Opportunities to Enhance Detection of Insider Risk Using Artificial Intelligence in Canada's Manufacturing Sector

By

Edie Brenning

Drafted April 2025

Table of Contents

Disclaimer

1) The author possesses relevant professional experience in some areas of the subject matter discussed in this research paper. Some of the content, conclusions, and interpretations presented are based on the author's prior knowledge and practical experience in the field, alongside existing literature and research. While every effort has been made to ensure accuracy, the views and interpretations are influenced by the author's personal background and experience.
2) Commercial products are identified to adequately specify certain procedures or outline examples of how certain AI systems can be applied in real world application. In no such case does identification imply recommendation or endorsement by Carleton University, or the author, nor does it imply that the identified products are necessarily the best available for the purpose.

Abstract

Canada's manufacturing sector plays a crucial role in Canada’s national security and economic stability. However, the increasing complexity of industrial processes and digital transformation exposes this sector to insider risks. These risks, ranging from intellectual property theft to sabotage of industrial controls systems, can have devastating consequences on an organization and can affect Canada’s resiliency to recover from incidents and disruption. Traditional security measures in manufacturing environments may fail to detect nuanced, evolving insider risks by overlooking or rationalizing problematic activities. Artificial Intelligence (AI) presents a transformative solution by enhancing detection of insider risk activity, leveraging AI systems to enable quicker response by utilizing machine learning and deep learning algorithms. This research paper aims to explore how prevalent insider risks are in Canada’s manufacturing sector, how the sector is presently leveraging AI systems in operations and identify opportunities and challenges in using AI-driven technologies to detect insider risk activity in Canada’s manufacturing sector.

Research Questions

This academic paper is based on the following research questions:

a) **How prevalent is insider risk in Canada's manufacturing sector?**

b) **What AI technologies are best suited for detecting insider risk activity in a manufacturing environment?**

c) **What are some challenges and considerations of utilizing AI for insider risk detection in manufacturing?**

Research Thesis

The introductory portion of this academic paper will identify what Canada defines as critical infrastructure, what the present national strategy is for critical infrastructure sectors, how risk management is embedded within the strategy, and how the manufacturing sector enhances Canada's resiliency in response to domestic and foreign threats.

The first part of the paper will provide an overview of what leading domestic and international security agencies are producing in the form of assessments and guides related to insider risks awareness and insider risk management. Part I will also explore the various types of manufacturing insider risk threat vectors and possible impact scenarios that could occur resulting in damage to organizational health and Canadian national security by default. The final section in Part I will outline a real-world case study of an insider risk incident in the U.S. manufacturing sector and examine the incident itself, outcomes and further impacts.

The second part of the paper will review published reports and guidelines issued by the Canadian Centre of Cyber Security and other leading Canadian agencies on the use of AI tools which include considerations and implementation strategies. Furthermore, concepts from research literature will be provided outlining the effectiveness of AI tools, distinct characteristics of AI subsets and an analysis of specific types in detecting insider risk patterns. They will then

be compared against manufacturing environments and application models evaluated in the Canadian manufacturing sector. In addition, this section will explore what modern day AI tools are accessible in the market that can be integrated into security technology systems and industrial control systems to alert security resources and facilitate quick intervention. Lastly, Part II will explore the importance of customization to manufacturing environments as part of a quick and efficient response strategy.

The third part of the paper will explore challenges and considerations of leveraging AI tools to detect insider risks such as bias, discrimination in training data, organizational challenges and job market impacts. By referencing Canadian population statistical information with respect to the usability of AI in work environments, an assessment will be made regarding its effects on Canadian manufacturing environments now and in the future. Additionally, by reviewing insider risk academic and technical resources, considerations will be brought forward with how implementing AI tools in a manufacturing environment may improve detection and enhance response capability. Additionally, Part III will provide insight into available tools that have been developed and published for organizations to combat insider risk challenges.

The final section of the paper will outline the research conclusions, which will include an examination on if the research supports the use of AI tools in manufacturing environments and their effectiveness in detecting insider risk activity. The final section will also highlight other developing research in the area, providing an overview of new academic and government initiatives such as the Insider Threat Alliance Project. In addition, a list of practical recommendations will be provided for organizations outlining opportunities and considerations if selecting AI-tools and provide responses to the research questions.

Research Overview: Manufacturing in the Context of Canadian CI

Canada's National Strategy for Critical Infrastructure & Risk Management

As defined by Public Safety Canada, Critical infrastructure (CI) refers to the processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government.[1] Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders.[2] Disruptions of critical infrastructure could result in catastrophic loss of life, adverse economic effects, and significant harm to public confidence.[3] There are 3 strategic objectives set out by Public Safety Canda in the *National Strategy for Critical Infrastructure*.[4] They are 1) to build partnerships, 2) to implement an all-hazards risk management approach and 3) advance the timely sharing and protection of information among partners.[5]

The National Strategy for Critical Infrastructure supports the principle that roles and activities should be carried out in a responsible manner at all levels of society in Canada.[6] Responsibilities for critical infrastructure in Canada are shared by federal, provincial and territorial governments and local authorities, and critical infrastructure owners have primary responsibility for protecting their assets and services.[7] The National Strategy is based on the recognition that enhancing the resiliency of critical infrastructure can be achieved through the

---

[1] Public Safety Canada, (21 July 2022) "National Strategy for Critical Infrastructure" online:
< https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx.>

[2] *Ibid.*
[3] *Ibid.*
[4] *Ibid.*
[5] *Ibid.*
[6] *Ibid.*
[7] *Ibid.*

appropriate combination of security measures to address intentional and accidental incidents, business continuity practices to deal with disruptions and ensure the continuation of essential services, and emergency management planning to ensure adequate response procedures are in place to deal with unforeseen disruptions and natural disasters.[8]

Furthermore, the second strategic objective of the Strategy outlines *to implement an all-hazards approach to Risk Management,* it outlines *the continuous, proactive and systematic process to understand, manage and communicate risks, threats, vulnerabilities and interdependencies across the critical infrastructure communities*.[9] Within the scope of this definition, critical infrastructure partners conduct an all-hazards risk analyses which takes into account accidental, intentional and natural hazards in the organization.[10] Within this risk management objective, it is an important consideration for corporate security departments and security personnel in critical infrastructure sectors to understand the risk landscape as part of departmental risk management plans, so as to strengthen the organization's resiliency and decrease its vulnerability to a security incident which may cause significant injury from short to long term.

Canadian government agencies play a significant role in ensuring security and resiliency of critical infrastructure sectors, such as manufacturing. Some examples of this include the Canadian Cyber Security Center, which establishes strategic partnerships with Canada's critical infrastructure owners and operators to share enhanced cyber threat information and to promote the integration of cyber defense technology.[11] In addition, Public Safety Canada, promotes risk

---

[8] *Supra* note 1.
[9] *Supra* note 1.
[10] *Supra* note 1.
[11] Canadian Centre for Cyber Security (Accessed Feb 2, 2025) Industry Collaboration. online: https://www.cyber.gc.ca/en/about-cyber-centre/industry-collaboration

management frameworks among critical infrastructure sectors, that can be applied to the manufacturing sector; and programs within Innovations, Science and Development Canada (ISED) which fund research into advanced and resilience manufacturing.[12]

Manufacturing as a Critical Infrastructure Sector

Manufacturing is one of Canada's most important economic sectors, employing 1.7 million people in a wide range of industries across the country.[13] This sector provides goods that are vital to other industries, government operations, and overall well-being of Canadians, such as defense equipment, medical supplies and critical technologies.[14] Accounting for approximately $174 billion of Canada's GDP, manufacturing represents more than 10% of Canada's total GDP.[15] Canada's manufacturing sector has stand-alone enterprises, but also has interdependencies with a wide range of other sectors, including transportation systems, energy, chemical and water.[16]

Manufacturing is identified by Public Safety Canada as one of ten critical infrastructure sectors and is part of the broader industrial sector in Canada[17], with membership that includes private sector organizations and government agencies (federal, provincial and territorial). [18]

[12] Innovation, Science and Economic Development Canada, (12 October 2021) "Canadian Manufacturing Sector Gateway" online: https://ised-isde.canada.ca/site/canadian-manufacturing-sector-gateway/en
[13] *Ibid.*
[14] *Ibid.*
[15] *Ibid.*
[16] *Ibid.*
[17] Public Safety Canada, (21 July 2022) "National Strategy for Critical Infrastructure" online: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx.
[18] *Ibid.*

Canadian Critical Infrastructure Sectors

- *Energy & Utilities*
- *Finance*
- *Food*
- *Transportation*
- *Government*
- *Information & Communication Technology*
- *Health*
- *Water*
- *Safety*
- ***Manufacturing***

(Public Safety Canada, 2019)

Manufacturers in the sector process raw materials and primary metals, produce engines, turbines, and power transmission equipment, produce electrical equipment and components, and manufacture cars, trucks, commercial ships, aircraft, rail cars, and their supporting components.[19] Since manufacturing industries are interconnected to many other critical infrastructure sectors, failure or disruption in the manufacturing sector could result in cascading disruptions to other critical infrastructure sectors in multiple regions.[20]

Manufacturing sector assets are privately owned and operated and include manufacturing facilities, processing and distribution facilities, sales offices, corporate headquarters, and product storage.[21]

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) identifies five industries within the critical manufacturing sector that serve as core components.[22] They are

[19] Cybersecurity & Infrastructure Security Agency (June 2023) Introduction to the Critical Manufacturing Sector Risk Management Agency. Online: https://www.cisa.gov/sites/default/files/2024-06/Critical%20Manufacturing%20SRMA%20Fact%20Sheet%20New%20Template%202June2023_FINAL_508c.pdf

[20] *Ibid.*

[21] *Ibid.*

[22] Cyber Security & Infrastructure Security Agency, "Critical Manufacturing Sector" online: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector

metals manufacturing, machinery manufacturing, electrical equipment, appliance, and component manufacturing and transportation equipment manufacturing. [23]

Unlike the U.S., Canada does not formally identify core components within the manufacturing sector. However, the Government of Canada has published reports outlining importance of the manufacturing sector in support of its strategic priorities. An example of this would be the document "*The Canadian Critical Minerals Strategy*" published by Natural Resources Canada. The report outlines Canada's vision to increase the supply of responsibly sourced critical minerals to support the development of domestic and global value chains for the green and digital economy.[24] The Strategy is a key pillar in achieving Canada's goal of a net-zero future and an important opportunity in sourcing critical minerals and manufacturing products they go into.[25] Strategies such as this demonstrate the critical importance that manufacturing has on Canada's economy and economic sustainability. Additionally, it demonstrates that Canada's manufacturing sector will be instrumental to increase Canada's trade opportunities with other countries as it positions itself as a leader in sustainability, global security and enhances partnership with allies.[26]

To ensure efficiency in production and to support supply chains, the manufacturing sector requires constant innovation, integration of new ideas and the adoption of up-to-date risk mitigation processes. The highly competitive nature of the global economy and the growing complexity of manufacturing supply chains will further increase the importance of protection

---

[23] *Supra* note 22.
[24] Natural Resources Canada (2022) The Canadian Critical Minerals Strategy. online: https://www.canada.ca/en/campaign/critical-minerals-in-canada/canadian-critical-minerals-strategy.html#a2
[25] *Ibid.*
[26] *Ibid.*

methods and the development and diffusion of new technologies moving forward.[27] Canadian manufacturers have long been leaders in research, investment in progressive technologies and transformation through their ability to raise capital through financial markets, unlike government agencies. This makes them ideal environments for the testing of new digital and technological tools on the market to enhance enterprise functions.

Findings and Analysis: Insider Risk Awareness, Manufacturing Threat Vectors & AI Potential

Part I. Insider Risk Awareness in Canadian and U.S. Manufacturing

a) Defining Insider Risk in Manufacturing

In recent decades, due to publicized incidents, organizations have varying degrees of understanding of the damages caused by insider risk incidents. Depending on the severity, they can cause impacts to small, medium, and large-scale operations. Specifically, with the rise of social media, online platforms and large migrations of data, the evolution of digital environments is advancing at a rapid pace. The shift to a digital world has not been without its challenges, which come in the form of increased vulnerabilities in some instances while striving for improved efficiency and interconnectedness. As Canada's critical infrastructure sectors adapt to an increasingly digital world, there is a heightened sense of social pressure to stay up to date with other global powerhouses when it comes to technology and innovation. While the digital race has advanced far beyond what some expected, Canadian government agencies have adopted a "controlled progression" approach to ensure advancements in technology do not compromise Canada's security posture, resiliency, consumer protections or human rights legislation.

[27] OECD (29 May 2007) Staying Competitive in the Global Economy: Moving Up the Value Chain. Online: https://www.oecd.org/en/publications/staying-competitive-in-the-global-economy_9789264034259-en.html.

While advancements in technologies have been both advantageous to critical infrastructure sectors, such as manufacturing, it has also increased their vulnerability in certain areas depending on the organization, processes and procedures related to their services. Advanced technological systems which improve efficiency and productivity in most people's everyday lives, may increase the likelihood for people to develop dependencies on technology to improve productivity or reduce the burden of manual tasks. This may be especially the case in a workforce like manufacturing, given there are often routine, manual work tasks, which could lead to vulnerabilities such as overlooked anomalies, deterioration of focus, or ignorance of "red flags" that can leave an organization susceptible to among other things, insider and external risks.

The Canadian Security Intelligence Service (CSIS) defines insider threat as **"**an individual who either wittingly or unwittingly exploits, or intends to exploit, their legitimate access to the assets of a department of the Government of Canada causing harm to Canada's national interest through espionage, terrorism, unauthorized disclosure of information, or loss or degradation of a capability to deliver a service or a product".[28] In recent years, there has been a shift in terminology from "insider threat" to "insider risk" in Canadian and U.S. government discourse to reflect a broader, more nuanced understanding of security challenges involved with internal personnel. This evolution indicates that not all activities by insiders are malicious or intentional, and some may occur from negligence that can still cause significant impacts. In referring to insider risk specifically, CSIS outlines a concept called the "critical path model" in describing the escalation of a person from normal behavior to abnormal insider risk activity. The

[28] Canadian Security Intelligence Service (2023) Insider Risk/Insider Threat presentation. Accessed online: https://gccollab.ca/file/view/19080185/insider-risk-insider-threat.

model suggests that personnel with pre-dispositions or vulnerabilities with the addition of stressors causes unwanted behaviours.[29] These behaviors are then not responded to appropriately by organizations which leads to hostile acts.[30] Indicators play an important role in detecting insider risk as no single indicator should be taken as confirmation of insider risk activity.[31] In most known cases, multiple indicators have been present.[32]

As one of the leading agencies for insider risk guidance and resilience in Canada, Public Safety Canada has published various reports on protecting critical infrastructure and enhancing resilience efforts around insider risks in Canada's critical infrastructure sectors. In the guide *Enhancing Canada's Critical Infrastructure Resilience to Insider Risk,* Public Safety Canada outlines 3 themes and 8 security actions to enhance insider risk resiliency.[33]

Among the 8 are 2 key actions where the advancement of technology could support some of the objectives outlined in each action. 1) Providing training, **raising awareness** and conducting exercises; and 2) **monitoring, responding and mitigating unusual behaviour**.[34] Within the actions are subsets of activities which can be directly linked to the concepts of insider risk detection and as emphasized on the following page.

---

[29] Canadian Security Intelligence Service (2023) Insider Risk/Insider Threat presentation. Accessed online: https://gccollab.ca/file/view/19080185/insider-risk-insider-threat
[30] *Ibid.*
[31] *Ibid.*
[32] *Ibid.*
[33] Public Safety Canada, (2019) "Enhancing Canada's Infrastructure Resilience to Insider Risk online: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/nhncng-crtcl-nfrstrctr-en.pdf
[34] *Ibid.*

Security Action #5: Provide Training, Raise Awareness and Conduct Exercises

- *Develop a security training program for all employees;*
- ***Raise awareness of indicators of potential security concerns**;*
- *Provide access to employee assistance programs to help prevent employees from becoming at risk of compromise;*
- *Develop and promote a culture of security vigilance by encouraging employees to say something if they see something;*
- *Conduct periodic exercises to test the security posture within an organization.*

(Public Safety Canada, 2022)[35]

Security Action #7: Monitor, respond to and Mitigate Unusual Behaviour

- *Establish a means of monitoring physical and network access from all endpoints and remote devices;*
- *Develop a culture that enhances employee awareness of security and **reporting suspicious activity or abnormal behaviour;***
- *Raise awareness of the potential risks associated with social media sites;*
- *Limit remote access to non-critical assets and systems where possible;*
- ***Establish protocols to report, track and respond to unusual incidents; and***
- *Consider engaging the security and intelligence community, including the RCMP or CSIS.*

(Public Safety Canada, 2022)[36]

Raising awareness of indicators of potential security concerns, reporting suspicious activity or abnormal behavior and establishing protocols to report, track and respond to these incidents are aligned with the fundamental program elements of detecting insider risk, according to Public Safety Canada.[37] By incorporating these actions within an organization, will greatly enhance its ability to mitigate insider risk incidents and demonstrate its commitment to protecting its critical processes.[38]

As organizations aim to manage insider risk with the advancements of technology, the report remains relevant today. The challenge continues to be the "how" in many of the outlined

[35] *Supra* note 34.
[36] *Supra* note 34.
[37] *Supra* note 34.
[38] *Supra* note 34.

objectives, which will require a shift away from conventional thinking or historical practices that may be outdated or ineffective. With operational environments becoming increasingly digital, manufacturers must identify and consider deploying digital tools to combat vulnerabilities within their systems that may be susceptible to known or unknown risks.

b) Insider Risk Threat Vectors in Manufacturing

Critical manufacturing environments are fundamentally different depending on their products and services. However, there are many similarities that can be found from one enterprise to another. Typically, they have core manufacturing processes that leverage systems and technology in their operations, they apply supply chain and inventory management principles, and they have a workforce.[39] As with most enterprises, their focus is to maximize revenue, reduce production costs and expand market presence. As a result, their risk profiles have similarities as well, with most protection efforts around critical assets, data and processes. These what are commonly referred to in an organization as the "crown jewels". Crown jewels are essential to organizational success, health and survival. Their compromise or disruption could cause significant financial loss, reputational damage, or operational failure. Therefore, ensuring adequate safeguards to deter, detect and respond to insider risks which could affect them is critical. In the manufacturing sector, crown jewels may be in the form of intellectual property, supply chains and vendor information, manufacturing processes, physical or digital assets.

Manufacturing environments by their nature still have a need for physical facilities to produce goods, even post pandemic where many businesses enabled remote work.[40] Therefore, physical assets and facilities are still extremely relevant. As a result, manufacturers may be

[39] Next Generation Manufacturing Canada (24 January 2025) A Proactive approach to cybersecurity in advanced manufacturing. online: https://www.canadianmetalworking.com/canadianfabricatingandwelding/article/automationsoftware/a-proactive-approach-to-cybersecurity-in-advanced-manufacturing
[40] *Ibid.*

exposed to multiple insider risk threat vectors despite being more connected and reliant on networked communications as opposed to decades prior. These threat vectors may come in the form of theft of intellectual property, sabotage of industrial control systems, unauthorized access and privilege abuse, third party risks, or negligence of security policy compliance, all of which, if executed, could cause significant disruption to operations, cause financial harm in the form of dollar loss and/or incur reputational damage as a result of loss in consumer trust.

In 2019, the U.S.'s Cyber Security & Infrastructure Security Agency (CISA) published an implementation guide, unique to the manufacturing sector, titled *Insider Threat Programs for the Critical Manufacturing Sector*.[41] The guide has 4 major components from understanding what insider risk is, to establishing an insider risk program, risk management strategy and provides program resources.[42] The implementation guide also lists various threat vectors and potential consequences that insiders can pose to the manufacturing sector. Specifically, *major disruption in manufacturing operations including malicious acts committed by insiders such as fraud, theft, sabotage, workplace violence, and more.[43] Unwitting insiders may inadvertently disclose proprietary or other sensitive information, unknowingly download malware, or facilitate other cybersecurity events.[44] The critical manufacturing sector reports the highest number of attacks on industrial control systems of any critical infrastructure sector.[45]*

Furthermore, the guide outlines an emphasis to implement risk management strategies that identify the assets or resources to be protected, identify potential threats, determine

---

[41] Cyber Security & Infrastructure Security Agency (August 2019) "Insider Threat Programs for the Critical Manufacturing Sector" Implementation Guide. online: https://www.nationalinsiderthreatsig.org/itrmresources/CISA%202019%20Insider%20Threats%20Programs%20For%20The%20Critical%20Manufacturing%20Sector%20Implementation%20Guide.pdf

[42] *Ibid.*

[43] *Ibid.*

[44] *Ibid.*

[45] *Ibid.*

vulnerabilities, assess risk, and deploy countermeasures.[46] Referring to the establishment of an insider risk program, the guide emphasizes the importance to taking proactive measures to detect, detect, mitigate and report the threats.[47] Also, that organizational insider risk programs should identify anomalous behaviours that may indicate an individual poses a risk.[48]

One observation that was noted in the research is that both Public Safety Canada and CISA have published guides for insider risk management, which are *Enhancing Canada's Critical Infrastructure Against Insider Risks*[49]*, and* CISA's *Insider Threat Mitigation Guide*,[50] CISA published a **specific** implementation guide for insider threat programs for the critical manufacturing sector.[51] It is the only sector out of the 16 identified critical infrastructure sectors that has a specific document pertaining to the development of insider threat programs that is publicly available.[52] The majority of other critical infrastructure sectors identified by CISA have sector-specific infrastructure protection plans, under their overarching risk management framework and in some instances are accompanied by a risk management agency fact sheet, specific to the sector.[53]

---

[46] *Supra* note 41
[47] *Supra* note 41.
[48] *Supra* note 41.
[49] *Supra* note 33.
[50] Cyber Security & Infrastructure Security Agency (Novermber 2020) Insider Threat Mitigation Guide. Online: https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide
[51] *Supra* note 41
[52] *Supra* note 41.
[53] Cyber Security & Infrastructure Security Agency (Accessed March 5, 2025) Critical Infrastructure Sectors. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Determining the exact number of Canadian manufacturers with insider risk programs is challenging due to limited publicly available data. However, a report published by the Conference Board of Canada in 2018 revealed that only 18% of Canadian organizations who participated in a survey (267) had a formal definition of insider risk, an increase from 13% in 2012.[54] Furthermore, the report suggests the cause of this to be that Canadian organizations lack understanding around what constitutes insider risk leaving them vulnerable to harm.[55] The report contributes the findings to increase in size and complexity of information technology, integration of personal electronic devices in the workplace, complex supply chains, and a lack of training and awareness.[56] The report outlined these as issues contributing to the challenge of identifying and addressing insider threats.[57]

Within the same survey, when asked if roles and responsibilities for managing insider threats are defined in their organization, 73.5% of responded replied "yes" in 2012.[58] In 2017, just 46.4% indicated the same, representing a 27.1% decrease.[59] At the same time, over 40% of respondents said they have received no insider threat training.[60] The findings are important to consider as the future of insider risk program development in the context of Canadian manufacturing and Canadian organizations as a whole.

While there are limited known insider risk incidents that are publicized in Canadian manufacturing, according to IBM's *Cost of Insider Threats: Global Report*, the incidence of

---

[54] Conference Board of Canada (October 29, 2018) The Insider Threat: Majority of Canadian Organizations Still Unclear on What It Means. Online: https://www.newswire.ca/news-releases/the-insider-threat-majority-of-canadian-organizations-still-unclear-on-what-it-means-698885751.html
[55] *Ibid.*
[56] *Ibid.*
[57] *Ibid.*
[58] *Ibid.*
[59] *Ibid.*
[60] *Ibid.*

insider risk events more than tripled from 2016 to 2020 in U.S.[61] In addition, criminal insider was listed as number two in both of the categories **top causes** and **top costs** after negligence within the report.[62] There are numerous historical known incidents of insider risk that have occurred in the U.S.'s critical manufacturing sector. One of which is explored in the case study below.

c) **Case Study**: 2020 General Electric Trade Secret Theft - Schenectady, New York

Overview: In 2020, an employee of General Electric (manufacturing & energy industry) stole trade secrets over several years and attempted to create a competing business with information obtained.[63]

Incident: The employee *Xiaoqing Zheng*, stole thousands of files containing sensitive information, such as engineering specs, drawings, design blueprints with the intention of benefitting a Chinese based company, which he had been involved in.[64]

Outcome: In 2018, Zheng was arrested by the FBI after investigators found stolen GE files on his electronic devices.[65] He was charged with economic espionage and theft of trade secrets.[66]In 2020, he was found guilty of conspiracy to steal trade secrets, and in 2022 was sentenced to two years in prison and required to pay a fine.[67]

---

[61] Ponemon Institute (2020) 2020 Cost of Insider Breach Report. online: https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/
[62] *Ibid.*
[63] U.S. Department of Justice Archives (1 April 2022) Former GE Power Engineer Convicted of Conspiracy to Commit Economic Espionage. Online: https://www.justice.gov/archives/opa/pr/former-ge-power-engineer-convicted-conspiracy-commit-economic-espionage
[64] Fox Business (4 January 2023) Former GE employee sentenced for conspiring to steal trade secret for China. online: https://www.foxbusiness.com/politics/former-ge-employee-sentenced-conspiring-steal-trade-secrets-china
[65] *Supra* note 63.
[66] *Supra* note 63.
[67] *Supra* note 63.

Impact: While the exact loss amount was not disclosed publicly, stolen technology is estimated to cost GE billions in loss of competitive advantage. In addition, the incident caused minor reputational damage and heightened the importance of strengthening insider risk detection.[68]

As both Canada and the U.S. security agencies emphasize that insider risks pose a threat to critical infrastructure, Canada does not provide a specific insider risk program implementation guide for the manufacturing sector. One contributing factor may be that there are more known insider risk incidents publicized in U.S. manufacturing versus those in Canada. Some attributes may be the large differential in population size and size differential of manufacturing sectors, or that the U.S. and CISA have established a greater need to support this critical sector to provide specific resource material to detect and identify insider risks in manufacturing environments. Another consideration is that the U.S. has far more competitors globally in sectors such as manufacturing, perhaps making it a more attractive target to impact or disrupt as one of the worlds superpowers.

Despite not having a manufacturing-specific insider risk program guide, the Communications Security Establishment Canadian Centre for Cyber Security published the *National Cyber Threat Assessment (NCTA) 2023-2024*[69] which outlined that critical infrastructure is increasingly at risk from cyber threat activities.[70] While the assessment does not associate cyber threats with insider risk activity specifically, it does outline correlations between critical infrastructure operational technology and the importance of protecting operational technology from threat actors. The assessment states that *the opportunities for critical*

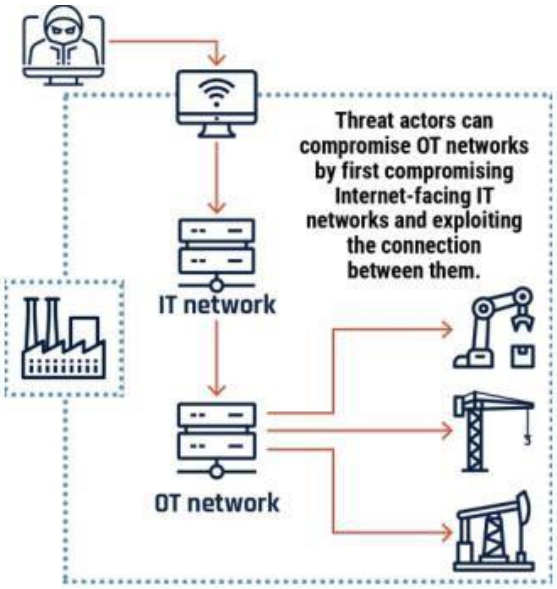
---

[68] Infosecurity Magazine Article (4 January 2023) General Electric Insider Handed Two Years for IP Theft. online: https://www.infosecurity-magazine.com/news/general-electric-insider-two-years.

[69] Communications Security Establishment (28 October 2022) Canadian Centre for Cyber Security: National Cyber Threat Assessment 2023-2024. Online: National cyber threat assessment 202https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf3–2024.

[70] *Ibid.*

infrastructure disruption expand as operators increasingly expose the operational technology (OT) underpinning industrial processes to the Internet. Internet-connected OT increases the threat surface of the organizations that employ it and increases the opportunity for cyber threat activity to have effects in the physical world.[71] The report describes how OT, which is used to control and monitor physical processes, is increasingly being connected to information technology (IT) by industry and critical infrastructure providers.[72] Connected, or smart, OT increases process efficiency through improved data exchange, centralized management, and automation.[73] In relation to the manufacturing sector, there are specific inferences that can be drawn from the 2023-2024 report that are still extremely relatable to today's manufacturing environments and that insiders could compromise OT networks via IT networks, by exploiting or manipulating the systems that are located on them.[74]



(NCTA 2023-2024, CSE)

[71] *Supra* note 69.
[72] *Supra* note 69.
[73] *Supra* note 69.
[74] *Supra* note 69.

It should be noted that in the Communications Security Establishments' most recent assessment, *NCTA 2025-2026*, OT systems are not referenced as continuously or increasingly being exposed to cyber threat activity or other risks caused by external or internal actors.[75]

Part II. Materializing Artificial Intelligence (AI) for Insider Risk Detection in Manufacturing Environments

a) Traditional Measures of Insider Risk Detection in Canadian Manufacturing

Within Canada's manufacturing sector, it is not uncommon for larger corporations to have an established corporate security department. While they vary in size internally or are outsourced completely, organizations may have acquired the need to leverage security tools within their business at some point in their history. A Canadian leading manufacturer, Imperial Oil, based out of Calgary, Alberta, has established just that, a well-structured corporate security division as part of its operating model. Under their corporate security division and product safety platform, Imperial Oil emphasizes the need to ensure product safety, workplace safety, and cybersecurity.[76] In addition, Imperial Oil's corporate security department outlines its commitment to install robust security measures which are designed to protect personnel and facilities from operational threats and cybersecurity attacks.[77] As such, Imperial Oil and manufacturing corporations alike demonstrate investment in corporate security departments to mitigate various types of risk including such as safety, external and insider risk.

Corporate security in collaboration with other departments are responsible for implementing traditional security controls in manufacturing environments may include access control systems, security personnel resources, video management systems, security infrastructure

---

[75] Communications Security Establishment (28 October 2022) Canadian Centre for Cyber Security: National Cyber Threat Assessment 2025-2026. Online: https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf
[76] Imperial Oil Article (2025) Safety. Accessed online: https://www.imperialoil.ca/sustainability/people/safety#Performance
[77] *Ibid.*

and cybersecurity protections among others. As corporate security departments across multiple critical infrastructure sectors explore new technology available on the market to mitigate risks, emerging AI technology is drawing attention to improve detection capacity while allowing more efficient use of human resources to focus on more important tasks.

b) Overview of AI and AI Subfields

According to the Government of Canada's *Directive on Automated Decision-Making*, published by the Treasury Board of Canada Secretariat (TBS), there are many different definitions of AI.[78] The Organization for Economic Co-operation and Development, (OECD) defines an AI system as:

> *A machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.*[79]

AI systems include both **knowledge-based systems** that use a combination of domain knowledge, rules, facts, and relationships curated by human experts, and **machine learning (ML) systems** that can learn from data and generalize it to perform tasks without explicit instructions.[80] When it comes to detecting anomalies and patterns with potential for insider risk, this requires amassing diverse data sets and finding ways to correlate anomalies so as to identify outliers. Therefore, machine learning AI systems have greater potential than knowledge-based

---

[78] Treasury Board of Canada Secretariat (25 April 2023) Directive on Automated Decision-Making. online: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

[79] OECD (5 March 2024) Explanatory memorandum on the updated OECD definition of an AI system. online: https://www.oecd.org/en/publications/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.html

[80] Government of Canada (4 March 2025) AI Strategy for the Federal Public Service 2025-2027: Overview. online: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/gc-ai-strategy-overview.html

systems for detection of this nature, as machine learning tools are trained through specific data sets, which they then leverage to detect patterns or anomalies that do not align with what they have been trained on. Furthermore, machine learning (specifically deep learning) uses the ability of computers to identify patterns, learn from data, and make inferences or decisions, without having been explicitly programmed to do so.[81] Deep learning (machine learning subset) involves training algorithms on large datasets that must be sourced to identify patterns and relationships. These patterns are then used to make predictions or decisions about new data.[82]

Classic or "nondeep" machine learning benefit from human intervention to allow a computer system to input patterns, learn, perform specific tasks, vet outputs and provide accurate results.[83] There is a lack of autonomy in basic machine learning versus deep learning that allows the algorithm to suggest anomalies be categorized as such based on similar characteristics. Human experts determine the hierarchy of features to align the system to understand the differences between data inputs, usually requiring more structured data to learn. Unlike machine learning, tools such as generative AI produce content such as text, audio, code, videos, and images.[84] The content produced is based on information collected from user inputs called "prompts", that are typically short instructional texts.[85]

Unlike generative AI, machine learning systems will offer results based on characterizing features which are required to be vetted/confirmed by a learning supervisor.[86] For example, if a

---

[81]Natural Resources Canada (9 November 2023) Machine Learning, technical service highlights. online: https://nrc.canada.ca/en/research-development/products-services/technical-advisory-services/machine-learning
[82] IBM (6 July 2023) AI vs Machine Learning vs Deep learning vs neural networks: What's the difference? Online: https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks
[83] *Ibid.*
[84] McKinsey & Company (19 January 2023)"What is Generative AI?" online: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai.
[85] *Ibid.*
[86] *Supra* note 82.

human was required to provide examples of fast food; he or she might suggest things like pizza, burgers or sandwiches, based on the characterization of those foods. Perhaps the portability, size, other factors may be classified as characterizing features as well.[87]

If the machine learning system was trained on images of a pizza, burger and sandwich, identifying the similarities, it could make recommendations on similar fast-food types based on what the system assumes are similar characteristics.[88] While both machine learning and deep learning provide interesting considerations, programming would require calibration from human experts using large volumes of data in order to establish proper recognition to generate desired results. This often requires software engineers and data scientists to ensure "clean data" is entered to create an effective machine learning algorithm with continuous vetting until the system can develop defined parameters.

In Canada, both the Communications Security Establishment (CSE) and Natural Resources Canada (NRC) offer machine learning / deep learning services to their collaborators.[89] NRC's *Digital Technologies Research Centre* offers machine learning services to query large volumes of text, preform machine translation and evaluation, uncover new molecular interactions, monitor engineering systems, and capture data through machine vision.[90]

c) Manufacturing AI Use Cases

In the context of Canadian manufacturing, there are already use-cases of machine learning algorithms being applied to process large volumes of data of production equipment and product to help optimize time-consuming aspects of the manufacturing process, including quality

---

[87] *Supra* note 82.
[88] *Supra* note 82.
[89] *Supra* note 81.
[90] *Supra* note 81.

control, equipment maintenance and product design.[91] Machine learning-based technologies used in manufacturing can include predictive analytics, intelligence process automation (IPA), visual inspection systems, user behavior analysis (UBA) and neural networks.[92] Leading manufacturers like Magna International, based in Aurora Ontario, achieved a 35% reduction in maintenance costs after implementing AI predictive systems across their production lines.[93] Furthermore, they've signed a strategic partnership with Sanctuary AI, a Vancouver based company, to develop integrating AI robots into its factories with specific tasks.[94]

Similarly, Bombardier's Thunder Bay facility reduced unplanned downtime by 40% through AI-driven maintenance solutions, resulting in annual savings of $2.3 million.[95] Modern manufacturing facilities are increasingly leveraging sensor networks and advanced analytics to monitor equipment performance in real time.[96] Machine learning algorithms have the ability to analyze historical and real-time data to establish normal operating patterns, flag anomalies that might indicate developing problems.[97] Bombardier's predictive maintenance system paid for itself within just nine months of implementation.[98] Predictive analysis in both use cases demonstrate that machine learning is capable of not only conduct predictive analysis to flag early detection, but that they improve resiliency and reduce downtime. This is extremely valuable towards long term growth and productivity.

---

[91] Business & Industry Canada (2 January 2025) 7 Game-Changing AI Applications Revolutionizing Canadian Manufacturing Today. online: https://www.industryandbusiness.ca/7-game-changing-ai-applications-revolutionizing-canadian-manufacturing-today
[92] *Ibid.*
[93] Times Colonist (11 April 2024) Auto parts maker Magna international signs strategic partnership with Sanctuary AI. online: https://www.timescolonist.com/automotive/auto-parts-maker-magna-international-signs-strategic-partnership-with-sanctuary-ai-8586145
[94] *Ibid.*
[95] *Supra* note 91.
[96] *Supra* note 91.
[97] *Supra* note 91.
[98] *Supra* note 91.

Perhaps once of the most applicable subsets of machine learning that may be effective in detecting insider risk is visual inspection systems. More compatible with physical environments, visual inspection systems powered by AI have revolutionized quality control in Canadian manufacturing facilities.[99] These systems combine high-resolution cameras and sophisticated machine learning algorithms to detect defects and inconsistencies at speeds far exceeding human capabilities.[100] Leading manufacturers across Ontario and Quebec have reported up to 99.9% accuracy in defect detection after implementing AI-powered visual inspection systems.[101] These systems can identify microscopic flaws, color variations, and structural anomalies in real-time, significantly reducing the risk of defective products reaching customers.[102]

The use cases mentioned previously demonstrate how AI systems are currently being leveraged by manufacturers to identify anomalies in existing processes by identify potential problems. They also demonstrate the possibilities that AI systems offer when it comes to anomaly detection and problematic behavior which may serve an additional purpose if caused by insider activity. In both applications, issuing an alarm when the presence of an unknown product is detected, or when the network identifies one or more unauthorized access attempts on a security device can be deployed just as an alarm notification is received when AI systems detect that a critical process step was missed or not completed accurately.

While there are multiple use cases of Canadian manufacturers integrating these machine learning systems within their existing processes and workflows, limited use cases exist of

---

[99] *Supra* note 91.
[100] *Supra* note 91.
[101] *Supra* note 91.
[102] *Supra* note 91.

Canadian manufacturers utilizing AI systems (specifically machine learning) for insider risk behavior detection.

While manufactures in Canada have demonstrated they are able to overcome the learning curves and come to a position of comfort with AI tools in their core processes, there are limited use cases of manufacturers leveraging them solely for insider risk detection in manufacturing environments. Furthermore, there is limited available information to understand whether the existing systems leveraged by Canadian manufacturers would also flag insider risk activity if it occurred, or if the type of algorithms developed (machine learning/deep learning) can identify trends, progressive or evolving abnormal activity to extent that insider risk behavior would be flagged.

It is not entirely surprising, given that there are limited known insider risk incidents that are publicized in Canadian manufacturing, that perhaps the problem is not significant enough for senior organizational leaders to warrant the prioritization of AI technology investment. It may be that organizations are more focused on leveraging the technology to enhance operational processes and are comfortable operating within their own risk tolerances. It may also be due to the lack of knowledge or information on the capabilities of AI to mitigate insider risk, or at this stage of strategic planning and forecasting, it does not present an opportunity for significant return on investment.

Although insider risk incidents are not widely publicized in Canadian manufacturing, it does not mean that they do not exist; perhaps they have gone undetected, or proper controls have not been put in place to identify them. When considering utilizing AI systems to detect insider risk in manufacturing environments, two options for organization decision-makers to consider are: 1) implementation of AI detection systems into existing security platforms; and 2)

implementation of AI detection systems into industrial control platforms. While there are a variety of AI system options, based on similar environmental characteristics, machine learning and "deep learning" specifically offer the most opportunity to detect insider risk in these critical systems.

d) Possibilities of AI Integration in Security Systems

Existing security systems provide a unique opportunity to incorporate AI-powered threat detection and prevention systems used to detect anomalies and malicious network traffic in real time. Furthermore, physical environments such as manufacturing can utilize AI systems in both IT & physical security systems. Video management systems (VMS) which manage, store, and analyze video footage have a variety of plug in options available from the company itself or are compatible with third party plug ins. The adaptability of VMS systems is extremely positive when it comes to assessing potential AI systems that are available on the market. Another option to utilize AI systems by integrating them into physical security device software such as metal detectors and x-rays.

In 2024, Smiths Detection, a detection and screening technology company, published a whitepaper titled *Automatic Object Recognition In Aviation Security*.[103] The paper explores the role of AI and deep learning with anticipated outcomes of how AI will change the landscape of security environments.[104] Furthermore, by training algorithms based on large data sets, acquired by industry partners, there is huge potential for automated object recognition to be far more efficient for detection.[105] The shift from methods used today to the anticipated AI powered

---

[103] Mader, Dr. A. (Date Unknown) Smiths Detection: Automatic Object Recognition in Aviation Security online: https://hello.smithsdetection.com/hubfs/Aviation_Whitepaper_AIandObjRecog_1.pdf?hsCtaTracking=0aa7a202-c944-4f6b-ace9-0cda50ecb792%7C12da59e2-bdae-4a29-91dd-5c7865a2dfba

[104] *Ibid.*

[105] *Ibid.*

recognition system strives for an "alarm-only" viewing at security checkpoints and this would require security resources only for alarm resolution.[106] Beyond screening, Smiths Detection explores how AI may go beyond object detection and has the potential for greater benefits such as image interpretation, behavioural analysis, identification of patterns in biometrics, ability to conduct risk assessments and preform predictive analysis.[107] While the paper shines light on current exploration of AI technology being incorporated in security systems, it also demonstrates how increased detection capability may be transferrable to security devices, not limited to the aviation sector. The research also sparks further inquiry into how the technology may also be leveraged to detecting insider risk activity in the form of "alarm-only" viewing and response.

Another example of AI technology being incorporated in existing security systems, the company Resolver launched a tool in 2025 leveraging artificial intelligence to transform risk management by way of intelligent triage. Resolver's *AI Intelligent Triage* offers an embedded AI predictive analysis tool to assist in more succinctly forming raw data inputted from incident reports to more detailed reports that can link multiple relationships.[108] Resolver's AI tools assist the user to provide more clear and concise reports, forming a timeline and using LLM (large language models) to provide input in the language of their choice, and having the option to seamlessly translate to another language of the reader's choice.[109] In the context of insider risk detection, more advanced reporting and intelligence linking predictive analysis, may be able to alert organization authorities to evolving risk trends, facilitating quicker intervention before risks materialize.

---

[106] *Supra* note 103.
[107] *Supra* note 103.
[108] Resolver (2025) AI Intelligent Triage. Online: https://www.resolver.com/ai/
[109] *Ibid.*

When it comes to detecting insider risk behavior digitally, most large manufacturing companies that invest in robust cybersecurity measures may have a SIEM (Security Information and Event Management) solution or SOAR (Security Orchestration, Automation, and response) solution. While SIEM solutions collect, aggregate and analyze data to detect threats, SOAR solutions focus on automating security processes and initiate incident response workflows to improve efficiency for cyber security teams.[110] There are many SIEM and SOAR platforms that now have AI automated actions, such as isolating infected devices or blocking IPs. Logpoint, a Denmark based company, utilizes machine learning to establish behavioral baselines for users and groups.[111] By analyzing deviations from these baselines, it effectively identified anomalous activities indicative of insider risks.[112] This approach reduces false positives and enhances the efficiency of corporate security teams to be alerted to suspicious activity and intervene in a timely manner.[113]

Splunk, an American software company that specializes in big data analytics, security and observability solutions, provides several ways of utilizing AI – machine learning across diverse product portfolios to detect insider risk behavior.[114] Splunk's cloud platform allows users to detect anomalies, such as identifying outliers in the number of application errors; generate forecasts such as forecasting resource utilization, make predictions like predicting potential outages and clustering data into groups like clustering network activity to detect potentially

---

[110]Stratejm (15 December 2021) *Security Orchestration Automation & Response (SOAR) in Action*. Video access online: https://stratejm.com/recording-security-orchestration-automation-response-in-action/security-orchestration-automation-response-soar-in-action

[111] Logpoint (20 January 2021) *Behavioral Approach to Security.* Online: https://www.logpoint.com/en/blog/behavioral-approach-to-security/

[112] *Ibid.*

[113] *Supra* note 111.

[114] Splunk Artificial Intelligence for Observability (Accessed March 22, 2025) An Introduction Use Case Guide. Online: https://www.splunk.com/en_us/pdfs/gated/ebooks/eight-use-cases-for-ai-in-observability.pdf

misconfigured services.[115] Additionally, ML-based analytics can be created directly using Splunk's search language — Search Processing Language (SPL) — with a number of ML search commands embedded into core search and reporting.[116] The patterns tab in the search and reporting app also presents embedded machine learning to help identify groups of similar events in search results.[117] Splunk also provides ML-powered SIEM platform, pre-defined threat detection modeling in user behaviour analytics, designed to identify advanced persistent threats and insider threats and workflows in IT Service Intelligence.[118] Market tools such as the ones that Splunk provides may be an attractive option for manufacturers given the capabilities to monitor infrastructure and can detect outliers in metrics or predict when resource utilization thresholds will be crossed.

There have been significant advancements of AI powered systems to enhance detection of insider risks incorporated as part of larger security infrastructure tools. These AI systems are extremely compatible with third-party tools, on-premises data centers, private clouds, security devices and custom third-party services.[119] While this demonstrates that compatibility and functionality are improving, it also provides increased opportunities for manufacturing organizations to leverage AI systems to detect anomalies and initiate quicker responses to mitigate damage to the organization.

e) Possibilities of AI Integration in Industrial Control Systems

Industrial control systems within an organization are unique and often customized to the internal processes themselves. Companies understand the uniqueness of their business and by

---

[115] *Supra* note 114.
[116] *Supra* note 114.
[117] *Supra* note 114.
[118] *Supra* note 114.
[119] *Supra* note 114.

leveraging opportunities with AI, can fully integrate it into their strategies. When it comes to implementation, understanding what objectives are hoped to be achieved and what critical processes are worth protecting, will more clearly identify the scope of how AI can be utilized within the industrial control system. According to Splunk, 87% of data science projects fail to make it to production, highlighting primarily, the importance of defining clear outcomes to make an ML project successful. [120] Furthermore, Splunk has observed the most successful ML projects are often tied to granular outcomes, such as increasing detection accuracy by 70% for alerts related to application errors or reducing manual triage time for Network Operations Center (NOC) analysts by 50% when assessing alerts.[121] There are opportunities to leverage AI tools to detect insider risk behavior to "flag" unusual or suspicious activity within the system based on control milestones build into the process. To track the inputs and confirm process integrity, AI tools may be able to alarm or shut down processes that do not meet certain requirements until an override is provided by a second (preferably more senior) operator.[122] This built in safeguard may prevent further insider risk damage whether it be intentional or unintentional.

While there are limited examples of manufacturers leveraging machine learning to detect insider risk behavior within industrial control systems, there are use-cases in Canada that demonstrate machine learning capabilities are enhancing Canadian manufacturers. Kruger Canada developed its first AI project for its brand-new state-of-the-art facilities located in Sherbrooke, Quebec.[123] Kruger set a goal to increase productivity at this facility, and mainly focused on leveraging AI tools that conduct demand forecasting using predictive analysis.[124] Jack

---

[120] *Supra* note 114.
[121] *Supra* note 114.
[122] *Supra* note 114.
[123] Ba, C. (15 November 2022) ScaleAI: Canadian Manufacturing Players at the forefront of AI. online: https://www.scaleai.ca/blog/canadian-manufacturing-players-at-the-forefront-of-ai
[124] *Ibid.*

Klejka, VP of Product at the Canadian company IVADO Labs stated "*The benefits of projects related to predictability are quite convincing; every member of your organization can easily understand how those initiatives can have a direct impact on improving margins and increasing the company's turnover*."[125] Predictive modeling can automate reoccurring tasks or even capture entire processes. It can be leveraged for inventory management, with predefined levels to avoid any shortages or disruptions.[126]

Companies that process large amounts of data through industrial control systems may be able to benefit from saving time and energy and identify ideal solutions.[127] Predictive analysis algorithms in the Kruger use case were leveraged on their production line, where instead of having a process engineer trying to find the best parameters out of thousands of product combinations, predictive algorithms defined what the optimal setting for each parameter would be to maximize production.[128]

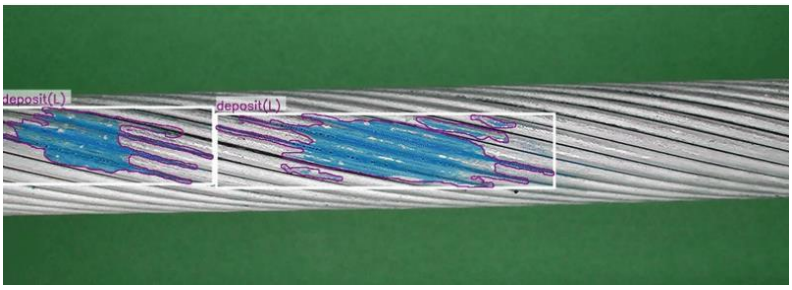
Another use case leveraging AI in Canadian critical manufacturing is the Mila -Hydro-Quebec partnership, which explores integrating robotics in power grid inspections, developing a fleet of robots to do the dangerous inspections for anomalies on power lines.[129] For several years, Hydro-Quebec has partnered with Mila, a Montreal-based artificial intelligence research institute, which has worked together to launch the applied research project with experts at Hydro-Quebec.[130] The objectives were to produce a robust dataset of annotated anomalies that could enable more extensive and in-depth algorithm analysis for inspecting cable conditions

---

[125] *Supra* note 123.
[126] *Supra* note 123.
[127] *Supra* note 123.
[128] *Supra* note 123.
[129] Mila (21 February 2025) AI-Powered Inspections: Hydro-Quebec Case Study online: https://mila.quebec/en/news/ai-powered-inspections-hydro-quebec-case-study
[130] *Ibid.*

across the network, and to adapt these algorithms for few-shot and zero-shot learning scenarios.[131]

For the data to reflect the diverse anomalies encountered on power line cables, Mila researchers with Hydro-Québec experts created CableInspect-AD, a high-quality, publicly available dataset for model training and evaluation tailored for power line inspections.[132] Curated by Hydro-Québec's research institute, IREQ, this unique dataset includes a wide range of real-world anomalies, such as scratches and broken strands, presented through thousands of high-resolution images of three distinct power line cable types showcasing seven common defects at varying severity levels.[133]



(Mila, 2025)

Once the robust datasets were acquired, the Mila team explored different AI methods for anomaly detection.[134] The team attempted vision-learning models (VLMs), which can detect anomalies without prior training on specific defects, and they performed very well.[135] The project provides an incredible overview of how machine learning models are increasingly being deployed in manufacturing industrial control systems and how they can be applied to critical applications with success.

---

[131] *Supra* note 129.
[132] *Supra* note 129.
[133] *Supra* note 129.
[134] *Supra* note 129.
[135] *Supra* note 129.

More information on the Mila-Hydro Quebec partnership can be found in **Appendix A**.

Both use cases demonstrate the ability to leverage AI in industrial control systems and critical applications that undoubtedly enhance productivity and improve efficiency in their operations. However, use cases on Canadian critical manufacturing companies' incorporation of AI tools to mitigate insider risks in their industrial controls systems are limited. These use cases demonstrate that while the focus has been leveraging AI tools to improve business functions and enhance productivity, there are limited examples of Canadian manufacturing organizations investing in AI tools to mitigate insider risk in critical processes. Given the important roles that industrial control systems and quality management systems play related to organizational performance and productivity, it is surprising that there are not more examples of organizations using AI tools to protect these critical systems.

Part III. Artificial Intelligence Challenges and Considerations in Manufacturing

a) Biases, Discrimination & Privacy

While the critical manufacturing sector continues to explore and enhance their knowledge of artificial intelligence and machine learning, there are some challenges organizations will need to evaluate during their research and development program phase. Primarily, what ethical concerns might arise with AI algorithm collection and use of data collected. Will the use of AI tools erode human judgment and dehumanize employees? Furthermore, how do organizations prevent fast positives and negatives that lead to constant correction and calibration? These questions prompt careful consideration and should be evaluated against positive opportunities presented by AI tools to determine investment potential.

Bias and discrimination in training data pose one ethical concern that is identified when exploring use of AI tools.[136] The concept being that AI algorithms used in machine learning applications, such as anomaly detection or predictive analysis, require large volumes of training data to "teach" the algorithm what to flag and what not to flag. Therefore, quality of the dataset is of utmost importance to ensure the algorithms are accurate. [137] Additionally, that deep learning algorithms may learn from biases leading to further discrimination in its application[138]

As machine learning must be trained on data provided by humans, the human biases embedded in machine learning datasets can pose significant ethical challenges when deploying these systems in manufacturing environments. Fore example, if training data is imbalanced or the model architecture is not designed to account for diverse inputs, the model may produce biased outputs.[139] Algorithmic biases can also arise from optimization techniques that favor majority group predictions over minority groups.[140] Additionally, during the deployment testing phase, even if a model appears unbiased during training, biases can still emerge when deployed in real-world applications.[141] If the system is not tested with diverse inputs or monitored for bias after deployment, it can lead to unintended discrimination or exclusion.[142]

Addressing biases in AI requires diverse and representative datasets, rigorous testing and a continuous feedback loop, where AI models are regularly evaluated and updated based on real-world interactions and new data.[143] In a manufacturing environment, this type of ethical concern

---

[136] Intelegain Technologies (26 March 2024) Ethical Considerations in AI & Machine Learning. Online: https://www.intelegain.com/ethical-considerations-in-ai-machine-learning.
[137] *Ibid.*
[138] *Ibid.*
[139] Chapman University (Accessed March 2, 2025) Bias in AI. Online: https://www.chapman.edu/ai/bias-in-ai.
[140] *Ibid.*
[141] *Ibid.*
[142] *Ibid*.
[143] *Ibid.*

could present itself in the form of employee evaluation tools imbedded in industrial control systems such as using sensor data or quality control metrics, there may be a bias should the algorithm favour a certain group of individuals (perhaps younger workers that move faster versus employees that are older). [144]

In addition, when considering implementing an AI system, privacy and data security are most always at the forefront of discussions. With the large amount of data required for training AI tools, there are serious concerns about collecting and storing personal data given the misuse or breaches that could occur, which may have severe consequences on an individual or organization.[145] As such, Canadian manufacturers must prioritize data protection, implement strong encryption, and adhere to privacy regulations set forth by the Office of the Privacy Commissioner of Canada, such as compliance with the *Personal Information Protection and Electronic Documents Act.*

The government of Canada and its member agencies are aware that developments in AI have created regulatory gaps that must be addressed for Canadians and Canadian businesses to trust AI technology. In 2022, Innovation, Science and Development Canada (ISED) tabled the Artificial Intelligence and Data Act (AIDA) as part of Bill C-27.[146] AIDA aims to build on existing Canadian consumer protection and human rights law, while address the risks presented by high-impact AI systems. Under the proposed framework, AIDA ‘s mandate would include

---

[144] Robbins, S., Yaqoob, A. (8 July 2024) ResearchGate: Ethical Concerns in AI-Enhanced Job Performance Metrics in Human Resources. Online: https://www.researchgate.net/profile/Steven-Robbins-12/publication/382073534_Ethical_Concerns_in_AI-Enhanced_Job_Performance_Metrics_in_Human_Resources/links/668bebe4af9e615a15d70a73/Ethical-Concerns-in-AI-Enhanced-Job-Performance-Metrics-in-Human-Resources.pdf

[145] Innovation, Science and Economic Development Canada (accessed 2 March 2025) The Artificial Intelligence and Data Act (AIDA) - Companion Document. Online: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s1

[146] *Ibid.*

protecting Canadians from collective harms, such as discrimination and biased outputs caused by AI systems.[147]

Since Royal Assent of Bill C-27, titled *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts,* ISED is intending to conduct a broad and inclusive consultation of industry, academia, civil society and Canadian communities to inform the implementation of AIDA and its regulations.[148] This is expected to include:

- The types of systems that should be considered as high impact;
- The types of standards and certifications that should be considered in ensuring that AI systems meet the expectations of Canadians.
- Priorities in the development and enforcement of regulations, including with regard to an AMPs scheme;
- The work of the AI and Data Commissioner; and
- The establishment of an advisory committee.

(Innovation, Science and Development Canada, 2025)

When reviewing both the framework for AIDA and Canadian governing body policies and directives, ethical and secure AI deployment will be a top priority amongst industry partners, including those in the manufacturing sector. Intercollaboration between Innovation, Science and Economic Development Canada, Treasury Board of Canada Secretariat and Standards Council of Canada, along with international bodies, will develop best practices to ensure ethical and secure AI deployment in Canada.[149] These policies and directives will serve as the foundational

[147] *Supra* note 145.
[148] *Supra* note 145.
[149] *Supra* note 145.

components for Canadian manufacturing organizations, which will be expected to align their AI practices with the regulations. Furthermore, organizations will need to continually assess and mitigate as the government identifies and responds to industry trends, loopholes, or gaps in policy.

b) Canadian Resources for Ethical Deployment of AI

Both public and private-sector organizations have published principles to guide responsible development and deployment of AI tools. Both government bodies and leading technology companies such as Microsoft have created AI ethics checklists and assessment tools to assist in moral deployment of these systems. In 2020, Microsoft published their first checklist: *Co-Designing Checklists to Understand Organizational Challenges and Opportunities around Fairness in AI.*[150] In 2024, they produced an additional publication called *Tinker, Tailor, Configure, Customize: The Articulation Work of Customizing AI Fairness Checklists*.[151] These resources, which were designed with 13 AI practitioners from seven organizations, aim to contextualize the uniqueness of how AI checklists may be used to try to develop a set of shared language and values in AI. These resources identify that there are sometimes tensions related to ownership over this process, and accountability may play a larger role in responsible AI deployment.[152]

In Canada, the Treasury Board of Canada Secretariat's *Directive on Automated Decision-Making* is an existing tool that determines the impact level of an automated decision-making

[150] Madaio, M., Stark, L, Wallach, H., Wortman Vaughan, J. (March 2020) Co-Designing Checklists to Understand Organizational Challenges and Opportunities around Fairness in AI. online: https://www.microsoft.com/en-us/research/publication/co-designing-checklists-to-understand-organizational-challenges-and-opportunities-around-fairness-in-ai/
[151] *Ibid.*
[152] *Ibid.*

system.[153] The directive aims to guide those leveraging artificial intelligence to make or support administrative decisions or improve service delivery do so in a manner that is compatible with core principles of administrative law such as transparency, accountability, legality, and procedural fairness.[154] The directive includes an algorithmic impact assessment tool and requires information be provided for multiple risk areas, such as personnel rights, privacy based on the type of automation (full or partial).[155]

The tool outlines the mitigation areas and de-risking of ethical concerns related to procedural fairness, bias in data quality and privacy and impact assessment levels clearly defined with descriptions to assist users. [156] It also includes impact level requirements and describes that levels II and III require consultation from qualified Government of Canada experts, industry experts or contractors with relevant specialization.[157] Level IV described in the directive, requires more advanced consultation with Government of Canada technical bodies such as National Research Council of Canada, Statistics Canada, Shared Services or the Communications Security Establishment of Canada.[158]

With the widespread adoption of AI automation tools, the manufacturing sector may have an increased risk of displacing jobs due to the potential of increased productivity AI tools present. Specifically, with machine learning technologies that leverage AI-powered quality control systems, it has transformed manufacturing quality metrics across Canada.[159] Recent data

---

[153] Government of Canada (2025) Algorithmic Impact Assessment Tool. online: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html

[154] Treasury Board of Canada Secretariat (2025) Directive on Automated Decision-Making. Online: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

[155] *Supra* note 153.

[156] *Supra* note 153.

[157] *Supra* note 153.

[158] *Supra* note 153.

[159] *Supra* note 153.

from Ontario manufacturers shows an average of 35% reduction in defect rates after implementing AI-based inspection systems.[160]

c) Concerns Regarding Job Displacement

While it is difficult to predict the impact of AI systems on Canadian jobs, past studies on technological transformation examined the potential impact of automation on the Canadian labor market.[161] Integrating data from the 2016 and 2021 census, with data from the Occupational Information Network—offers some experimental estimates of occupational exposure to AI using the methodology developed by Statistics Canada.[162] The measure used is the complementarity-adjusted AI occupational exposure index, which can classify jobs into three AI groups using the median AI occupational exposure index and complementarity scores: (1) high exposure and low complementarity, (2) high exposure and high complementarity, and (3) low exposure (regardless of the degree of complementarity).[163]

The first two groups consist of jobs that may be highly exposed to AI, but the first group may have relatively more tasks that could be replaced by AI in the future, while the second group may have relatively more tasks that are highly complementary with AI.[164] The third group of jobs are those that may be less exposed to AI than the first two groups, regardless of the degree of complementarity.[165]

---

[160] *Supra* note 144.
[161] Statistics Canada (25 September 2024) Exposure to Artificial Intelligence in Canadian Jobs: Experimental estimates. Online: https://www150.statcan.gc.ca/n1/pub/36-28-0001/2024009/article
[162] Felten, E., Raj, M. and R. Seamans. (2021) Occupational, Industry, and Geographic Exposure to Artificial Intelligence: A Novel Dataset and its Potential Uses. Strategic Management Journal 42(12): 2195-2217. Online: https://www150.statcan.gc.ca/n1/pub/36-28-0001/2024009/article/
[163] *Ibid.*
[164] *Ibid.*
[165] *Ibid.*

According to Stats Canada, in May 2021, 31% of employees aged 18 to 64 in Canada were in jobs that may be highly exposed to AI and relatively less complementary with it, 29% were in jobs that may be highly exposed to and highly complementary with AI, and 40% were in jobs that may not be highly exposed to AI.[166]

While manufacturing jobs have varying degrees of exposure to AI, depending on the specific tasks involved, roles that involve repetitive, routine manual tasks may have a high exposure and low complementarity rate which make them susceptible to automation by AI. Research indicates that positions requiring people skills and complex decision-making are less exposed to AI automation.[167]

Nevertheless, employers may not immediately replace human labor with AI due to financial, legal and institutional constraints even if it is technologically feasible to do so.[168] The experimental estimates presented should be interpreted with some reservation. At the very least, many roles may simply require a certain degree of job transformation and technical skill development to improve output production.[169]

Ethical considerations do play a significant role in considering whether to implement AI tools across a variety of sectors. In manufacturing environments, where automation may benefit organizational production, senior leaders must weigh several factors including ethical concerns, financial impacts, and reputation when strategic planning. Failure to consider ethical considerations, however, may expose the organizational to increased insider risk should labor requirements change and layoffs prompt employees to have negative associations to the

---

166 *Supra* note 162.
167 *Supra* note 162.
168 *Supra* note 162.
169 *Supra* note 162.

organization. Organizations would need to consider mitigation efforts or may choose the alternative such as investing in employee development, allowing for upskilling to occur that may complement AI systems. This may improve productivity, allow for less over-reliance on technology, and minimize harmful brand reputation.

d) Potential Challenges with Organization Integration

For organization who may be considering implementing AI systems to detect insider risk, there are several operational challenges which should also be considered before on-boarding a specific platform.

Carnegie Melon's Software Engineering Institute outlines numerous challenges organizations may face in their report *Dangers of AI for Insider Risk Evaluation (DARE).* The report outlines *Change as a Constant* as one important challenge to consider.[170] In manufacturing environments, this is particularly true as organizations are consistently changing their products and product manufacturing processes for new products, usability and competitive advantage.[171] Therefore, as product models change, equipment must be adapted and re-programmed to achieve different outputs. This constant adaptation to new modelling and refinement means that data associated to quality control systems or industrial control systems would require frequent updating.[172] As a result, AI tools which have been trained to detect insider risk on specific data sets, must be updated or refined for every new process generated, as models would no longer be accurate.[173]

---

[170] Whisnant, A. (October 2024) Carnegie Mellon University, Software Engineering Institute: *Dangers of AI for Insider Risk Evaluation (DARE).* Online: https://insights.sei.cmu.edu/library/dangers-of-ai-for-insider-risk-evaluation-dare/
[171] *Ibid.*
[172] *Ibid.*
[173] *Ibid.*

Additionally, the report outlines that *overtrust (automation bias)* may be another organization consideration when implementing AI tools.[174] In a manufacturing environment, this may result when AI insider risk detection tools are implemented in either security systems or industrial control systems, and employees have an overreliance on AI results and do not challenge or confirm some, resulting in bias or error. This can lead to relaxed oversight, poor decision making, or deterioration of skills required to assess and evaluate results with non-AI methods.[175]

e) Concerns with Integrity of AI Systems

AI tools, specifically machine learning applications, require training on large data sets for algorithms to identify anomalies. Specifically relating to manufacturing AI tools to detect insider risk, the tools must be trained by humans on insider risk data in the form of pre-determined or "known" anomalies. This will help the systems identify similar patterns associated to known anomalies within the system and prompt an alarm to human resources if there is a correlation between "known" and "suggested" anomalies within the systems.[176] By prompting an alarm, it initiates a second inspection or requirements acknowledgement of the false positives.[177] There are limitations however, with available training data to have a system effectively trained.[178]

Examples of insider risk anomalies that a system may be trained on are incorrect inputs, unauthorized entries, not following process, may be examples of insider risk data to which there is limited training data for programming. [179] As a result, low and slow attacks are less likely to be

---

[174] *Supra* note 170.
[175] *Supra* note 170.
[176] *Supra* note 170.
[177] *Supra* note 170.
[178] *Supra* note 170.
[179] *Supra* note 170.

detect, especially over large historical data that may cause problems with scalability, as the level of granularity in the data will not be available and go unchallenged.[180]

One insider risk behavior that has been noted more recently is malicious actors poisoning data sets when building models in machine learning systems.[181] Injecting malicious data used to train models or manipulating the data to their benefit can severely degrade their performance and reliability.[182] Malicious insiders may input data specifically to "trick the system" into making incorrect decisions or providing harmful outputs could have negative consequences and fail to conduct detection or predictive analysis correctly.[183] As a result, AI models may be compromised and untrustworthy. In poisoning attacks, attackers can deliberately add malicious samples in the training phase to manipulate the trained machine learning model and change the generated predictions.[184] An evasion attack is developed after the model is deployed in practice, and it requires an attacker to modify specific data samples (called adversarial examples) to induce their misclassification to a desired output label.[185] To combat insider risk via data poisoning, research literature suggests that *establishing enhanced loss functions* may combat data poisoning instead of standard loss functions. This would involve fine tuning of the machine learnings objectives in the training phrase, to limit the influence of poisoned samples.[186] Furthermore, tr*aining data sanitization* is recommended to isolate the poisoning points using outlier detection methods, clustering or anomaly detection.[187]

---

[180] *Supra* note 170.
[181] Oprea, A. (November 2022) Northeastern University: Poisoning Attacks Against Machine Learning: Can Machine Learning Be Trustworthy? Online: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934932.
[182] *Ibid.*
[183] Perception Point (Accessed 2 March 2025) Top 6 AI Security Risks and How to Defend Your Organization. Online: https://perception-point.io/guides/ai-security/top-6-ai-security-risks-and-how-to-defend-your-organization
[184] *Supra* note 181.
[185] *Supra* note 181.
[186] *Supra* note 181.
[187] *Supra* note 181.

The vulnerability of AI against data poisoning can be observed as one of the main impediments of AI development in industry and, especially, in critical settings, such as cybersecurity, health care, and manufacturing.

In manufacturing settings, integrity of AI systems may affect robustness through intentional or unintentional attacks.[188] For example, should an insider commit a malicious act with the credentials of another employee, it would be difficult to for an AI system detect or associate if credentials compliance measures are not strictly adhered to.[189] In addition, unintentionally, employees may become lax in complying with credential policies (logging in and out of ICS or security systems), making it difficult for AI tools to associate anomalies with specific users or detect trends in employee user activity.[190] Long term trends or escalations in behavior may go undetected if one insider leverages multiple user accounts to commit malicious acts over a certain period.[191]

To mitigate integrity concerns of AI systems, it is important that security controls, compliance and quality control measures be put into effect by organizational employees; specifically involving AI system programmers, modifiers, or third parties contracting to make system adjustments. Appropriate oversight should be applied to ensure mitigation of potential vulnerabilities or risk of adversarial attacks by those able to manipulate the systems.[192]

---

[188] *Supra* note 183.
[189] *Supra* note 183.
[190] *Supra* note 183.
[191] *Supra* note 183.
[192] *Supra* note 181.

Research Conclusions: The Future of AI in Critical Manufacturing & Practical Recommendations for Deployment

a) Future Possibilities of AI Integration in Canadian Manufacturing

The integration of AI and machine learning systems to detect insider risks in manufacturing environments presents many new opportunities and challenges, especially as they relate to securing largely physical environments. When assessing how manufacturing fits into the national strategy of protecting Canada's critical infrastructure, we know that it plays a significant role especially for resiliency and recovery. Furthermore, that while insider risk incidents are more prevalent in the U.S., Canada is not immune to insider risks, which makes them extremely relevant in todays manufacturing industry. Despite, there being limited insider risk incidents in manufacturing publicized in Canada, we know from other sectors, they occur and are relevant. In addition, our U.S. counterparts have designed a specific guide to developing insider risk programs in critical manufacturing, which brings light to how important the sector itself is as part of the wider critical infrastructure network.

The research uncovered that AI tools have been widely adopted in manufacturing environments both in Canada and abroad. With the advancements of smart manufacturing systems, and the IoT (internet of things) increasing digital capacity in manufacturing environments, the next natural progression is to leverage new and existing AI technology to transform routine manual tasks that are preformed repetitively and do not require a high level of accuracy. It is unknown however, if the current AI tools that are deployed, are also leveraged to detect insider risk activity.

Throughout the paper, there were examples of what AI systems are presently on the market today that can be deployed in both security systems and industrial control systems applications to detect insider risk activity. There is limited data to support their use and

effectiveness which may suggest that the sector is not prepared to rely solely on outsourcing its detection efforts to AI systems, despite their ability to enhance detection of insider risk activity. Due to some of the challenges and concerned outlined earlier in this paper, organization may struggle with designed how to mitigate such challenges, such as: ethical, technical or organizational.

As AI technology advances at a rapid rate, there is an emerging risk of insiders exploiting the new, largely unregulated AI systems and their applications. Data poisoning is an example of this and should be considered if manufacturers opt for AI system technology for detecting insider risks. As the research indicates, there are multiple government agencies working to standardize the use of AI in its application in both public and private sectors, with formal integration yet to be outlined.

Government of Canada agencies, such as Innovation, Science and Economic Development Canada and the Treasury Board of Canada Secretariat, have begun formatting a structure and proposing legislation with respect to how AI should be managed and applied in Canadian Society. As a global leader in AI development and deployment, Canada has indicated its commitment to ensuring ethical use of AI systems and mitigating all known harms to Canadian users or those affected by its use. Working with global partners, industry partners and academia, the government continues to strengthen its oversight in delivery, application and effects on Canadians and the Canadian economy, while not comprising national security.

b) Insider Threat Alliance Project

One initiative that aims to bridge the gap between AI insider risk detection and critical infrastructure environments is the newly formed Insider Threat Alliance Project. An initiative that brings together researchers from 3 Canadian universities (Polytechnique Montreal, HEC

Montreal, and Universite de Montreal), to focus on developing integrated insider risk management solutions using AI.[193] Launched in 2023, and backed by industry partners, including the National Bank of Canada, Desjardins, Qohash, Mondata, and Cybereco, The Insider Threat Alliance Project established an institutional chair labelled *GEDAI (Detection, Analysis, and Automated Management of internal Breaches and Anomalies).*[194] With funding of 5.4 million dollars over five years from Natural Sciences and Engineering Research Council (NSERC) and Mathematics of Information Technology and Complex Systems research organization (MITACS), the research will explore leveraging AI to learn, model knowledge, and apply automated reasoning to enhance the detection and management of internal breaches and anomalies.[195]

The mandate the Insider Risk Alliance Project and established scope of the institutional chair *GEDAI* is to develop AI-driven tools tailored to detect and manage insider risks, which may potentially benefit the critical manufacturing sector where industrial control system security is critical.[196]

c) Conclusions and Practical Recommendations

The research set out in this academic paper focuses on identifying how prevalent insider risks are in Canada's critical manufacturing sector. The research suggests that at this time, there are limited incidents of insider risks (at least that have been publicized) in Canadian critical manufacturing. However, while not directly linked, there are documented incidents of insider risk attacks on Canadian critical infrastructure in the form of financial institution data breaches, cyber-attacks, and theft of intellectual property, as well as documented incidents on U.S. critical

[193] Polytechnique Montreal (19 October 2023) Cybersecurity: GEDAI Chair Created to Tackle Insider Threats. Online: https://www.polymtl.ca/carrefour-actualite/en/news/cybersecurity-gedai-chair-created-tackle-insider-threats
[194] *Ibid.*
[195] *Ibid.*
[196] *Ibid.*

infrastructure. The reality these incidents present for the Canadian critical manufacturing sector, is that it is not exempt from or immune to insider risk, and that if detection methods are not properly implemented to protect assets or "crown jewels" of an organization, it is susceptible to vulnerabilities such as insider risk incidents.

Wen conducting an industry review of AI tools or systems for detecting insider risk, there are options either currently being deployed with limited uses or are in some stage of development. Industry leading video management system providers are currently piloting and deploying minor AI enhancements to existing systems and are modifying their software to become more compatible with third party AI technologies. Challenges that remain with these systems are compatibility with existing security detection systems, limitations with generated results, and compatibility with other operational systems. In many cases, interconnected systems require extensive customization, back-end software engineering and maintenance, which is not particularly favourable in a cost-benefit analysis – at this stage of development anyhow. With how AI tools are currently being deployed in a limited capacity, it is not a 1-stop-shop solution for sector companies, rather it improves detection ability by flagging or alerting resources to increase response potential.

Among the various types of AI and AI subsets, research indicates machine learning and deep learning have the most potential for enhancing insider risk detection in critical manufacturing. In real-world use cases, technology companies are beginning to uncover the benefits that machine learning can provide that reduce the burden on human resource allowing for automated, routine tasks to be transferred to AI enhanced systems. The transition to "alarm-only" responses by human resources will effectively enhance detection efforts, allow quicker response times and reduce fatigue, and improve response quality. Additionally, there are opportunities for advanced AI systems to conduct behavioural assessments in the workplace, conduct risk assessments using features like

predictive analysis, and user behavior analytics (UBA) which will elevate and enhance insider risk detection far more proactively than that of human resources who monitoring in some cases multiple security devices. In manufacturing environments, which may have a larger impact on Canada's economy and national security, these features could prove extremely valuable and may demonstrate industry leading practices which could translate into marketable opportunities.

Of course, careful risk assessment and consideration will need to be applied for decision-makers in Canada's critical manufacturing sector, given that success in applying AI tools for insider risk detection have a larger interconnectedness with Canada's AI national strategy. Success in application of AI tools in this context, may demonstrate significant advancement for Canadian critical infrastructure security by further securing Canadian manufacturing processes which are recognized as a critical sector. It may indicate on a global scale that Canada is able to leverage such technology to effectively detect and mitigate insider risk at the industry level and deter insiders from committing undesired actions against an organization and Canada by default.

In Conclusion, based on the research conducted in this area, some identified best practices can be put forward for deploying AI tools in manufacturing environments to detect insider risk based on historical incidents, industry trends, and existing government standards. They are:

1. **AI-Specific Security Solutions.** Manufacturers, particularly those who already leverage AI tools for predictive maintenance, quality control, and supply chain optimization, should leverage AI-specific security solutions within their existing security infrastructure or industrial control systems. By protecting these systems with AI-specific security systems, will improve detection of abnormal behaviour patterns that might indicate a security breach or a malfunction in AI algorithms.

2. **Ensure Sufficient Monitoring of AI Systems.** Manufacturers should implement a routine monitoring system that can detect and respond to potential threats in real time and have resources identified to preform recovery actions immediately. Additionally, AI security tools can analyze large volumes of data which may need to be routinely monitored for any anomalies in the form of data poisoning, potential biases that may occur within the data or reports to ensure system optimization and compliance with ethical standards.
3. **Regular Risk Assessments.** As AI technologies evolve, so too do the risks associated with them. Manufacturers should conduct regular risk assessments to identify potential vulnerabilities in their AI systems and connected devices. These assessments should be part of a broader process evaluations in quality control, physical security or cybersecurity organization hygiene strategy that is continuously updated as new threats emerge.[197]

The evolution and application of AI tools will undoubtedly challenge conventional thinking when it comes to detecting insider risk and will present unlimited potential to leveraging this new technology in everyday work environments. Manufacturers in Canada, often industry leaders in innovation, provide the perfect testing grounds to incorporate AI machine learning detection tools in existing security systems and industrial control systems to determine suitability and effectiveness. The key turning point will be when manufacturing organizations decide to invest heavily in AI technology in the hopes of greater return on investment (and risk reduction), which may snowball other organizations to follow suite in implementing an AI insider risk detection system within their own organization.

[197] *Supra* note 32.

Appendix A

Mila Hydro-Québec Partnership

The world as we know it runs on electricity, and power lines are a critical infrastructure for delivering power to homes and businesses. To ensure their reliable operation, they must be routinely inspected for issues and anomalies, but manually inspecting the extensive networks requires significant time, resources, and manpower (Mila, 2025).

For several years, Hydro-Québec, a Mila partner organization, has worked to integrate robotics in power grid inspections, developing a fleet of robots to do the dangerous, dizzying task of skimming power lines hundreds of feet in the air (Mila, 2025).

Yet across the thousands of kilometers of power lines in Quebec, the odds of finding an anomaly — a scratch, a stain, a broken wire, or even just some bird poop — are deceptively rare (Mila, 2025). For that reason, the vast amount of collected data poses a significant analytical challenge, since the anomalies being identified are so uncommon. This question led to an applied research project between Mila and Hydro-Québec to help improve power line maintenance by efficiently identifying anomalies using AI (Mila, 2025).

More information on the project can be found on Mila's website:

https://mila.quebec/sites/default/files/styles/fixed_width_1200/public/news/11175/alexandru-boicu-h0z0ptvgvr8-unsplash.jpg.webp?itok=yUytklUV

Works Cited

LEGISLATION: CANADA

Bill-C27 *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*. (2022). 1st Reading June 17, 2022. 44th Parliament, 1st session. Retrieved from the Parliament of Canada <https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/441C27E>

SECONDARY MATERIALS: PARLIAMENTARY & GOVERNMENT DOCUMENTS

Ba, C. (15 November 2022) ScaleAI: Canadian Manufacturing Players at the forefront of AI. online: <https://www.scaleai.ca/blog/canadian-manufacturing-players-at-the-forefront-of-ai>

Business & Industry Canada (2 January 2025) 7 Game-Changing AI Applications Revolutionizing Canadian Manufacturing Today. online: <https://www.industryandbusiness.ca/7-game-changing-ai-applications-revolutionizing-canadian-manufacturing-today>

Communications Security Establishment (28 October 2022) Canadian Centre for Cyber Security: National Cyber Threat Assessment 2023-2024. Online: National Cyber Threat Assessment 202 <https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf3–2024.>

Communications Security Establishment (28 October 2022) Canadian Centre for Cyber Security: National Cyber Threat Assessment 2025-2026. Online: <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf>

Canadian Security Intelligence Service (2023) Insider Risk/Insider Threat presentation. Accessed online: <https://gccollab.ca/file/view/19080185/insider-risk-insider-threat>.

Chapman University (Accessed March 2, 2025) Bias in AI. Online: <https://www.chapman.edu/ai/bias-in-ai.>

Conference Board of Canada (October 29, 2018) The Insider Threat: Majority of Canadian Organizations Still Unclear on What It Means. Online: <https://www.newswire.ca/news-releases/the-insider-threat-majority-of-canadian-organizations-still-unclear-on-what-it-means-698885751.html>.

Cyber Security & Infrastructure Security Agency (Accessed March 5, 2025) Critical Infrastructure Sectors. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Cybersecurity & Infrastructure Security Agency (Accessed March 5, 2025), “Critical Manufacturing Sector” online: <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/critical-manufacturing-sector>.

Cybersecurity & Infrastructure Security Agency (June 2023) Introduction to the Critical Manufacturing Sector Risk Management Agency. Online: https://www.cisa.gov/sites/default/files/2024-06/Critical%20Manufacturing%20SRMA%20Fact%20Sheet%20New%20Template%202June2023_FINAL_508c.pdf

Cybersecurity & Infrastructure Security Agency (August 2019) “Insider Threat Programs for the Critical Manufacturing Sector” Implementation Guide. online:

<https://www.nationalinsiderthreatsig.org/itrmresources/CISA%202019%20Insider%20Threats%20Programs%20For%20The%20Critical%20Manufacturing%20Sector%20Implementation%20Guide.pdf>.

Felten, E., Raj, M. and R. Seamans. 2021. Occupational, Industry, and Geographic Exposure to Artificial Intelligence: A Novel Dataset and its Potential Uses. Strategic Management Journal 42(12): 2195-2217. Online: <https://www150.statcan.gc.ca/n1/pub/36-28-0001/2024009/article/>.

Fox Business (4 January 2023) Former GE employee sentenced for conspiring to steal trade secret for China. online: <https://www.foxbusiness.com/politics/former-ge-employee-sentenced-conspiring-steal-trade-secrets-china>.

Frenette, M., Mehdi, T. (25 September 2024) Statistics Canada: Exposure to Artificial Intelligence in Canadian Jobs: Experimental estimates. Online: <https://www150.statcan.gc.ca/n1/pub/36-28-0001/2024009/article/.>

Government of Canada (2025) Algorithmic Impact Assessment Tool. online: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>.

Government of Canada (4 March 2025) AI Strategy for the Federal Public Service 2025-2027: Overview. online: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/gc-ai-strategy-overview.html>.

IBM (6 July 2023) AI vs Machine Learning vs Deep learning vs neural networks: What's the difference? Online: <https://www.ibm.com/think/topics/ai-vs-machine-learning-vs-deep-learning-vs-neural-networks>.

Imperial Oil Article (2025) Safety. Accessed online: <https://www.imperialoil.ca/sustainability/people/safety#Performance>.

Infosecurity Magazine Article (4 January 2023) General Electric Insider Handed Two Years for IP Theft. online: <https://www.infosecurity-magazine.com/news/general-electric-insider-two-years>.

Innovation, Science and Economic Development Canada, (12 October 2021) "Canadian Manufacturing Sector Gateway" online: <https://ised-isde.canada.ca/site/canadian-manufacturing-sector-gateway/en>.

Innovation, Science and Economic Development Canada (accessed 2 March 2025) The Artificial Intelligence and Data Act (AIDA) - Companion Document. Online: <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s1>.

Inelegant Technologies (26 March 2024) Ethical Considerations in AI & Machine Learning. Online: <https://www.intelegain.com/ethical-considerations-in-ai-machine-learning>.

iTransition (21 March 2024) Machine Learning in manufacturing: key applications, examples & adoption guidelines. online: <https://www.itransition.com/machine-learning/manufacturing.>

Logpoint (20 January 2021) *Behavioral Approach to Security.* Online:

< https://www.logpoint.com/en/blog/behavioral-approach-to-security/.>

Madaio, Chen, J., Wallach, H., Wortman Vaughan, J. (April 2024) Tinker, Tailor, Configure, Customize: The Articulation Work of Customizing AI Fairness Checklists. online: <https://www.microsoft.com/en-us/research/publication/tinker-tailor-configure-customize-the-articulation-work-of-customizing-ai-fairness-checklists/.>

Madaio, M., Stark, L, Wallach, H., Wortman Vaughan, J. (March 2020) Co-Designing Checklists to Understand Organizational Challenges and Opportunities around Fairness in AI. online: <https://www.microsoft.com/en-us/research/publication/co-designing-checklists-to-understand-organizational-challenges-and-opportunities-around-fairness-in-ai/>

Mader, Dr. A. (Date Unknown) Smiths Detection: Automatic Object Recognition in Aviation Security online: <https://hello.smithsdetection.com/hubfs/Aviation_Whitepaper_AIandObjRecog_1.pdf?hsCtaTracking=0aa7a202-c944-4f6b-ace9-0cda50ecb792%7C12da59e2-bdae-4a29-91dd-5c7865a2dfba.>

McKinsey & Company (19 January 2023)"What is Generative AI?" online: <https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai.>

Mila (21 February 2025) AI-Powered Inspections: Hydro-Quebec Case Study online: <https://mila.quebec/en/news/ai-powered-inspections-hydro-quebec-case-study.>

Natural Resources Canada (2022) The Canadian Critical Minerals Strategy. online: <https://www.canada.ca/en/campaign/critical-minerals-in-canada/canadian-critical-minerals-strategy.html#a2.>

Natural Resources Canada (9 November 2023) Machine Learning, technical service highlights. online: <https://nrc.canada.ca/en/research-development/products-services/technical-advisory-services/machine-learning.>

Next Generation Manufacturing Canada (24 January 2025) A Proactive approach to cybersecurity in advanced manufacturing. online: <https://www.canadianmetalworking.com/canadianfabricatingandwelding/article/automationsoftware/a-proactive-approach-to-cybersecurity-in-advanced-manufacturing.>

OECD (5 March 2024) Explanatory memorandum on the updated OECD definition of an AI system. online: https://www.oecd.org/en/publications/explanatory-memorandum-on-the-updated-oecd-definition-of-an-ai-system_623da898-en.html.

OECD (29 May 2007) Staying Competitive in the Global Economy: Moving Up the Value Chain. Online: <https://www.oecd.org/en/publications/staying-competitive-in-the-global-economy_9789264034259-en.html>

Oprea, A. (November 2022) Northeastern University: Poisoning Attacks Against Machine Learning: Can Machine Learning Be Trustworthy? Online: <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934932.>

Perception Point (Accessed 2 March 2025) Top 6 AI Security Risks and How to Defend Your Organization. Online: <https://perception-point.io/guides/ai-security/top-6-ai-security-risks-and-how-to-defend-your-organization.>

Polytechnique Montreal (19 October 2023) Cybersecurity: GEDAI Chair Created to Tackle Insider Threats. Online: <https://www.polymtl.ca/carrefour-actualite/en/news/cybersecurity-gedai-chair-created-tackle-insider-threats>

Ponemon Institute (2020) 2020 Cost of Insider Breach Report. online: <https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/.>

Public Safety Canada, (2019) “Enhancing Canada’s Infrastructure Resilience to Insider Risk online: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/nhncng-crtcl-nfrstrctr-en.pdf.>

Public Safety Canada, (21 July 2022) “National Strategy for Critical Infrastructure” online: < https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx.>

Public Safety Canada, (21 July 2022) “National Strategy for Critical Infrastructure” *Implement all-hazards risk management approach* online: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.>

Public Safety Canada, (2019) “Enhancing Canada’s Infrastructure Resilience to Insider Risk online: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncng-crtcl-nfrstrctr/nhncng-crtcl-nfrstrctr-en.pdf>

Resolver (2025) AI Intelligent Triage. Online: https://www.resolver.com/ai/

Robbins, S., Yaqoob, A. (8 July 2024) ResearchGate: Ethical Concerns in AI-Enhanced Job Performance Metrics in Human Resources. Online: <https://www.researchgate.net/profile/Steven-Robbins-12/publication/382073534_Ethical_Concerns_in_AI-Enhanced_Job_Performance_Metrics_in_Human_Resources/links/668bebe4af9e615a15d70a73/Ethical-Concerns-in-AI-Enhanced-Job-Performance-Metrics-in-Human-Resources.pdf>

Splunk Artificial Intelligence for Observability (Accessed March 22, 2025) An Introduction Use Case Guide. Online: <https://www.splunk.com/en_us/pdfs/gated/ebooks/eight-use-cases-for-ai-in-observability.pdf>

Statistics Canada (25 September 2024) Exposure to Artificial Intelligence in Canadian Jobs: Experimental estimates. Online: <https://www150.statcan.gc.ca/n1/pub/36-28-0001/2024009/article>

Stratejm (15 December 2021) *Security Orchestration Automation & Response (SOAR) in Action*. Video access online: <https://stratejm.com/recording-security-orchestration-automation-response-in-action/security-orchestration-automation-response-soar-in-action.>

Times Colonist (11 April 2024) Auto parts maker Magna international signs strategic partnership with Sanctuary AI. online: <https://www.timescolonist.com/automotive/auto-parts-maker-magna-international-signs-strategic-partnership-with-sanctuary-ai-8586145.>

Treasury Board of Canada Secretariat (25 April 2023) *Directive on Automated Decision-Making*. online: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592#appA.>

U.S. Department of Justice Archives (1 April 2022) Former GE Power Engineer Convicted of Conspiracy to Commit Economic Espionage. Online: <https://www.justice.gov/archives/opa/pr/former-ge-power-engineer-convicted-conspiracy-commit-economic-espionage.>

Whisnant, A. (October 2024) Carnegie Mellon University, Software Engineering Institute: *Dangers of AI for Insider Risk Evaluation (DARE).* Online: <https://insights.sei.cmu.edu/library/dangers-of-ai-for-insider-risk-evaluation-dare/.>