance emerged as one of the most consistent challenges to AI adoption. The literature identified poor data quality, inconsistent metadata, and lack of interoperability as root causes of AI system failure [2], [36], [56]. Case studies showed technically sound models failing due to unreliable or non-representative input data, particularly in predictive maintenance and

Figure 6: Challenges of AI adoption in Canadian manufacturing.



quality control applications [20], [28]. Interviewees cited legacy infrastructure, decentralized data practices, and the absence of standardized naming or lineage protocols as barriers that undermined confidence in outputs [12], [37]. Canadian SMEs in particular highlighted the difficulty of integrating AI with outdated enterprise resource planning and SCADA systems, which limited interoperability and real-time analytics [56].

Impact: Without structured data governance, manufacturers face operational setbacks, such as system brittleness, model bias, and limited reproducibility. This undermines auditability, increases integration costs, and restricts cross-facility learning, compounding the risk of fragmented or unreliable AI deployment [26], [28], [56].

3.8.1.3 Psychosocial Risk is Foreseeable but Neglected

Despite inclusion in ISO 45003 and ISO 31000, psychosocial risks remain under-addressed in AI deployments [112], [127]. Interviews and case studies repeatedly identified emotional distress, stress from opaque decision systems, role ambiguity, cognitive overload, and surveillance-related anxiety as workforce impacts [11], [17], [25]. Case studies showed morale declining when AI systems displaced tacit expertise without retraining, while interviews revealed fear of replacement and stigma from AI-generated performance scoring [12], [56], [60].

Impact: Ignoring psychosocial risks erodes trust, increases turnover, and undermines system usability. The relational harms associated with AI systems, such as loss of autonomy, dehumanized feedback, and erosion of team cohesion, can render systems socially unworkable even when technically successful [57], [59].

3.8.1.4 Organizational Silos Undermine AI Adoption Success

AI initiatives are frequently led by isolated champions within IT or operations, with minimal engagement from HR, health and safety, procurement, quality, or executive leadership [6], [56]. Case studies showed that successful AI efforts relied on interdisciplinary teams and co-

developed governance practices, while stalled pilots were often traced to siloed approaches that excluded key functions [20], [28]. The literature pointed to poor enterprise integration as a recurring root cause of adoption failure [36]. Interviews confirmed the same trend, with participants citing a lack of shared language, limited change management capacity, and absent cross-functional accountability as reasons why projects "died quietly" despite technical feasibility [12], [56].

Impact: Siloed governance fragments risk visibility, duplicates effort, and weakens implementation consistency. Without cohesive oversight, manufacturers miss opportunities for knowledge transfer and fail to embed AI systems within actual workflow realities.

3.8.1.5 AI Readiness is Frequently Overestimated

Many firms equated AI readiness with having run a pilot project or possessing basic IT infrastructure, but case studies and interviews exposed deeper misalignments in governance maturity, risk appetite, and long-term strategy [12], [56]. Several pilots failed to scale because firms underestimated the importance of lifecycle planning, data architecture, and trust frameworks [28]. The literature emphasized that true readiness includes these foundations, along with leadership capacity for change and ethical oversight [56], [69], [131]. Interviews further revealed that firms often lacked realistic self-assessments of capacity, leading to rushed deployments, insufficient safeguards, and low return on investment [11], [37].

Impact: Overestimating AI readiness fuels disillusionment, system abandonment, and ethical shortcuts. Without structured readiness assessments, firms risk vendor dependency, burnout, and weakened innovation culture.

3.8.1.6 Frontline Practice and Governance Feedback Loops are Weak

Manufacturers consistently reported feeling disconnected from the development of standards and policies that govern them. Interviewees expressed frustration with "static documents" that lacked contextual relevance and offered little guidance for their operational realities [12], [56]. The literature critiqued the top-down design of many standards, noting that without mechanisms for adaptation they risk becoming symbolic rather than functional [36], [95]. Case studies reinforced this, showing that success was more likely when governance was treated as an adaptive practice responsive to frontline feedback [20], [28]. However, few mechanisms exist to relay implementation realities back to standards bodies or regulators, leaving a persistent gap between policy design and practice [56].

Impact: The absence of bidirectional feedback hampers adaptive governance, breeds compliance fatigue, and limits the evolution of meaningful safeguards. Firms without the resources to translate abstract frameworks into practice are particularly vulnerable to symbolic compliance, undermining both risk management and trust [12].

3.8.2 Challenges Related to Standardization

While the standards review revealed meaningful progress toward codifying lifecycle-oriented approaches to AI risk, the case studies and interviews indicated that their practical utility in Canadian manufacturing remains limited. Instruments such as ISO/IEC 22989 [69], ISO/IEC 23894 [53], and ISO/IEC 42001 [54] articulate principles of risk management, accountability, and lifecycle alignment, but they remain abstract to end users. Evidence across sources highlighted five recurring issues, which are discussed in sections 3.8.2.1 through 3.8.2.5.

3.8.2.1 Lifecycle Standards are too Abstract for Manufacturing Contexts

AI-specific standards provide lifecycle guidance on risk, data, and oversight, but they remain principle-based, suggesting what to do rather than how to do it in industrial workflows [36], [53], [54], [56]. Case studies revealed pilot projects proceeding without validation or monitoring protocols, confirming that firms often treat standards as conceptual anchors rather than applied playbooks [20], [28]. SMEs described receiving broad directives from standards but no practical roadmaps, leaving them to design ad hoc validation or stress testing processes [6], [12], [56].

Implication: Abstraction at the point of use hinders implementation and increases the risk of silent failure modes and costly rework, with SMEs disproportionately exposed because they lack the governance capacity to operationalize generic clauses [6], [12], [56].

3.8.2.2 Human and Organizational Risks are Underrepresented

While psychosocial and organizational risks are recognized in OH&S frameworks, such as CAN/CSA-Z1003/BNQ 9700-803 and ISO 45003, they are largely absent from AI-specific standards, which tend to emphasize technical system assurance [57], [58], [61], [112]. Evidence from interviews and case studies consistently pointed to workforce stress, surveillance anxiety, loss of tacit knowledge, and silent resistance when workers were excluded from AI design [12].

Implication: By omitting psychosocial and organizational dimensions, AI-specific standards undermine completeness of risk assessments and misalign with occupational health obligations. This increases the likelihood of disengagement, turnover, and failed adoption, even when technical performance is strong [56], [57], [59].

3.8.2.3 Uptake is Uneven and Particularly Low Among SMEs

Although international standards on AI adoption exist, their practical uptake is low, particularly among SMEs, who often lack awareness, resources, or interpretive capacity [6], [12], [28], [37]. Case studies revealed firms abandoning pilots due to cost and complexity, while interviews described reliance on individual AI champions, making projects vulnerable if key staff were to depart [12], [42], [56]. The literature highlighted that large firms with compliance infrastructure can integrate standards, but SMEs struggle to justify the expense of purchasing and interpreting documents, hindering adoption [36], [42].

Implication: Uneven uptake of standards produces a two-tier governance environment where well-resourced firms internalize global frameworks while SMEs operate informally or disengage, widening their exposure to unmanaged risk and reducing sector-wide consistency in safety, accountability, and data integrity [6], [12], [28], [56].

3.8.2.4 Feedback Loops Between Practice and Standards Bodies Are Weak

Practitioners reported that standards often feel disconnected from implementation realities, such as system drift, integration challenges, or workforce adaptation [11], [20], [56]. Case studies confirmed that governance guidance rarely accounts for operational contingencies or change management requirements [28]. Interviews described frustration with static documents that do not evolve with emerging risks, such as psychosocial stressors or LLM-enabled vulnerabilities [12], [56].

Implication: When feedback channels are limited, standards could lean more toward theoretical consensus than operational realities. This may reduce usability, limit adaptive refinement, and erode compliance motivation, particularly among firms without the resources to translate abstract guidance into practice.

3.8.2.5 Canada Lags in Sector-Specific and Risk-Responsive Standardization

Compared to the EU's enforceable, risk-tiered AI Act or Japan's national AI strategy, Canada's approach remains voluntary, fee-based, and fragmented [42], [98], [105]. The literature and interviews confirmed that firms, especially SMEs, must shoulder the full burden of determining relevance, interpretation, and application, often while competing in global supply chains where compliance with EU obligations is a procurement prerequisite [6], [12], [56], [94].

Implication: Canada's fragmented AI framework risks leaving manufacturers underprepared, overburdened, and internationally uncompetitive. Without enforceable sector-specific instruments or funded interpretive infrastructure, SMEs in particular face stalled innovation, constrained market access, and heightened liability exposure [56], [94].

3.8.3 Gaps and Opportunities for Standardization

The findings in this report reflect not only discrete implementation challenges but also deeper, systemic gaps in Canada's current approach to AI governance in manufacturing. These gaps are structural, cultural,



"The findings in this report reflect not only discrete implementation challenges but also deeper, systemic gaps in Canada's current approach to AI governance in manufacturing."

and relational in nature, effectively cutting across lifecycle phases, organizational functions, and policy environments. Addressing them requires an integrated strategy focused on competence, coherence, and collaboration. Sections 3.8.3.1 through 3.8.3.5 synthesize the five compound gaps and the opportunities they present for more responsible and scalable AI adoption.

3.8.3.1 The Implementation Readiness Gap

Evidence from case studies and interviews showed that many firms equate AI readiness with the completion of pilot projects or basic IT investments, while lacking lifecycle maturity in areas such as validation, monitoring, or contingency planning [12], [28], [56]. The literature confirmed that readiness requires structured governance, risk literacy, and cross-functional leadership, which most SMEs lack. This overestimation of capacity leads to silent failures, low returns on investment, and disillusionment [12], [37].

Opportunity: Introduce structured self-assessment tools and staged AI maturity models that emphasize systems readiness (data governance, lifecycle fluency, and change leadership) as prerequisites for deployment. This reframes readiness from a technology-first to a systems-first benchmark, reducing fragility and stalled adoption.

3.8.3.2 The Interpretability and Translation Gap

Standards such as ISO/IEC 23894 [53] and ISO/IEC 42001 [54] provide lifecycle guidance but remain too abstract for most manufacturers, who are told what to do but not how to do it [56]. Case studies revealed pilots that proceeded without stress testing or post-deployment monitoring because firms lacked practical templates [20], [28]. Interviews underscored that SMEs often lack compliance resources, leaving them unable to translate abstract frameworks into daily operations.

Opportunity: Develop national interpretive infrastructure, including sector-specific guides, plain language toolkits, and subsidized access to standards, that translates global frameworks into actionable industrial practice. This would balance uptake and reduce stratified compliance between large and small firms.

3.8.3.3 The Human and Psychosocial Gap

Psychosocial risks, including technostress, surveillance anxiety, role ambiguity, and tacit knowledge loss, were consistently reported in interviews and case studies [12], [56], [59], [60], yet remain largely absent from AI-specific standards. The literature highlighted that these risks are foreseeable and measurable [8], [36]. By ignoring psychosocial safety, firms undermine trust, accelerate disengagement, and create barriers to sustainable adoption [56], [59], [60].

Opportunity: Reframe psychosocial safety as a core implementation criterion and embed it into AI adoption frameworks through participatory design requirements, psychosocial risk assessments, and post-deployment monitoring. Recognizing human well-being as a systemic determinant of adoption success would bring governance into alignment with OH&S norms.

3.8.3.4 The Feedback and Learning Gap

Evidence across all sources confirmed weak feedback loops between frontline implementation and standards development. Interviews described frustration with static documents that do not evolve with practice [12], [56]. Case studies revealed governance blind spots in areas such as drift detection, change management, and legacy integration, which were absent from standards.

Opportunity: Establish structured feedback mechanisms in national AI programs and standardization processes, such as post-deployment reporting loops, SME advisory panels, and implementation-focused co-design groups. Embedding bidirectional learning would prevent standards from remaining symbolic and ensure they adapt alongside emerging risks.

3.8.3.5 The Strategic Alignment Gap

Canada's AI standardization environment remains voluntary, fragmented, and inconsistently aligned with global compliance regimes such as the EU AI Act [96], [97]. Firms reported shouldering disproportionate responsibility for interpreting and applying standards, with SMEs most affected by resource constraints [6], [12] [56]. This could create a widening gap between international compliance expectations and domestic readiness [94].

Opportunity: Develop a coordinated national strategy for AI in manufacturing that integrates regulatory alignment, SME supports, and risk-tiered compliance pathways. Such a strategy would reduce duplication, align domestic practice with international obligations, and strengthen competitiveness in global supply chains.

3.8.4 Bridging Gaps Through Integrated Mitigation

The findings in this section describe an environment of high ambition constrained by uneven governance infrastructure, limited implementation support, and underrecognized human impacts. AI adoption in Canadian manufacturing is progressing, but without deliberate efforts to close the compound gaps identified here, manufacturers risk unintended harm, inefficiency, and loss of competitive advantage at an international scale.

4 Recommended Strategies for Strengthening Standardization

The assessment of AI in Canadian manufacturing highlights a diverse set of risks that are deeply interlinked rather than isolated. Addressing these risks requires a systems-based approach where manufacturers, industry associations, standards bodies, and governments work together to build enabling infrastructure. Grounded in good practice for risk management (ISO 31000 [127], ISO/IEC 23894 [53]), this section translates the systemic gaps identified in Section 3.8 into concrete recommended mitigation strategies.

4.1 Mitigation Strategy Framework

This framework organizes mitigation strategies according to the eight primary risk classes introduced in Section 3.7 (see Table 10). Each strategy addresses the specific vulnerabilities surfaced during the assessment while also reinforcing lifecycle integrity and structural coherence. In addition, the structure reflects the principles set out in ISO 31000, ISO/IEC 22989 [69], and ISO/IEC 42001 [54], including:

- **Use of best available information:** All mitigation strategies are supported by evidence triangulated across the interviews, literature, standards, and case studies.
- **Lifecycle integration:** Mitigation strategies are mapped to phases (e.g., design, development, deployment, and post-deployment).
- **Governance domain mapping:** Each recommendation is linked to a functional domain (e.g., data governance, health and safety, organizational learning, and cybersecurity).

Furthermore, the mitigation strategies go beyond compliance to emphasize capacity-building, resilience, and relational integrity. This means addressing not only what can go wrong with systems but also how to support the people, structures, and ecosystems required to make AI work in practice. As such, each strategy is designed to:

- Reduce likelihood or severity of known risks;
- Enhance implementation capacity through education, feedback, or system design;
- Bridge structural gaps (e.g., access, interpretability, coordination); and
- Embed trust and transparency as part of system function.

Section 4.2 provides risk-specific strategies and recommendations across the eight categories of risk, along with examples of each strategy's potential actions and potential impacts on AI adoption in the Canadian manufacturing sector.

4.2 Recommendations

The analysis of risks and gaps demonstrated that while additional standards may be helpful, what Canadian manufacturers really need are more effective ways to make existing standards more practical, relevant, and accessible. The interviews, case studies, and literature consistently revealed that firms, especially SMEs, struggle to interpret abstract frameworks, integrate them across functions, and align them with operational realities [6], [12], [28], [56].

Interviewees pointed out that in many cases, standards outline what should be done but provide little guidance on how to do it in a manufacturing context.

This section translates the findings into five actionable recommendations, which are grounded in lifecycle principles from ISO/IEC 23894 [53] and ISO/IEC 42001 [54] and informed by the lived experience and practical insights of the Canadian manufacturers who participated in the interviews and were represented in the literature review. The recommendations emphasize readiness, data foundations, human-system integration, feedback mechanisms, strategic alignment, and interpretability support. Together, they provide a pathway for strengthening adoption capacity while ensuring that AI systems are technically reliable, socially workable, and globally competitive.

4.2.1 Develop Implementation-Focused Guidance for Standards

Canadian manufacturers often overestimate their readiness for AI, equating basic IT infrastructure or pilot project experience with implementation maturity when their governance and lifecycle capacity are weak [6], [12], [28]. Case studies showed that pilots frequently failed without scaling due to a lack of ownership and integration across functions [20], [56], while interviews revealed that SMEs rarely conduct post-deployment monitoring unless mandated.

Although ISO/IEC 23894 [53] and ISO/IEC 42001 [54] emphasize lifecycle governance, they remain abstract, outlining principles rather than providing concrete operational pathways. Missing elements include standardized validation protocols, fallback planning, and SME-friendly maturity models that help organizations assess whether they are ready to adopt AI [28], [56]. SMEs face additional barriers, such as limited budgets, fewer technical staff, and difficulty interpreting complex technical frameworks and standards, which makes accessible, step-by-step implementation models essential.

Lifecycle readiness also extends beyond deployment. Many firms lack defined processes for ongoing monitoring, retraining, and safe decommissioning. Strengthening post-deployment governance requires periodic audits, performance dashboards, and automated alerts for anomalies or bias, as well as scheduled retraining and validation cycles triggered by changes in output behaviour. Documenting lessons learned during decommissioning, alongside clear accountability for post-use impacts, should form part of lifecycle closure.

Recommendation 1: Companion guides to ISO/IEC 23894 [53] and ISO/IEC 42001 [54] could be developed for the manufacturing sector, embedding tools such as pre-deployment validation checklists, cross-functional project management templates (e.g., RACI chart), and fallback procedures. For SMEs, these guides could

illustrate how to start small, demonstrate value, and scale adoption through staged readiness levels and lightweight governance practices. Public investment in readiness assessments and staged maturity models would allow SMEs to evaluate governance capacity before adoption, reducing stranded pilot projects and enhancing system resilience [6], [12], [28].

Potential Actions:

- **Applied interpretation guides:** Short, practical add-ons that show exactly how existing standards (e.g., safety, quality, risk) apply in AI-supported processes. For example, a process map showing how a hazard identification clause applies to an AI-enabled inspection workflow.
- **Sector-specific examples:** Manufacturing-relevant demonstrations (e.g., quality checks, predictive maintenance, vision systems) that allow teams to understand how to interpret a standard in their specific environment.
- **Before-and-after workflow visuals:** Show manufacturers how processes change once AI enters the system, including what stays the same, what needs modification, and where responsibilities shift.
- **Navigation tools for standards:** A simple tool for organizations to identify which standards apply and how they connect, instead of guessing across dozens of documents.

Potential Impacts:

- Reduces misinterpretation and ad hoc adoption.
- Builds confidence in applying standards without needing an external consultant.
- Supports SMEs that lack internal expertise.
- Increases consistency of implementation across the sector.

4.2.2 Improve Data and Infrastructure Foundations

Data governance was consistently identified as a structural weakness across the literature, case studies, and interviews [2], [26], [36]. Poor metadata, non-representative datasets, and legacy enterprise resource planning or SCADA systems were cited as common reasons for AI underperformance in Canadian manufacturing [12], [28], [56]. In several case studies, technically sound models failed because input data was incomplete or biased [20].

While ISO/IEC 22989 [69] and ISO/IEC 5339 [108] establish lifecycle terminology and principles, they do not provide specific benchmarks for data quality or interoperability across industrial systems. Interviews revealed that SMEs often lacked clarity on what constitutes sufficient data quality to safely deploy AI, leaving them to rely on ad hoc thresholds [12]. Missing elements include industrial data quality indicators, lifecycle retraining protocols, and vendor accountability clauses for outsourced data handling [28].

Recommendation 2: Sector-specific frameworks could be developed to help align standards (e.g., ISO/IEC 22989, ISO/IEC 5338, ISO/IEC 5339, ISO/IEC 5259-1) into interoperable manufacturing profiles, defining thresholds for data quality and continuous retraining cycles. Publicly funded interpretive supports, such as open access playbooks, shared reference datasets, |and vendor accountability templates, could reduce fragmentation, making AI data governance actionable for SMEs.

Potential Actions:

- Standardized data quality checklists tied to lifecycle stages (e.g., training, validation, deployment, retraining).
- Clear thresholds for representativeness, completeness, and drift detection in industrial datasets.
- Vendor accountability templates that clarify data ownership, quality obligations, and retraining responsibilities.

Potential Impacts:

- Reduces AI underperformance caused by hidden data issues.
- Improves reliability and reproducibility of AI systems.
- Supports SMEs in making defensible deployment decisions.

4.2.3 Integrate Psychosocial and Human Factors

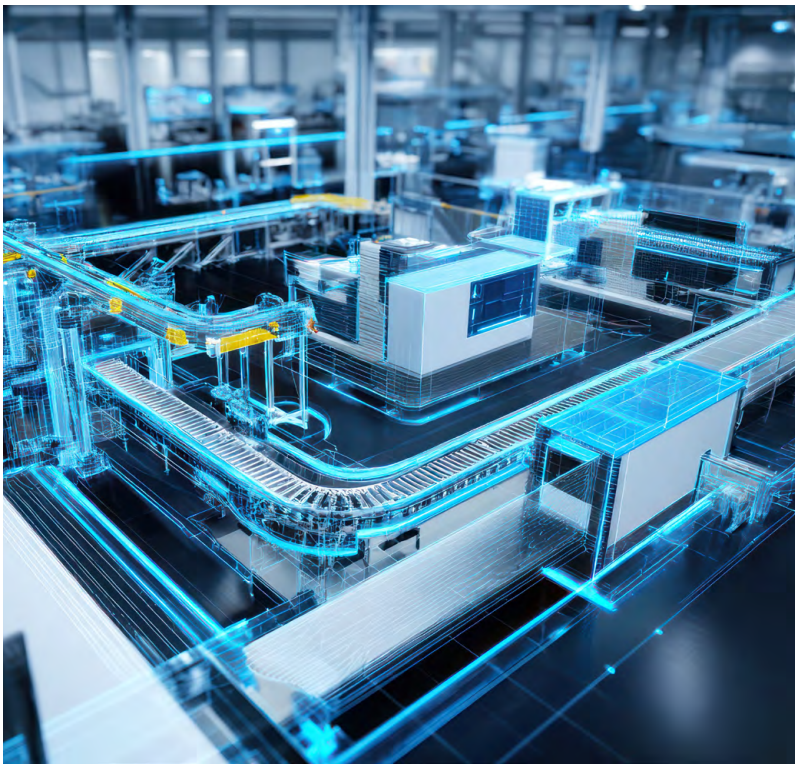
Psychosocial impacts, which are currently unaddressed in both organizational processes and industry standards, create real financial, legal, and performance risks. Although they were prominent in the interviews and case studies, human-machine interaction and psychosocial risks are largely absent from AI-specific standards [11], [12], [56]. Workers reported stress from human-machine teaming, opaque decision systems, cognitive overload from monitoring, and loss of tacit skills when AI displaced manual judgment [12], [20], [56]. The literature confirmed that while these risks are foreseeable and measurable, they are underrecognized in governance frameworks [57], [59], [60].

ISO/IEC 42001 [54] establishes organizational requirements for AI management systems, including stakeholder oversight and lifecycle governance, but it does not extend to detailed guidance on usability testing, human-machine interaction, or psychosocial protection [54]. These dimensions fall outside its scope and are more directly addressed in complementary standards (e.g., ISO 9241-11 and ISO 45003) [59]. Integrating principles from these related frameworks would strengthen the practical application of ISO 42001 [54] in manufacturing environments, particularly where AI systems affect worker cognition, autonomy, and trust.

Recommendation 3: Standards could include practical requirements that make AI systems easier and safer for people to use. This includes designing explainable systems so operators can understand how decisions are made and setting usability limits to prevent cognitive overload. Standards could also help preserve workers' tacit knowledge as automation increases and ensure operators have clear rights to question or override AI decisions. These measures, aligned with OH&S standards, such as CAN/CSA-Z1003/BNQ 9700-803 and ISO 45003 [61], [112], could help reduce stress, build trust, and prevent disengagement.

Potential Actions:

- **Psychosocial risk screening for all AI projects:** Evaluate anticipated impacts on workload, autonomy, pace, cognitive burden, and job clarity.



- **Early worker engagement:** Understand stress points before rollout and design mitigation strategies.
- **Decision authority clarity:** Matrices that show exactly what the AI decides, what humans decide, and when escalation is required.
- **Human-AI interaction key performance indicators:** Error patterns, hesitation points, override frequency, confusion signals, and near-miss trends.
- **Psychological safety commitments:** No-blame reporting, support for raising concerns, and recognition for identifying AI faults.

Potential Impacts:

- Avoids preventable mental-health-related costs (e.g., absenteeism, turnover, errors).
- Reduces ethical and legal exposure.
- Builds trust in AI adoption instead of resistance.
- Makes AI safer and more reliable in real-world workflows.

4.2.4 Strengthen Lifecycle Governance with Co-Created Guidance Tools

Manufacturers reported that standards are disconnected from practice, offering abstract principles without acknowledging day-to-day integration challenges. Case studies confirmed that issues such as drift detection and legacy integration are rarely reflected in current governance tools [20], while interviews described frustration with static documents that lack contextual relevance.

Recommendation 4: Canadian and international standards bodies could establish structured feedback channels, such as SME consultation panels, post-implementation reporting loops, and co-design working groups. Embedding practitioner perspectives before, during, and after standard development could help improve operational fit and legitimacy, ensuring that governance evolves alongside real-world manufacturing practice.

Potential Actions:

- **Lifecycle templates for each phase:** Pilot → Scale → Sustain → Retire; with tasks, owners, indicators, and risks clearly mapped.
- **Transition planning tools:** Guidance for handoffs between teams, changes in decision authority, updating standard operating procedures, and revising training materials.
- **Change management guidance:** Built directly into standards; not optional but required.
- **Drift detection and escalation routines:** Monthly or quarterly checkpoints, drift indicators, and clear escalation triggers.

Potential Impacts:

- Reduces surprises during scale-up.
- Prevents operational drift and hidden failures.
- Ensures AI adapts with the organization, not away from it.

4.2.5 Build Governance Maturity

Standards assume that foundational governance structures are already in place, but many organizations have gaps in roles, documentation, oversight, and change management. Even when firms are aware of AI standards, uptake is low, particularly among SMEs. Interviews revealed reliance on individual AI champions, leaving organizations vulnerable if those staff depart. Missing supports include free or subsidized interpretive guides, SME-oriented toolkits, and training programs that explain standards in plain language and industrially relevant contexts.

Recommendation 5: National programs could fund intermediary supports that translate AI standards into more practical tools for manufacturers, including modular implementation templates, open access guides, and subsidized SME training. These supports could help reduce stratified compliance and help ensure equitable adoption across Canada's manufacturing base.

Potential Actions:

- **Foundations toolkit:** Templates for roles, responsibilities, documentation systems, change management routines, and oversight structures.
- **Training programs and micro-credentials:** Focused on standards interpretation, AI governance, and system integration. For example, a Standards Interpretation 101 course with real manufacturing scenarios.
- **Governance readiness assessments:** A simple diagnostic tool companies can use to evaluate their preparedness for adopting standards or AI.
- **Baseline management system requirement:** Encourage industry associations or regulators to promote a minimum governance standard before layering in specialty or AI-specific standards.
- **Guidance for right-sizing governance:** Help SMEs adopt governance practices that fit their size; not overwhelming but not absent.

Potential Impacts:

- Aligns organizations with the level of structure that standards assume.
- Reduces chaos at transition points (e.g., scaling, handoffs, system drift).
- Builds in-house expertise.
- Supports sustainable AI adoption instead of crisis-driven implementation.

4.3 Insight for Addressing Standards Gaps

The mitigation strategies presented in Section 4.2 are only as strong as the standards and governance ecosystem that manufacturers can realistically access and apply. The findings show that the current ecosystem for AI adoption in the Canadian manufacturing sector is fragmented, abstract, and often inaccessible, particularly for SMEs. From the end-user perspective, the primary issue is not the absence of standards, but the difficulty of finding, interpreting, and integrating them into daily practice.

The manufacturing sector already works within a broad landscape of guidance documents, technical codes, and evolving AI frameworks, and introducing additional AI-specific requirements without first considering how existing standards might be adapted could contribute to further complexity. In practice, many of the foundational principles required to manage AI-related risks, such as those governing safety, quality, and risk management, are already present in existing standards. The real challenge lies in understanding and applying these principles to new AI contexts.

Equally important is the user experience of standards adoption. The interviews and case studies revealed that many manufacturers do not know where to begin, and even when they are aware of relevant standards, many face barriers related to cost, technical language, and interpretive complexity. Current processes assume a baseline of expertise and governance maturity that does not reflect the reality of most Canadian SMEs. In practice, firms need an interface to the standards ecosystem with clear entry points, practical guidance, and curated pathways that help them understand what is most relevant to their context.

There is an opportunity for standards bodies and industry partners to design sectoral "starter kits" for standards, which could include bundled sets of documents, interpretive guides, and templates that map the ecosystem of applicable requirements for a given subsector (e.g., automotive, food processing, and advanced materials). Such kits could be paired with digital navigation tools that allow manufacturers to filter standards by risk class, lifecycle stage, or organizational function. By making the standards environment clear and navigable, standards bodies can transform overwhelming complexity into actionable insight.

Finally, while standards development processes already involve diverse technical and policy experts, greater participation from those who apply these standards day-to-day (e.g., plant managers, HR leaders, OH&S professionals, and supervisors) could help improve usability. Embedding these roles into standards development and revision processes could help ensure that documents not only set principles but also provide applicable methods aligned with organizational and human realities.

Ultimately, unless Canada invests in translation infrastructure, practical navigation tools, and participatory development processes, the standards ecosystem for AI adoption in the Canadian manufacturing sector may remain difficult for many firms to access.

5 Conclusions

This research report examined the current landscape of AI adoption in Canadian manufacturing, identifying the risks, gaps, and opportunities that will shape its future trajectory. By analyzing evidence from the literature, case studies, semi-structured interviews, and standards, the research surfaced challenges that include technical fragility, data quality deficits, psychosocial harms, organizational silos, and regulatory misalignment. The findings also indicate that these risks are deeply interconnected, reflecting systemic weaknesses in lifecycle integration, operational readiness, and workforce support.

To address the identified risks and gaps, the report presented a multidimensional framework of mitigation strategies organized by lifecycle phases and functional domains. It emphasized that technical safeguards alone are insufficient for effective AI adoption, which requires coherent organizational systems, psychosocial protections, cross-functional collaboration, and alignment with international regulatory trends. The mitigation strategies demonstrate that safer, more sustainable adoption is possible when manufacturers, policymakers, and standards bodies treat AI not simply as a tool to be deployed, but as a sociotechnical system to be managed with care.

The findings converge on three imperatives. First, manufacturers could benefit from strengthening foundational readiness (e.g., data practices, workforce skills, and risk literacy) before moving toward large scale AI deployment. Second, standards bodies could consider developing sector specific guidance that helps translate existing standards in ways that are more accessible and practical for SMEs. Third, policymakers could explore approaches that go beyond voluntary guidance to build more coordinated, risk responsive systems that align with international expectations while remaining sensitive to domestic needs.

The path toward successful AI adoption in Canadian manufacturing is not about eliminating risk, but about embedding adaptive practices that anticipate, monitor, and mitigate evolving challenges over time. Canada's opportunity lies in turning its strong ethical orientation and global credibility in responsible AI into tangible supports for manufacturers navigating practical implementation, which requires leadership, investment, and trust-building across the entire ecosystem.

Ultimately, the findings of this report call for a move from fragmented ambition to coordinated action that is grounded in human-centred design, resilient systems, and adaptive practice. By treating AI not only as a technological innovation but also as a shared responsibility, Canadian manufacturing could chart a course toward safe, competitive, and socially sustainable adoption.

References

[1] R. S. Peres, X. Jia, J. Lee, K. Sun, A. W. Colombo, and J. Barata, "Industrial artificial intelligence in Industry 4.0 – Systematic review, challenges and outlook," *IEEE Access,* vol. 8, pp. 220121–220139, 2020, https://doi.org/10.1109/ACCESS.2020.3042874.

[2] B. P. Sah, N. I. Tanha, M. A. Sikder, and S. M. Habibullah, "The integration of Industry 4.0 and lean technologies in manufacturing industries: A systematic literature review," *IJMISDS,* vol. 1, no. 3, pp. 14–25, 2024, https://doi.org/10.62304/ijmisds.v1i3.164.

[3] R. Cioffi, M. Travaglioni, G. Piscitelli, A. Petrillo, and F. De Felice, "Artificial intelligence and machine learning applications in smart production: Progress, trends, and directions," *Sustainability,* vol. 12, no. 2, 2020, Art. no. 492, https://doi.org/10.3390/su12020492.

[4] R. Rakholia, A. L. Suárez-Cetrulo, M. Singh, and R. S. Carbajo, "Advancing manufacturing through artificial intelligence: Current landscape, perspectives, best practices, challenges, and future directions," *IEEE Access,* vol. 12, pp. 131621–131637, 2024, https://doi.org/10.1109/ACCESS.2024.3458830.

[5] M. Ghosh, "AI-driven predictive maintenance in Indian manufacturing: Enhancing operational efficiency," *Innovative Research Thoughts,* vol. 8, no. 4, 2022, https://doi.org/10.36676/irt.v8.i4.1512.

[6] G. A. Harris and A. Yarbrough, "Industry 4.0 Technology adoption issues for small- and medium-sized manufacturers and the role of AI to improve adoption rates," in *Pan Pacific Strategic Electronics Symposium (Pan Pacific),* Kona, HI, United States, Jan. 29–Feb. 1, 2024, pp. 1–6, https://doi.org/10.23919/PanPacific60013.2024.10436513.

[7] K. Kovič, P. Tominc, J. Prester, and I. Palčič, "Artificial intelligence software adoption in manufacturing companies," *Appl. Sci.,* vol. 14, no. 16, 2024, Art no. 6959, https://doi.org/10.3390/app14166959.

[8] R. Geissbauer, S. Schrauf, V. Koch, and S. Kuge, "Industry 4.0 – Opportunities and challenges of the industrial internet," PricewaterhouseCoopers, Frankfurt, Germany, Dec. 2014. [Online]. Available: https://www.pwc.nl/en/assets/documents/pwc-industrie-4-0.pdf

[9] Innovation, Science and Economic Development Canada. "Key small business statistics," Innovation, Science and Economic Development Canada, Ottawa, ON, Canada, 2024. [Online]. Available: https://ised-isde.canada.ca/site/sme-research-statistics/en/key-small-business-statistics/key-small-business-statistics-2023

[10] A. Arcand, "Manufacturing Canada's future," Canadian Manufacturers and Exporters, Ottawa, ON, Canada, Nov. 2023. [Online]. Available: https://cme-mec.ca/wp-content/uploads/2023/11/2023-CME-Report-Manufacturing-Canadas-Future_Final-2_web.pdf

[11] J. P. Nelson, J. B. Biddle and P. Shapira, "Applications and societal implications of artificial intelligence in manufacturing: A systematic review," Jul. 25, 2023, https://doi.org/10.48550/arXiv.2308.02025.

[12] A. Taherizadeh and C. Beaudry, "An emergent grounded theory of AI-driven digital transformation: Canadian SMEs' perspectives," *Ind. Innov.,* vol. 30, no. 9, pp. 1244–1273, 2023, https://doi.org/10.1080/13662716.2023.2242285.

[13] Canadian Institute for Advanced Research. "The Pan-Canadian AI Strategy." [Online]. Available: https://cifar.ca/ai

[14] J. Wan, X. Li, H. N. Dai, A. Kusiak, M. Martinez-Garcia, and D. Li, "Artificial-intelligence-driven customized manufacturing factory: Key technologies, applications, and challenges," in *Proc. IEEE,* vol. 109, no. 4, pp. 377–398, 2021, https://doi.org/10.1109/JPROC.2020.3034808.

[15] H. Ding, R. X. Gao, A. J. Isaksson, R. G. Landers, T. Parisini, and Y. Yuan, "State of AI-based monitoring in smart manufacturing and introduction to focused section," *IEEE/ASME Trans. Mechatron.,* vol. 25, no. 5, pp. 2143–2154, 2020, https://doi.org/10.1109/TMECH.2020.3022983.

[16] J. Wan, M. Xia, and A. Kusiak, "Guest editorial: Special section on internet of things and artificial intelligence for product life-cycle management of complex equipment," *IEEE Trans. Ind. Inform.,* vol. 18, no. 11, pp. 8074–8076, 2022, https://doi.org/10.1109/TII.2022.3186890.

[17] Z. Huang, Y. Shen, J. Li, M. Fey, and C. Brecher, "A survey on AI-driven digital twins in Industry 4.0: Smart manufacturing and advanced robotics," *Sensors,* vol. 21, no. 19, 2021, Art. no. 6340, https://doi.org/10.3390/s21196340.

[18] S. P. Murzin, "Artificial intelligence-driven innovations in laser processing of metallic materials," *Metals,* vol. 14, no. 12, 2024, Art. no. 1458, https://doi.org/10.3390/met14121458.

[19] A. Badrinarayanan, "AI in manufacturing: Driving operational excellence," in *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.,* vol. 10, no. 6, pp. 585–594, 2024, https://doi.org/10.32628/CSEIT24106199.

[20] R. Branco et al., "Explainable AI in manufacturing: An analysis of transparency and interpretability methods for the XMANAI platform," in *Proc. IEEE International Conference on Engineering, Technology, and Innovation (ICE/ITMC),* Edinburgh, United Kingdom, Jun. 19–22, 2023, pp. 1–8, https://doi.org/10.1109/ICE%2FITMC58018.2023.10332373.

[21] P. Toth, "Cybersecurity – A critical component of industry 4.0 implementation," NIST, Manufacturing Innovation Blog, Sep. 7, 2022. [Online]. Available: https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-critical-component-industry-40-implementation.

[22] P. Waghanna, A. Reddy, S. Deshpande, S. Chavan, V. R. Jaiswal, and V. Naranje, "Effects of adopting Industry 4.0 on a manufacturing plant," in *Proc. 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),* Noida, India, Mar. 14–15, 2024, pp.1–6, https://doi.org/10.1109/ICRITO61523.2024.10522189.

[23] A. N. Anang, P. O. Obidi, A. O. Mesogboriwon, J. O. Obidi, M. kuubata, and D. Ogunbiyi, "The role of artificial intelligence in Industry 5.0: Enhancing human-machine collaboration," *World Journal of Advanced Research and Reviews,* vol. 24, no. 2, pp. 380–400, 2024, https://doi.org/10.30574/wjarr.2024.24.2.3369.

[24] M. Tshehla-Nkuna, N. Sukdeo, S. C. Mukwakungu, and C. Mbohwa, "Exploring the impact of advanced manufacturing technologies in South Africa's pharmaceutical industry," in *Proc. International Conference on Artificial Intelligence, Computer, Data Sciences, and Applications (ACDSA),* Victoria, Seychelles, Feb 1–2, 2024, pp. 1–6, https://doi.org/10.1109/ACDSA59508.2024.10467315.

[25] S. P. Leo Kumar, "State of the art-intense review on artificial intelligence systems application in process planning and manufacturing," *Eng. Appl. Artif. Intell.,* vol. 65, pp. 294–329, 2017, https://doi.org/10.1016/j.engappai.2017.08.005.

[26] I. K. Nti, A. F. Adekoya, B. A. Weyori, and O. Nyarko-Boateng, "Applications of artificial intelligence in engineering and manufacturing: A systematic review," *J. Intell. Manuf.,* vol. 33, no. 6, pp. 1581–1601, 2022, https://doi.org/10.1007/s10845-021-01771-6.

[27] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, "Artificial intelligence applications for Industry 4.0: A literature-based study," *J. Ind. Integr. Manag.,* vol. 7, no. 1, pp. 83–111, 2022, https://doi.org/10.1142/S2424862221300040.

[28] F. Dinmohammadi, "Adopting artificial intelligence in Industry 4.0: Understanding the drivers, barriers and technology trends," in *Proc. 28th International Conference on Automation and Computing (ICAC),* Birmingham, United Kingdom, Aug. 30–Sep. 1, 2023, pp. 1–6, https://doi.org/10.1109/ICAC57885.2023.10275230.

[29] B. Lal, V. S. N., M. A. Kumar, N. Chinthamu, and S. Pokhriyal, "Development of product quality with enhanced productivity in Industry 4.0 with AI driven automation and robotic technology," in *Proc. Second Int. Conf. Augment. Intell. Sustain. Syst. (ICAISS),* Trichy, India, Aug. 23–25, 2023, pp. 184–189, https://doi.org/10.1109/ICAISS58487.2023.10250736.

[30] M. Katari, L. Shanmugam, and J. N. Arasu Malaiyappan, "Integration of AI and machine learning in semiconductor manufacturing for defect detection and yield improvement," *JAIGS,* vol. 3, no. 1, pp. 418–431, 2024, https://doi.org/10.60087/jaigs.v3i1.191.

[31] B.-H. Li, B.-C. Hou, W.-T. Yu, X.-B. Lu, and C.-W. Yang, "Applications of artificial intelligence in intelligent manufacturing: A review," *Frontiers Inf. Technol. Electronic Eng.,* vol. 18, no. 1, pp. 86–96, 2017, https://doi.org/10.1631/FITEE.1601885.

[32] J. Senoner, T. Netland, and S. Feuerriegel, "Using explainable artificial intelligence to improve process quality: Evidence from semiconductor manufacturing," *Manag. Sci.,* vol. 68, no. 8, pp. 5704–5723, 2022, https://doi.org/10.1287/mnsc.2021.4190.

[33] O. Krupicka, S. A. M. Gilani, A. Tantry, S. Askri, T. Mulla, F. Khan, F. Armosh, and R. Peel, "The Application of machine learning in supporting supply chain management operations in the manufacturing sector based in England," In: Mansour, N., Bujosa Vadell, L.M. (eds) Green Finance and Energy Transition. Contributions to Finance and Accounting. Springer, Cham. https://doi.org/10.1007/978-3-031-75960-4_39

[34] R. Wang and Y. Yin, "Exploring the impact of artificial intelligence on knowledge management in automotive manufacturing within different cultures: China and Germany as examples," in *Proc. 25th European Conference on Knowledge Management,* Veszprém, Hugary, Sep. 5–6, 2024, vol. 25, no. 1, pp. 1051–1061, https://doi.org/10.34190/eckm.25.1.2415.

[35] R. A. Adebayo, N. C. Obiuto, O. K. Olajiga, and I. C. Festus-Ikhuoria, "AI-enhanced manufacturing robotics: A review of applications and trends," *World Journal of Advanced Research and Reviews,* vol. 21, no. 3, pp. 2060–2072, 2024, https://doi.org/10.30574/wjarr.2024.21.3.0924.

[36] K. Alwani and M. C. Urban, "The digital age: Exploring the role of standards for data governance, artificial intelligence and emerging platforms," Canadian Standards Association, Toronto, ON, Canada, May 2019. [Online]. Available: https://www.csagroup.org/wp-content/uploads/CSA-Group-research-Digital-Economy.pdf

[37] A. Lockhart, "Automation nation? AI adoption in Canadian businesses," The Dais, Toronto, ON, Canada, Sep. 2023. [Online]. Available: https://dais.ca/reports/automation-nation-ai-adoption-in-canadian-businesses

[38] CGI Canada, *Cutting through the AI hype in Canada manufacturing.* (May 9, 2024). [Online Video]. Available: https://www.youtube.com/watch?v=c_kddOD7lTY

[39] M. Ghoreishi and A. Happonen, "New promises AI brings into circular economy accelerated product design: A review on supporting literature," *E3S Web Conf.,* vol. 158, 2020, Art. no. 06002, https://doi.org/10.1051/e3sconf/202015806002.

[40] Sherry. "7 Game changing AI applications revolutionizing Canadian manufacturing today." Business & Industry Canada. Accessed: Jun. 7, 2025. [Online]. Available: https://www.industryandbusiness.ca/7-game-changing-ai-applications-revolutionizing-canadian-manufacturing-today/

[41] P. Trakadas et al., "An artificial intelligence-based collaboration approach in industrial IoT manufacturing: Key concepts, architectural extensions and potential applications," *Sensors,* vol. 20, no. 19, 2020, Art. no. 5480, https://doi.org/10.3390/s20195480.

[42] A. Brandusescu, "Artificial intelligence policy and funding in Canada: Public investments, private interests," Centre for Interdisciplinary Research on Montreal, McGill University, Montreal, QC, Canada, Mar. 2021. [Online]. Available: https://www.mcgill.ca/centre-montreal/files/centre-montreal/aipolicyandfunding_report_updated_mar5.pdf

[43] M. Lee, "Locating Canada in Industry 4.0: Barriers and opportunities," Centre for International Governance Innovation, Waterloo, ON, Canada, 2025. Accessed: Jun. 7, 2025. [Online]. Available: https://www.cigionline.org/static/documents/DPH-paper-Lee_sTqA57x.pdf

[44] Natural Resources Canada. "Canada and the Northwest Territories partner on innovative, AI-based core scanning initiative to support critical minerals development." Accessed: Sep. 1, 2025. [Online]. Available: https://www.canada.ca/en/natural-resources-canada/news/2025/07/canada-and-the-northwest-territories-partner-on-innovative-ai-based-core-scanning-initiative-to-support-critical-minerals-development.html

[45] Canadian Northern Economic Development Agency. "Regional artificial intelligence initiative (RAII)." Accessed: Sep 1, 2025. [Online]. Available: https://www.cannor.gc.ca/eng/1731601687376/1731601710675

[46] Innovation, Science and Economic Development Canada. "Canada's Advanced Manufacturing Cluster." [Online]. Available: https://ised-isde.canada.ca/site/global-innovation-clusters/en/canadas-advanced-manufacturing-cluster

[47] Innovation, Science and Economic Development Canada. "Canada's AI-powered supply chains cluster (Scale AI)." [Online]. Available: https://ised-isde.canada.ca/site/global-innovation-clusters/en/canadas-ai-powered-supply-chains-cluster-scale-ai

[48] Innovation, Science and Economic Development Canada. "Global Innovation Clusters." [Online]. Available: https://ised-isde.canada.ca/site/global-innovation-clusters/en

[49] Government of Canada. "Directive on automated decision-making." [Online]. Available: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

[50] Innovation, Science and Economic Development Canada. "Strategic Response Fund (SRF)." [Online]. Available: https://ised-isde.canada.ca/site/ised/en/programs-and-initiatives/strategic-response-fund

[51] National Research Council of Canada. "About the NRC Industrial Research Assistance Program." [Online]. Available: https://nrc.canada.ca/en/support-technology-innovation/about-nrc-industrial-research-assistance-program

[52] Business Development Bank of Canada. "Canada Digital Adoption Program." [Online]. Available: https://www.bdc.ca/en/canada-digital-adoption-program

[53] *Information Technology — Artificial Intelligence — Guidance on Risk Management,* ISO/IEC 23894, International Organization for Standardization, Geneva, Switzerland, 2023. [Online]. Available: https://www.iso.org/standard/77304.html

[54] *Information Technology — Artificial Intelligence — Management System,* ISO/IEC 42001, International Organization for Standardization, Geneva, Switzerland, 2023. [Online]. Available: https://www.iso.org/standard/42001

[55] H. Liu and H. Faryaar, "Technology adoption by women-owned businesses in Canada," Statistics Canada, Ottawa, ON, Canada, Aug. 2024. [Online]. Available: https://doi.org/10.25318/36280001202400800003-eng

[56] S. Chatterjee, N. P. Rana, Y. K. Dwivedi, and A. M. Baabdullah, "Understanding AI adoption in manufacturing and production firms using an integrated TAM-TOE model," *Technol. Forecast. Soc. Change,* vol. 170, 2021, Art. no. 120880, https://doi.org/10.1016/j.techfore.2021.120880.

[57] National Defence Canada. "The nine dimensions of health: Psychosocial work environment." [Online]. Available: https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2024/07/nine-dimensions-health-psychosocial-work-environment.html

[58] J. Samra, "The evolution of workplace mental health in Canada: Research report (2007–2017)," Fredericton, NB, Canada, 2017. [Online]. Available: https://drjotisamra.com/wp-content/uploads/2018/01/The-Evolution-of-Workplace-Mental-Health-in-Canada.pdf

[59] M. D. McDonnell and B. J. McAllister, "Psychosocial risks in the Canadian construction and extractive industries," *Extr. Ind. Soc.,* vol. 19, 2024, Art. no. 101515, https://doi.org/10.1016/j.exis.2024.101515.

[60] Canadian Psychological Association. "'Psychology works' fact sheet: Mental health and the workplace." [Online]. Available: https://cpa.ca/psychology-works-fact-sheet-mental-health-and-the-workplace

[61] *Psychological Health and Safety in the Workplace,* CAN/CSA-Z1003-13/BNQ 9700-803, Canadian Standards Association, Toronto, ON, Canada, 2013. [Online]. Available: https://www.csagroup.org/article/can-csa-z1003-13-bnq-9700-803-2013-r2022-psychological-health-and-safety-in-the-workplace

[62] International Society of Automation. "ISA/IEC 62443 series of standards bundle." [Online]. Available: https://www.isa.org/products/isa-iec-62443-series-of-standards-bundle

[63] S. Barocas, M. Hardt, and A. Narayanan, *Fairness and Machine Learning.* Cambridge, MA, United States: MIT Press, 2023. [Online]. Available: https://mitpress.mit.edu/9780262048613/fairness-and-machine-learning/

[64] M. Lane and A. Saint-Martin, "The impact of artificial intelligence on the labour market: What do we know so far?" Organisation for Economic Co-operation and Development, Paris, France, Rep. No. 256, 2021. [Online]. Available: https://dx.doi.org/10.1787/7c895724-en.

[65] M. Alam, M. R. Islam, and S. K. Shil, "AI-based predictive maintenance for US manufacturing: Reducing downtime and increasing productivity," *IJAETI,* vol. 1, no. 1, pp. 541–567, 2023. [Online] Available: https://ijaeti.com/index.php/Journal/article/view/711/738

[66] L. Romero. "Rate of adoption and deployment of artificial intelligence in enterprise in Singapore in 2024." Statista.com. Accessed: Dec. 27, 2024. [Online]. Available: https://www.statista.com/statistics/1489731/ai-adoption-rate-singapore/

[67] Organisation for Economic Co-operation and Development. "Global Partnership on Artificial Intelligence." [Online]. Available: https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html

[68] Organisation for Economic Co-operation and Development AI Policy Observatory. "OECD AI Principles overview." [Online]. Available: https://oecd.ai/en/ai-principles

[69] *Information Technology — Artificial Intelligence — Artificial Intelligence Concepts and Terminology,* ISO/IEC 22989, International Organization for Standardization, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/74296.html

[70] *Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML),* ISO/IEC 23053, International Organization for Standardization, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/74438.html

[71] National Institute of Standards and Technology, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," National Institute of Standards and Technology, Gaithersburg, MD, United States, Jan. 2023. [Online]. Available: https://doi.org/10.6028/NIST.AI.100-1

[72] K. Anggadol. "AI regulation in Canada: New laws and regulations to know." Canadian Lawyer. [Online]. Available: https://www.canadianlawyermag.com/resources/legal-education/ai-regulation-in-canada-new-laws-and-regulations-to-know/389978

[73] A. LaCasse. "Ahead of 2025 federal election, will Canada pass Bill C-27?" International Association of Privacy Professionals. Accessed: Jul. 1, 2025. [Online]. Available: https://iapp.org/news/a/ahead-of-2025-federal-election-will-canada-pass-bill-c-27-

[74] D. Fraser and S. A. Dykema. "The demise of the Artificial Intelligence and Data Act (AIDA): 5 key lessons." McInnes Cooper. [Online]. Available: https://www.mcinnescooper.com/publications/the-demise-of-the-artificial-intelligence-and-data-act-aida-5-key-lessons

[75] Government of Canada, 2000. *Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.* [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

[76] Government of British Columbia, 2019. *Workers Compensation Act, R.S.B.C. 2016, c. 1.* [Online]. Available: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/19001_02

[77] Government of Alberta, 2000. *Occupational Health and Safety Act, S.A. 2000, c. O-2.2.* [Online]. Available: https://canlii.ca/t/56jxc

[78] Government of Saskatchewan, 2020. *The Occupational Health and Safety Regulations, R.R.S. S-15.1, Reg. 10.* [Online]. Available: https://publications.saskatchewan.ca/#/products/111283

[79] Government of Manitoba, 2022. *Workplace Safety and Health Act and Regulation, C.C.S.M. c. W210.* [Online]. Available: https://www.gov.mb.ca/labour/safety/pdf/whs_workplace_safety_act_and_regs.pdf

[80] Government of Ontario, 1990. *Occupational Health and Safety Act, R.S.O. 1990, c. O.1.* [Online]. Available: https://www.ontario.ca/laws/statute/90o01

[81] Government of Quebec, 2002. *Act Respecting Occupational Health and Safety, R.S.Q., c. S-2.1.* [Online]. Available: https://www.legisquebec.gouv.qc.ca/fr/document/lc/s-2.1?langCont=en

[82] Government of New Brunswick, 1983. *Occupational Health and Safety Act, S.N.B. 1983, c. O-0.2.* [Online]. Available: https://laws.gnb.ca/en/document/cs/o-0.2

[83] Government of Nova Scotia, 1996. *Occupational Health and Safety Act, S.N.S. 1996, c. 7.* [Online]. Available: https://nslegislature.ca/sites/default/files/legc/statutes/occupational%20health%20and%20safety.pdf

[84] Government of Prince Edward Island, 1988. *Occupational Health and Safety Act, R.S.P.E.I. 1988, c. O-1.1.* [Online]. Available: https://www.princeedwardisland.ca/sites/default/files/legislation/o-1-01-occupational_health_and_safety_act.pdf

[85] Government of Newfoundland and Labrador, 1990. *Occupational Health and Safety Act, R.S.N.L. 1990, c. O-3.* [Online]. Available: https://www.assembly.nl.ca/legislation/sr/statutes/o03.htm

[86] Government of Yukon, 2002. *Occupational Health and Safety Act, R.S.Y. 2002, c.159.* [Online]. Available: https://laws.yukon.ca/cms/images/LEGISLATION/PRINCIPAL/2002/2002-0159/2002-0159.pdf

[87] Government of Northwest Territories, 2015. *Occupational Health and Safety Regulations, N.W.T. Reg. 039-2015.* [Online]. Available: https://www.justice.gov.nt.ca/en/files/legislation/safety/safety.r8.pdf

[88] Government of Nunavut, 2016. *Occupational Health and Safety Regulations, Nu. Reg. 003-2016.* [Online]. Available: https://www.nunavutlegislation.ca/en/consolidated-law/occupational-health-and-safety-regulations-official-consolidation

[89] Government of Canada, 1985. *Canadian Human Rights Act, R.S.C., 1985, c. H-6.* [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/h-6/

[90] Government of Canada, 1985. *Canada Labour Code, R.S.C., 1985, c. L-2.* [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/l-2/

[91] Global Affairs Canada. "Export controls." [Online]. Available: https://www.international.gc.ca/controls-controles/about-a_propos/expor/before-avant.aspx

[92] Government of Canada, 2021. *Canadian Net-Zero Emissions Accountability Act, S.C. 2021, c. 22.* [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/C-19.3

[93] L. Espina-Romero, H. Gutiérrez Hurtado, D. Ríos Parra, R. A. Vilchez Pirela, R. Talavera-Aguirre, and A. Ochoa-Díaz, "Challenges and opportunities in the implementation of AI in manufacturing: A bibliometric analysis," *Sci,* vol. 6, no. 4, 2024, Art. no. 60, https://doi.org/10.3390/sci6040060.

[94] A. Gaon and Y. Reinfeld, "The implications of the EU's new AI regulation: A comprehensive analysis for Canada," Dec. 3, 2024, https://dx.doi.org/10.2139/ssrn.4986407.

[95] Organisation for Economic Co-operation and Development, *OECD Employment Outlook 2023: Artificial Intelligence and the Labour Market.* OECD Publishing, Paris, 2023. [Online]. Available: https://doi.org/10.1787/08785bba-en

[96] EU Artificial Intelligence Act. "High-level summary of the AI Act." [Online]. Available: https://artificialintelligenceact.eu/high-level-summary

[97] J. Kelly, S. A. Zafar, L. Heidemann, J. -V. Zacchi, D. Espinoza and N. Mata, "Navigating the EU AI Act: A methodological approach to compliance for safety-critical products," *2024 IEEE Conference on Artificial Intelligence (CAI),* Singapore, Singapore, 2024, pp. 979-984. [Online]. Available: https://ieeexplore.ieee.org/document/10605271

[98] C. T. Marsden and G. Christou, "Artificially intelligent regulation: global norms, international political economy and the Brussels effect," International Conference on AI and the Digital Economy (CADE 2024), Hybrid Conference, Venice, Italy, 2024, pp. 95-97. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10700864

[99] European Union Agency for Fundamental Rights, "Data quality and artificial intelligence – Mitigating bias and error to protect fundamental rights," European Union Agency for Fundamental Rights, Vienna, Austria, 2019. [Online]. Available: https://data.europa.eu/doi/10.2811/546219

[100] Executive Office of the President, "Ensuring a national policy framework for artificial intelligence," Federal Register, vol. 90, no. 239, pp. 58499–58501, Dec. 16, 2025. [Online]. Available: https://www.federalregister.gov/documents/2025/12/16/2025-23092/ensuring-a-national-policy-framework-for-artificial-intelligence

[101] M. F. Holland, "Working smarter: How manufacturers are using artificial intelligence," National Association of Manufacturers, Washington, DC, United States, May 2024. [Online]. Available: https://nam.org/wp-content/uploads/2024/05/NAM-AI-Whitepaper-2024-1.pdf

[102] DLA Piper. "Data protection laws in China." [Online]. Available: https://www.dlapiperdataprotection.com/index.html?c=CN

[103] Y. Han, A. Ceross, and J. Bergmann, "Regulatory frameworks for AI-enabled medical device software in China: Comparative analysis and review of implications for global manufacturer," *JMIR AI,* vol. 3, no. 1, 2024, Art. no. e46871, https://doi.org/10.2196/46871.

[104] J. Lopez-Garcia and E. M. Rojas, "Barriers to AI adoption and their influence on technological advancement in the manufacturing and finance and insurance industries," in *Proc. IEEE Colombian Conference on Communications and Computing (COLCOM),* Aug. 21–23, 2024, pp. 1–6, https://doi.org/10.1109/COLCO`M62950.2024.10720309. [Online]. Available: https://ieeexplore.ieee.org/document/10720309

[105] Government of Japan, "AI strategy 2019. AI for everyone: People, industries, regions and governments," Government of Japan, Cabinet Secretariat, Tokyo, Japan, Jun. 2019. Accessed: Jun. 20, 2025. [Online]. Available: https://www8.cao.go.jp/cstp/ai/aistratagy2019en.pdf

[106] Department for Science, Innovation and Technology, "AI opportunities action plan," Department for Science, Innovation and Technology, Government of the United Kingdom, London, United Kingdom, Jan. 2025. Accessed: Jun. 20, 2025. [Online]. Available: https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

[107] *Information Technology — Artificial Intelligence – AI System Life Cycle Processes,* ISO/IEC 5338, International Organization for Standardization, Geneva, Switzerland, 2023. [Online]. Available: https://www.iso.org/standard/81118.html

[108] *Information Technology — Artificial Intelligence – Guidance for AI Applications,* ISO/IEC 5339, International Organization for Standardization, Geneva, Switzerland, 2024. [Online]. Available: https://www.iso.org/standard/81120.html

[109] *Safeguarding of Machinery,* CSA Z432, Canadian Standards Association, Toronto, ON, Canada, 2023. [Online]. Available: https://www.csagroup.org/store/product/CSA_Z432%3A23

[110] *Control of Hazardous Energy – Lockout and Other Methods,* CSA Z460, Canadian Standards Association, Toronto, ON, Canada, 2020. [Online]. Available: https://www.csagroup.org/store/product/CSA%20Z460%3A20

[111] *Occupational Health and Safety – Hazard Identification and Elimination and Risk Assessment and Control,* CSA Z1002, Canadian Standards Association, Toronto, ON, Canada, 2012. [Online]. Available: https://www.csagroup.org/store/product/CAN-CSA-Z1002-12

[112] *Occupational Health and Safety Management — Psychological Health and Safety at Work — Guidelines for Managing Psychosocial Risks,* ISO 45003, International Organization for Standardization, Geneva, Switzerland, 2021. [Online]. Available: https://www.iso.org/standard/64283.html

[113] *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements,* ISO/IEC 27001, International Organization for Standardization, Geneva, Switzerland, 2013. [Online]. Available: https://www.iso.org/standard/27001

[114] *Information Security, Cybersecurity and Privacy Protection — Guidelines for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors,* ISO/IEC 27018, International Organization for Standardization, Geneva, Switzerland, 2025. [Online]. Available: https://www.iso.org/standard/27018

[115] *Information Technology — Governance of IT — Governance Implications of the Use of Artificial Intelligence by Organizations,* ISO/IEC 38507, International Organization for Standardization, Geneva, Switzerland, 2022. [Online]. Available: https://www.iso.org/standard/56641.html

[116] *IEEE Standard for General Requirements of Online Detection Based on Machine Vision in Intelligent Manufacturing,* IEEE 2671, Institute of Electrical and Electronics Engineers, Piscataway, NJ, United States, 2022. [Online]. Available: https://standards.ieee.org/ieee/2671/7176

[117] *Artificial Intelligence — Functional Safety and AI Systems,* ISO/IEC TR 5469, International Organization for Standardization, Geneva, Switzerland, 2024. [Online]. Available: https://www.iso.org/standard/81283.html

[118] *Information Technology — Artificial Intelligence (AI) — Bias in AI Systems and AI Aided Decision Making,* ISO/IEC TR 24027, International Organization for Standardization, Geneva, Switzerland, 2021. [Online]. Available: https://www.iso.org/standard/77607.html

[119] Government of Quebec. "2022-2027 Québec strategy to support research and investment in innovation." [Online]. Available: https://www.quebec.ca/en/gouvernement/ministeres-organismes/economie/publications/2022-2027-quebec-strategy-to-support-research-and-investment-in-innovation

[120] ABGi Canada. "The new SQRI^2 Innovation strategy in Quebec." [Online]. Available: https://abgi-canada.com/en/the-new-sqri^2-innovation-strategy-in-quebec

[121] Innovation, Science and Economic Development Canada. "Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems." [Online]. Available: https://ised-isde.canada.ca/site/ised/en/voluntary-code-conduct-responsible-development-and-management-advanced-generative-ai-systems

[122] Mitacs. "Talent and research powering innovation." [Online]. Available: https://www.mitacs.ca

[123] European Commission. "Apply AI Strategy." [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/apply-ai

[124] F. Sickinghe. "The EU's Apply AI Strategy: An overly ambitious blueprint for sectoral transformation?" Bird & Bird. [Online]. Available: https://www.twobirds.com/en/insights/2025/the-eus-apply-ai-strategy-an-overly-ambitious-blueprint-for-sectoral-transformation-(1)

[125] Innovation, Science and Economic Development Canada. "Canada – European Union Digital Partnership." [Online]. Available: https://ised-isde.canada.ca/site/ised/en/canada-european-union-digital-partnership

[126] United Nations Educational, Scientific and Cultural Organization. Ethics of artificial intelligence: The Recommendation." [Online]. Available: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

[127] *Risk Management — Guidelines,* ISO 31000, International Organization for Standardization, Geneva, Switzerland, 2018. [Online]. Available: https://www.iso.org/standard/65694.html

[128] H. M. Ahmad, A. Rahimi, and K. Hayat, "Deep learning transforming the manufacturing industry: A case study," in Proc. *IEEE HPCC/DSS/SmartCity/DependSys,* Haikou, Hainan, China, Dec. 20–22, 2021, pp. 1286–1291, https://doi.ieeecomputersociety.org/10.1109/HPCC-DSS-SmartCity-DependSys53884.2021.00196.

[129] S. Abdulnour, C. Baril, G. Abdulnour, and S. Gamache, "Implementation of Industry 4.0 principles and tools: Simulation and case study in a manufacturing SME," *Sustainability,* vol. 14, no. 10, 2022, Art. no. 6336, https://doi.org/10.3390/su14106336.

[130] F. Longo, A. Nervoso, L. Nicoletti, V. Solina, and A. O. Solis, "Modeling & simulation for assessing production policies: A real case study from a manufacturing company in Canada," *Procedia Comput. Sci.,* vol. 232, pp. 1192–1200, 2024, https://doi.org/10.1016/j.procs.2024.01.117.

[131] T. C. Callari, R. V. Segate, E.-M. Hubbard, A. Daley, and N. Lohse, "An ethical framework for human-robot collaboration for the future people-centric manufacturing: A collaborative endeavour with European subject-matter experts in ethics," *Technol. Soc.,* vol. 78, 2024, Art. no. 102680, https://doi.org/10.1016/j.techsoc.2024.102680.

[132] R. Agrawal, A. Majumdar, A. Kumar, and S. Luthra, "Integration of artificial intelligence in sustainable manufacturing: Current status and future opportunities," *Oper. Manag. Res.,* vol. 16, pp. 1720–1741, 2023, https://doi.org/10.1007/s12063-023-00383-y.

[133] J. M. Rožanec et al., "Predicting operators' fatigue in a human in the artificial intelligence loop for defect detection in manufacturing," *IFAC-Pap.,* vol. 56, no. 2, pp. 7609–7614, 2023, https://doi.org/10.1016/j.ifacol.2023.10.1157.

[134] Aster Cloud. "Toyota shifts into overdrive: Developing an AI platform for enhanced manufacturing efficiency," [Online]. Available: https://aster.cloud/2024/12/10/toyota-shifts-into-overdrive-developing-an-ai-platform-for-enhanced-manufacturing-efficiency

[135] E. Bendoly, A. Chandrasekaran, M. R. F. Lima, R. Handfield, S.H. Khajavi, and S. Roscoe, "The role of generative design and additive manufacturing capabilities in developing human–AI symbiosis: Evidence from multiple case studies," *Decis. Sci.,* vol. 55, no. 4, pp. 325–345, 2024, https://doi.org/10.1111/deci.12619.

[136] K. Skrzek, E. Mazgajczyk, and B. Dybała, "Application of fuzzy logic-based expert advisory systems in optimizing the decision-making process for material selection in additive manufacturing," *Materials,* vol. 18, no. 2, 2025, Art. no. 324, https://doi.org/10.3390/ma18020324.

[137] P. Bougault, R. A. El Haddad, and L. Ma, "Industrial Applications of AI in Aircraft Manufacturing: A PRISMA Systematic Literature Review," *Research Square,* 2024. [Online]. Available: https://doi.org/10.21203/rs.3.rs-6199323/v1

[138] M. Eugeni et al., "An Industry 4.0 approach to large-scale production of satellite constellations: The Case study of composite sandwich panel manufacturing," *Acta Astronaut.,* vol. 192, pp. 276–290, 2022, https://doi.org/10.1016/j.actaastro.2021.12.039.

[139] A. B. Pazhayattil and G. Konyu-Fogel, "An empirical study to accelerate machine learning and artificial intelligence adoption in pharmaceutical manufacturing organizations," *Journal of Generic Medicines,* vol. 19, no. 2, pp. 81–91, 2023, https://doi.org/10.1177/17411343221151109.

[140] D. R. Domínguez, M. B. Infante Abreu, and A. L. Parv, "Main trend topics on Industry 4.0 in the manufacturing sector: A bibliometric review," *Appl. Sci.,* vol. 14, no. 15, 2024, Art. no. 6450, https://doi.org/10.3390/app14156450.

Appendix A—Interview Protocol

1. What is your name?
2. What is your current job title or role?
3. How many years of experience do you have in manufacturing and/or AI-related work?
4. How involved are you in decisions related to AI in your organization?
5. What is your primary area of expertise?
6. What organization do you work for?
7. Which industry sector best describes your organization?
8. What is the primary country your company operates in?
9. How many employees does your company have?
10. At what stage of AI adoption is your organization currently?
11. What types of AI applications are currently in use in your organization?
12. How integrated is AI into your production or operations?
13. **A.** This first question pertains to AI adoption and applications. From your perspective, how is AI currently being used in your organization's manufacturing work, and what kinds of systems have you personally worked with or observed?

    B. What influenced your organization's decision to explore or adopt AI, and how were you personally involved or impacted during that stage?
14. **A.** What kinds of risks have you encountered or considered in relation to using AI in your work or within your organization's manufacturing operations?

    B. How have you seen those risks managed or assessed in your context—either formally or informally?
15. **A.** Have you experienced or become aware of any cybersecurity or operational challenges related to AI systems in your work environment?

    B. From your experience, how has AI affected safety, production workflows, or efficiency in your area of work?
16. **A.** In your experience, how have existing standards or regulations shaped the way AI is used in your organization's manufacturing practices?

    B. Are there any gaps, limitations, or grey areas in policy or standards that you've noticed while working with or around AI systems?

17. **A.** How has the use of AI affected your role or the roles of others around you in the organization?

    B. Have you noticed any changes in how people feel about their work, decision-making, or accountability as AI has been integrated?

18. **A.** Looking ahead, what AI advancements do you think will have the most impact on manufacturing—from your point of view?

    B. What advice, lessons, or insights would you share based on your own experience working with AI in manufacturing so far?

19. Is there anything else related to AI adoption in manufacturing that you would like to share?

CSA Group Research

In order to encourage the use of consensus-based standards solutions to promote safety and encourage innovation, CSA Group supports and conducts research in areas that address new or emerging industries, as well as topics and issues that impact a broad base of current and potential stakeholders. The output of our research programs will support the development of future standards solutions, provide interim guidance to industries on the development and adoption of new technologies, and help to demonstrate our on-going commitment to building a better, safer, more sustainable world.

CSA GROUP™

© 2026 Canadian Standards Association. All Rights Reserved.