ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP074

MANAGING ROBOTICS AND DIGITIZATION RISK

D. Marais*, J. Mostert, R. Prinsloo, Necsa SOC Ltd, Pretoria, South Africa

Abstract

Robotic and digitization risks refer to the potential negative consequences that can arise from the use of robots and digital technologies in various industries, which include experimental physics control systems. Risks include the compromising or malfunctioning of these systems, resulting in injury, equipment damage, loss of data or disruptions to critical infrastructure and services. Notwithstanding the negative consequences, the benefits, including enhanced efficiency, productivity, accuracy, safety, cost savings, reduced human error, and real-time data access, typically outweigh the associated risks.

This paper provides a summary of how to moderate these risks by taking proactive steps to reduce the likelihood of negative consequences and minimize their impact if they do occur. A comprehensive risk management approach is proposed, that incorporates a combination of technical, organizational, and cultural strategies which can help mitigate the potential risks.

INTRODUCTION

Robotic risks primarily concern physical machinery and autonomous systems, such as manufacturing robots causing workplace injuries due to malfunctions, or self-driving cars involved in accidents due to unforeseen road conditions. Digitization risks are associated with the use of digital technologies and data; for example, data breaches due to insufficient cybersecurity measures, or business disruptions from software failures. Though there is an overlap, like a hacked robotic system causing harm, robotic and digitization risks are distinct categories, each presenting unique challenges and consequences.

In the field of experimental physics, where researchers not only delve into the fundamental mysteries of the universe, but also engage in more routine pursuits such as calibrating sensors or analysing large data sets, the integration of robotic and digital technologies brings both unprecedented potential and a distinctive set of risks.

Anecdotes

The advent of cutting-edge technologies like Large Language Models (LLMs) and text-to-image generators, used for tasks ranging from data analysis to experiment design, further amplify this potential and risk, setting the stage for a new era in experimental physics. These tools underscores the evolving landscape of risks in this field.

The following examples anecdotally highlights potential pitfalls and unforeseen consequences that can arise from the interaction between humans, machines, and digital transformation. These cases shed light on the delicate balance between innovation and vulnerability, emphasizing the importance of proactive measures to mitigate the adverse outcomes that can result from the rapid evolution of technology.

Bing Image Creator Bing Image Creator generates images from natural language descriptions using the DALL-E Artificial Intelligence (AI) backend [1]. This system offers the potential to significantly reduce both time and costs when generating improved visualizations across a wide array of scientific fields. These applications span from conceiving and portraying novel materials to simulating and visualizing robot behaviours and interactions in diverse scenarios. Care in using such a system must however be taken as natural language can easily be misinterpreted as is demonstrated in Fig. 1, where Bing Image Creator was asked to "*generate an image of a neutron powder diffractometer with a banana detector*". In the field of neutron scattering, a 'banana detector' is a neutron detector with a specific configuration and does not refer to a physical banana [2].

Figure 1: AI generated image of a neutron powder diffractometer with a banana detector.

ChatGPT ChatGPT is a language model developed by OpenAI, based on the GPT (Generative Pre-trained Transformer) architecture [3]. It is designed to generate human-like text based on the input it receives. ChatGPT is particularly well-suited for natural language processing tasks, including generating conversational responses, answering questions, providing explanations, and engaging in interactive text-based communication.

Whilst performing a literature review, ChatGPT was posed the question "*What is the best software for neutron guide design?*". It responded with descriptions of "Monte Carlo Simulation of Time-of-Flight Spectroscopy (McStas)", "Virtual Instrument for the Simulation of Spectrometer Experiments (Vitess)" and "Neutron Beam Line Analysis (NEBULA)". Upon posing a follow-up question as to where NEBULA can be obtained, the reply was as

* deon.marais@necsa.co.za

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP074

follows: "*I apologize for the confusion in my previous response. As of my knowledge cutoff in September 2021, there is no software tool called NEBULA specifically developed for neutron beam line analysis or neutron guide design.*".

This interaction highlights how powerful Artificial Intelligence (AI) can be by correcting itself, however it also emphasises that AI systems should not blindly be trusted in critical decision processes.

RISK EXAMPLES

Robotic Risk

Within robotic risks lies the delicate balance between innovation and uncertainty stemming from the harmonious yet complex interaction between humans and machines. The machinery and automated systems that populate experimental setups hold the promise of enhancing precision, efficiency, and the capacity for ground-breaking discoveries. However, this very complexity also serves as a breeding ground for potential challenges.

One of the foremost concerns is the possibility of malfunctioning instruments. The movement of robotic arms and positioning apparatus can falter due to mechanical failures or even autonomous information integration, resulting in technical anomalies that disrupt data collection or compromise the integrity of experiments. Researchers, who entrust these systems to perform flawlessly, find themselves facing the unforeseen consequences of automation.

Yet, the risks stretch beyond mere technical errors. The convergence of robots and human researchers can lead to convoluted scenarios where safety hazards emerge. The fusion of robotic precision and experimental unpredictability can, paradoxically, create circumstances where robots inadvertently become sources of danger. Researchers working in close proximity to sensitive equipment and materials might encounter unanticipated safety risks as robots navigate their surroundings.

Data integrity, which refers to the accuracy, consistency, and reliability of data, forms yet another pivotal point of robotic vulnerability. Data integrity may be compromised due to human error, software bugs, hardware failures and software updates to name but a few. Errors propagated by robotic systems, whether in data acquisition or processing, can cascade into inaccuracies that undermine the reliability of experimental results. The convergence of automation and sophisticated scientific inquiry accentuates the need for rigorous validation and monitoring to safeguard the purity of research outcomes.

Moreover, the shift towards robotics can inadvertently trigger a form of dependency on automation. The delegation of tasks to robotic systems, while augmenting research capabilities, could potentially erode researchers' hands-on skills. This raises concerns about the ability to troubleshoot technical issues that may arise, and whether the mastery of intricate, manual techniques could be lost in the quest for automated precision.

Digitization Risk

The transformation of analogue information into digital formats has brought many advantages for collecting, analysing, and sharing data. However, this move to digital isn't without its challenges, especially in experimental physics.

One major concern is data security. The convenience of digital storage comes with the risk of data breaches, which can have a significant impact on years of research. The consequences of a breach extends beyond the compromise of sensitive data; it undermines the integrity of research outcomes and scientific progress.

In the pursuit of efficiency and ease of access, digitization can paradoxically present both benefits and risks. The unintended loss of data or the complete breakdown of digital systems, whether stemming from hardware malfunctions, software glitches, cyberattacks, or human oversight, can severely obstruct the advancement of research. Furthermore, these disruptions may give rise to dire consequences, including safety hazards and potential environmental repercussions.

Data quality and reliability are critical in experimental physics. The digitization process can however introduce an element of uncertainty through various mechanisms, such as interpolation, data model extension and unintended operation in ranges outside of applicability. Errors propagated during the digitization process can creep into datasets, casting doubt upon the accuracy of experimental results.

Additionally, digitization can change how collaborations are facilitated, often requiring adjustments in communication methods, tools, and platforms to accommodate the digital environment. While digitizing data assists in sharing knowledge, the lack of consistent standards can make it difficult for effective data exchange, hindering interdisciplinary cooperation and scientific advancement.

MITIGATION STRATEGIES

Mitigating robotic and digitization risks involves taking proactive steps to reduce the likelihood of negative consequences and minimize their impact if they do occur. Overall, a comprehensive risk management approach that incorporates a combination of technical, organizational, and cultural strategies can help mitigate the potential risks associated with the increasing use of robotics and digitization. Some ways to mitigate these risks include the implementation of the following strategies.

Appropriate and Efficient Integration

Appropriate and efficient integration of new robotic and digital systems, processes, or technologies is crucial for organizations to optimize their operations, enhance productivity, and achieve their strategic objectives. This however has an associated risk which can be managed by following the guidelines proposed:

- Define clear objectives and requirements as to what the specific functionalities are for the new system to be implemented.
- Conduct a comprehensive assessment of existing systems, processes, and data to identify integration points,

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP074

potential challenges, and opportunities for improvement.

- Standardize data formats, data mapping and transformation rules, coding, and naming conventions to ensure seamless data exchange between systems. This helps avoid data inconsistencies and integration errors.
- Customize the systems to meet specific requirements and conduct thorough testing to identify and rectify integration, software or hardware malfunctions.
- Develop a change management plan to help employees adapt to the new systems and provide adequate training.
- Maintain thorough documentation of the integration process, configurations, and any customizations. This documentation is invaluable for troubleshooting and future upgrades.

Maintenance and Testing of Systems

Regular maintenance and testing of robotic systems is needed to ensure they are functioning properly and can identify and address any potential issues before they become major problems. A typical maintenance strategy for robotic systems includes the following:

- Develop a regular maintenance schedule based on the manufacturer's recommendations and the specific operating conditions of the robotic system. The schedule should include routine inspections, cleaning, and lubrication of mechanical components, as well as testing of sensors, controllers, and other electronic components.
- Conduct preventative maintenance to identify and address potential issues before they become major problems. This can include checking for signs of wear and tear, monitoring performance data, and replacing components that are nearing the end of their lifespan.
- Provide training to staff on the proper maintenance procedures and best practices for safe operation of the robotic system. This should include instructions on how to identify potential issues and how to perform routine maintenance tasks.
- Keep accurate records of all maintenance activities, including the date, time, and details of any repairs or replacements made. This can help identify trends or recurring issues and guide future maintenance decisions.

Cyber Security Measures

Cyber security involves a range of technical, managerial, and operational measures with specific emphasis on the practice of protecting computer systems, networks, and digital devices from unauthorized access, theft, damage, or disruption of information and services. It is an increasingly important area of concern for individuals, businesses, governments, and other organizations in the digital age, where cyber threats are becoming more frequent and sophisticated. Cyber security aims to ensure the confidentiality, integrity, and availability of digital assets and protect against various cyber threats, such as malware, phishing, hacking, and other types of cyber-attacks.

A strategy for implementation of strong cyber security measures includes the following:

- Conduct a risk assessment to identify potential cyber security threats and vulnerabilities to digital systems.
- Develop a cybersecurity policy that includes guidelines and procedures for data security, access control, incident response, and employee training.
- Implement technical controls, such as firewalls, intrusion detection and prevention systems, encryption, and anti-virus software.
- Conduct regular vulnerability assessments and penetration testing to identify and address any weaknesses or vulnerabilities in digital systems.
- Establish a security incident response plan to quickly respond to and mitigate cybersecurity incidents, including notification procedures, containment strategies, and recovery plans.
- Provide ongoing training and awareness programs for employees to promote safe and secure use of digital systems and data.

Employee Training and Awareness Programs

Employee training and awareness programs to educate staff on best practices for data security and safe use of robotic systems, as well as protocols for responding to potential cyber threats should be implemented.

A strategy for implementing an Employee Training and Awareness Program with respect to data security and safe use of robotic systems includes the following:

- Develop a training program that covers data security policies and procedures, safe use of robotic systems, and cyber threat awareness. This should be tailored to the specific needs and roles of employees and should include practical exercises and real-life scenarios.
- Provide regular training sessions for all employees, including new staff, on the importance of data security and safe use of robotic systems. This should include information on how to detect and report security incidents and how to follow incident response procedures.
- Conduct simulated phishing attacks and other social engineering exercises to test employees' knowledge and awareness of cyber threats and data security practices.
- Use gamification and other interactive training methods to engage employees and reinforce the importance of data security and safe use of robotic systems.
- Develop a communication plan to regularly remind employees about the importance of data security and safe use of robotic systems. This can include newsletters, posters, and email reminders.

Industry Standards and Best Practices

There are several industry standards and best practices that organisations can follow for managing robotics and digitization risk in order to protect sensitive information, and ensure the safety of workers and the public. Some examples are as follows:

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP074

- ISO/IEC 27001: This is an international standard for information security management systems. It provides a framework for managing and protecting sensitive information, including data related to robotics and digitization [4].
- NIST Cybersecurity Framework: Developed by the National Institute of Standards and Technology (NIST), this framework provides guidelines for improving cybersecurity across a variety of industries, including robotics and digitization [5].
- IEC 62443: This is a series of standards developed by the International Electrotechnical Commission (IEC) for industrial control systems security. It provides guidelines for securing industrial automation and control systems, which may include robotics and digitization [6].
- IEC 61508: This is a standard for functional safety of electrical, electronic, and programmable electronic safety-related systems [7].
- ANSI/RIA R15.06-2012: This is a safety standard for industrial robots developed by the Robotic Industries Association (RIA). It provides guidelines for the design, construction, and operation of industrial robots to ensure the safety of workers and the public [8].
- ISO 10218-2: This is another safety standard for industrial robots which provides guidelines for the safety requirements of industrial robot systems and their integration [9].
- IEEE Standards: The Institute of Electrical and Electronics Engineers (IEEE) has developed numerous standards related to robotics and digitization.
- Best Practices: There are several best practices that organizations can follow to manage robotics and digitization risk, such as regularly updating software and firmware, implementing strong passwords and access controls, conducting regular risk assessments, and providing employee training and awareness programs.

A strategy for implementing the adoption of industry standards and best practices includes the following:

- Conduct a thorough risk assessment to identify potential reliability and safety risks related to the use of robotic and digital systems. This should include a review of all system components, including hardware, software, and networking infrastructure.
- Review relevant industry standards and best practices related to the reliability and safety of robotic and digital systems.
- Develop a plan for implementing the identified standards and best practices in the organization. This should include the development of policies, procedures, and guidelines for the use of robotic and digital systems, as well as training and awareness programs for employees.
- Implement regular maintenance and testing of robotic and digital systems to ensure that they are functioning as intended and in compliance with industry standards and best practices.
- Conduct regular audits and assessments to ensure that the organization is meeting the required standards and best practices for the reliability and safety of robotic and digital systems.

Contingency Plans and Backup Systems

Contingency plans and backup systems are measures taken to mitigate the risks associated with robotic and digitization systems. These plans and systems are put in place to ensure that, in the event of a system failure or other emergency, the impact on the organization's operations is minimized, and that the system can be quickly restored to its normal state and that critical operations can continue even in the event of an emergency. Together, contingency plans and backup systems help to ensure the reliability and safety of robotic and digitization systems.

A strategy for implementing and developing contingency plans and backup systems include:

- Identify critical components of the robotic and digital systems that could impact safety or reliability if they were to fail. This could include hardware components, software systems, and networking infrastructure.
- Develop a comprehensive contingency plan that outlines how to respond in the event of a system failure or other emergency. This plan should include procedures for system shutdown, backup and recovery, and alternative operating procedures.
- Implement backup systems for critical components, such as redundant servers or backup power supplies. These systems should be regularly tested to ensure that they are functioning as intended and can be quickly activated in the event of a failure.
- Develop a communication plan that outlines how to communicate with stakeholders in the event of a system failure or emergency. This should include procedures for notifying employees, customers, and other stakeholders, as well as contingency plans for alternative communication methods if primary channels are unavailable.
- Regularly review and update the contingency plan and backup systems to ensure that they are still effective and relevant. This should include regular testing and evaluation of backup systems and procedures.

Ethical and Social Guidelines

Ethical and social guidelines with respect to robotic and digitization risk refer to principles, policies, and practices that guide the development, deployment, and use of robotic and digital systems in a manner that aligns with ethical and social values. These guidelines are designed to ensure that robotic and digital systems are safe, reliable, and beneficial for individuals and society as a whole. Some common ethical and social guidelines with respect to robotic and digitization risk includes:

- Privacy: Personal information must be protected from unauthorized access, use, and disclosure. This can include measures such as data encryption, access controls, and data minimization.

ISBN: 978-3-95450-238-7 ISSN: 2226-0358 doi:10.18429/JACoW-ICALEPCS2023-TUPDP074

- Transparency: Robotic and digital systems must be open and transparent in their operation. This can include measures such as providing clear explanations of how the systems work, making data available to users, and ensuring that algorithms are explainable.
- Accountability: Measures such as establishing clear lines of responsibility and liability for system failures, and providing mechanisms for redress in the case of harm must be in place.
- Safety: Robotic and digital systems must be safe for individuals and society as a whole. This can be accomplished by designing systems with fail-safes and redundancies, and conducting regular risk assessments and safety tests.
- Human control and autonomy: Robotic and digital systems should be designed and used in a way that preserves human control and autonomy, and that does not compromise human decision-making and judgment.
- Social and environmental responsibility: Systems should be developed and used in a way that takes into account their social and environmental impact, and that contributes to the well-being of society.

A strategy for implementing and establishing clear ethical and social guidelines to ensure the reliability and safety of robotic and digital systems comprise the following:

- Establish a cross-functional team of experts, including technologists, legal experts, ethicists, and social scientists, to develop ethical and social guidelines for the use of robotic and digital systems.
- Conduct a thorough review of existing regulations and ethical standards related to the use of robotic and digital systems, such as those established by government agencies and industry associations.
- Develop a set of ethical and social guidelines that address issues such as privacy, data security, transparency, and accountability in the use of robotic and digital systems. These guidelines should be aligned with the organization's values and mission and should be communicated clearly to all stakeholders.
- Incorporate the ethical and social guidelines into the design and development of robotic and digital systems. This could include conducting ethical impact assessments and integrating privacy and security features into the systems.
- Establish a system for monitoring and evaluating the ethical and social impact of the use of robotic and digital systems. This could include conducting regular audits and assessments to ensure compliance with the guidelines and identifying areas for improvement.
- Continuously review and update the ethical and social guidelines to ensure that they remain relevant and effective in the rapidly evolving landscape of robotic and digital systems.

CONCLUSION

In addressing robotic and digitization risks within the realm of experimental physics infrastructure, a collaborative approach between technology developers, regulators, policymakers, and stakeholders is essential. Rigorous testing and validation of robotic systems, complemented by robust protocols for human-robot interaction, form a critical foundation. Embracing a culture of continuous training and learning ensures that researchers remain proficient not only in wielding the latest technology but also in addressing unforeseen challenges. By understanding and proactively mitigating these risks, the scientific community can harness the potential of robotics and digitization to unveil the secrets of the universe while ensuring safety, accuracy, and the integrity of their endeavours.

ACKNOWLEDGEMENTS

This contribution is financially supported by the National Research Foundation (NRF) of South Africa, grant number 151509, and Necsa SOC Ltd. Any opinion, finding and conclusion or recommendation expressed in this material is that of the author(s) and the supporters does not accept any liability in this regard.

The author(s) generated this text in part with GPT-3, OpenAI's large-scale language-generation model. Upon generating draft language, the author reviewed, edited, and revised the language to their liking and takes ultimate responsibility for the content of this publication.

REFERENCES

[1] Bing Image Creator, www.bing.com/create

[2] V. Laliena, M. A. Vicente Álvarez, and J. Campo, "Routines for optimizing neutron scattering instruments with McStas", *J. Neutron Res.*, vol. 21, no. 3–4, pp. 95–104, 2019. doi:10.3233/JNR-190117

[3] ChatGPT, chat.openai.com

[4] ISO, *Information Security, Cybersecurity and privacy protection - Information Security Management Systems - Requirements*, Oct. 2022.

[5] M. P. Barret, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, Gaithersburg, MD, USA: NIST CSWP, Apr. 2018. doi:10.6028/NIST.CSWP.04162018

[6] *Security of Industrial Automation and Control Systems*, ISA/IEC 62443 Series of Standards, Sept. 2023. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[7] *Functional safety of electrical/electronic/programmable electronic safety-related systems,* IEC 61508*,* International Electrotechnical Commission, April 2010.

[8] *Industrial Robots and Robot Systems - Safety Requirements,* ANSI/RIA R15.06-2012, American National Standards Institute, March 2013.

[9] "Robots and robotic devices — Safety requirements for industrial robots" — *Part 2: Robot systems and integration,* ISO 10218-2:2011, International Organization for Standardization, Jul. 2011.