White Rose Research Online

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk
Universities of Leeds, Sheffield and York

Deposited via The University of York.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/id/eprint/247909/

Version: Published Version

Proceedings Paper:
JOGIA, VIRA, ALEXANDER, ROB and Garnett, PHILIP RICHARD (2025) Implications of AI on Process Safety. In: Hazards Process Safety Conference 35.

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

UNIVERSITY OF LEEDS
University of Sheffield
UNIVERSITY of York

Implications of AI on Process Safety

Author[1] Vira Jogia FIchemE CEng, Process Safety Consultant, VRJ Consultancy Ltd. Author[2] Dr Rob Alexander, Senior Lecturer Department of Computer Science, University of York. Author[3] Prof. Philip Garnett, Professor of Systems and Organisation & Society and Ethics Pillar lead at the Institute for Safe Autonomy, University of York.

Abstract

This paper evaluates the impact of AI on the IChemE Safety Centre (ISC) Process Safety Framework. This framework, used in industry, was chosen because it provides an abstract view of key aspects of process safety that an organisation should focus on, rather than a more detailed management system. This is an advantage for this research as the technology is new; therefore, we do not have a lot of answers. However, we use this as a starting point for the conversation and to raise awareness.

A recent rapid uptake of AI / ML technology within the process industry has been observed [1]. The drive for efficiency, sustainability, and competitiveness has led companies to trial cutting-edge innovations to enhance production, reduce costs, and improve safety standards [1], [2]. However, AI increases complexity and has significant implications for Process Safety [2], [3].

The ISC's process safety framework, which is underpinned by leadership, offers "a structured approach to understanding and managing process safety across an organisation. It is not a management system but rather a framework that helps organisations view process safety through six key functional areas" [37]

1. Knowledge & Competence
2. Engineering & Design
3. Systems & Procedures
4. Assurance
5. Human Factors
6. Culture

It is deduced that the use of AI creates additional and not well-understood complexities; however, it is up to the end user to weigh up the benefits versus the complications created by the AI.

Background

Although the idea of this subject of safety issues related to the uptake of AI / ML technology within the process industry is not new, there have been voices that have discussed the safety implications of adopting AI since 2008 [2], [4], [5], [6], [7]. However, one significant change is that there has been a rapid uptake of AI technology.

The current and future trends show that the industry is not slowing down with the adoption of new technology. The need to remain competitive has driven the uptake of technology in the process industries. For example, Vaidya et al 2018, Dotoli et al 2015, Napolene et al 2021, Jamsa 2007, S Von Delft et al 2021 [8], [9], [10], [11], [12] all outline that the rate at which process industries can respond to a changing market is crucial to gaining a competitive edge, hence the need for adopting new technology.

The literature to date has revealed numerous benefits of adopting AI from a business perspective. The impact on yield, availability, overall equipment effectiveness (OEE) and claims for energy efficiency are the main positives [11]. However, research has yet to prove any real-world claims of improved safety.

Khan et al, 2021 [2] argue that the scale and complexity of chemical manufacturing processes increase as more and more parameters are integrated into the process. The chemical industry will have to deal with the complex issues created by AI and create a more collaborative, intelligent plant.

This paper highlights factors to consider when considering the use of AI from a process safety perspective. The IChemE Safety Centre (ISC) Process Safety Framework is not designed to provide a management system; however, it does aid organisations to focus on top-level aspects of process safety, such as 1. Knowledge & Competence, 2. Engineering & Design, 3. Systems & Procedures, 4. Assurance, 5. Human Factors, 6. Culture.

Research on the safety issues of AI technology is new; therefore, we do not have a lot of answers. However, we use this as a point to start the discussions.

Process Safety Frameworks

Process safety frameworks are adopted to prevent major accidents, such as explosions and toxic releases, thereby protecting lives and the environment. They are built to ensure regulatory compliance and promote a positive safety culture by adopting risk-based process safety management. [13]

In simple terms, a process safety management system integrates risk awareness and control into everyday operations, encouraging continuous improvement through regular audits and performance monitoring.[14]

We hear a lot of positive news about incorporating AI into PSM systems, from AI control systems and training AI to carry out HazOps to predictive analytics for forecasting equipment failures [15], [16]. However, we must also consider the new layers of complexity which arise from using AI [15]. Most of the time, AI is perceived as a black box making opaque decisions, there are new vulnerabilities to cyber attacks and an overreliance on AI [17]; all these aspects create unknown implications, which we attempt to unveil.

We will now go through the IChemE ISC PS framework and look at the implications of AI on process safety. Detailed PS frameworks, such as the CCPS or Energy Institute, which provide a management system, can not be used, as there are too many unknowns. Using the IChemE ISC PS framework as its top-level functions as a place to start discussions to see where AI will impact PS.

The ISC states that “The process safety framework is not a management system but simply provides a framework to view process safety across an organisation through six key functional areas.” [37].

Implications for Leadership

It is well reported that a lack of leadership and management is a key finding in the root cause analysis of major accidents. [18]. Therefore, we look at how leadership decisions to adopt AI and its implications for process safety.

Nordberg 2024 [19] states that the terms responsibility and accountability are intertwined and that “Conflicting usages appear even within the same text, such as corporate governance (CG) and corporate social responsibility (CSR) calling on companies to assume fiduciary and moral responsibilities towards stakeholders, framed as an act of accountability.”

For the purpose of this research paper, we will simply state that it is the responsibility of leaders and individuals involved in implementing new technology to assess the ethical and moral aspects of using AI in hazardous process industries. Whereas when considering accountability, it is acknowledged that AI is not a moral agent; therefore, it cannot be held responsible [20].

However, we do know that AI can make decisions, it acts and omits, and these affect outcomes, which can influence humans [21]. For example, AI can be used to collect, collate, and process safety data, and may, for some unknown reason, omit valuable information, leading to an incorrect decision being made.

The defence industry uses JSP 936v1.1 (2024), which provides guidance for the Ministry of Defence to ethically implement AI in military applications. The guidance is based around 5 principles: human-centricity, responsibility, understanding, bias and harm mitigation, and reliability. [22] This industry sector has started to consider the ethical and moral aspects of using AI. It is noted that JSP 936v1.1 (2024) advises the defence industry to seek legal advice, as the UK is compliant with laws governing the use of AI for military purposes, as well as with UN directives that may be impacted.

Hazardous process industry leaders can learn from JSP 936v1.1 (2024) to ensure the effective development and utilisation of AI. We interpret that they could seek appropriate counsel to ensure the approach aligns with current regulatory frameworks and laws, for example, the UK COMAH Regulations. Furthermore, any AI capabilities must be clearly communicated to all relevant stakeholders. This level of transparency is crucial for fostering trust and ensuring compliance within the AI landscape.

- *" Appropriate legal advice **must** be sought through existing channels at the beginning of AI project, & at relevant stages throughout programme, to ensure that all relevant national & international law relating to the development & use of AI, including associated data, are identified & complied with" [22]*
- *"Any systems of control to ensure use of AI-enabled capability is in line with national & international legal obligations **must** be clearly communicated to relevant stakeholders" [22]*

At the time of writing this paper, the chemical industry did not have its own guidance on AI assurance. As we are in a regulatory void, it should not mean that leaders after a major accident are allowed to say, "we didn't know". Existing regulations should be considered when adopting AI. The chemical industry can start by assessing whether or not existing regulations are being complied with if it adopts AI. We conclude that leaders should stay current with new regulations for the use of AI. Other industry sectors, such as aviation and automotive, have published guidance on governing the use of AI [23], [24]; therefore, leaders should become well-versed in these. Leaders should take legal advice about the use of AI in the chemical industry. They can also ask some helpful questions, such as: Who is responsible for the consequences of using AI? Who is liable to pay damages? Can I get insurance?

1 Knowledge and Competence

The ISC framework states, "Knowledge and competence is vital in all aspects of an organisation to ensure that decisions and tasks are undertaken correctly and with an understanding of consequences." [37]

Process Safety Management systems all refer to process knowledge management, which is linked to employee skills and competence [13]. Experienced people or subject matter experts (SMEs) generate detailed information about chemical processes, hazards, and controls. This knowledge and competence play a large part in the prevention of major accidents. This is of particular importance as AI will not replace humans nor will it have human judgment, including our tacit knowledge, more commonly referred to as "gut feelings".

We recognise two key aspects where the adoption of AI impacts knowledge and competence. Firstly, the ageing workforce in the UK and secondly, the changing nature of knowledge required to safely adopt AI in high-hazard industries.

A large proportion of the chemical industry is nearing retirement, which means essential knowledge and expertise will leave the companies. The importance of employee experience and knowledge is highlighted by Schinner et al [25] who say "companies increasingly depend on the knowledge, skills, and experience of their older workers".

For example, Murray 2014 and Saleem et al 2018 [26], [27] state that an organisation such as NASA "was unable to return to the moon because they no longer had knowledge of how to build rockets and spacecraft due to the loss of knowledge workers through retirements and deaths."

A similar issue is being faced in the oil and gas industry, where essential pockets of knowledge will be lost due to employees departing. People with 30 years of experience, knowledge, competence and skillsets in the industry comprise a very specialised knowledge base [27].

The loss of knowledge and competence due to an aged expert-level workforce leaving industry is already impacting an organisation's ability to identify and assess hazards [1], [28]. This adds to the issue, creating a new complexity to an organisation's ability to incorporate technological advances safely.

Previous research demonstrated that there is a long timeframe involved for employees to become subject matter experts [1], [28]. Joe et al [29] also highlight the "distinction between base knowledge, which is established through education, such as an academic qualification, and the experience that needs to be built on this foundation". The challenges arise from the loss of knowledge and the time it takes to generate SMEs versus the rapid uptake of AI. In an era where employees are now expected to adopt technologies such as AI, which bring about more complex interactions [25], this creates a new level of complexity that the chemical industry should take note of to ensure an organisation's ability to incorporate technological advances in a safe manner.

We propose that SMEs will need new skills, and that engineering teams may require a different membership. For example, a traditional engineering design team, consisting of a chemical engineer, a mechanical engineer and an EC&I engineer, may also require a data engineer or, better still, a specialist software engineer who understands the chemical industry.

The second aspect where the adoption of AI impacts knowledge and competence is understanding what knowledge is required. Khan et al. speak of required reviews of the chemical engineering curriculum to understand the gaps in education [2]. However, the impact is not only at a university level but also needs to be considered for the current chemical engineers in industry. We should be asking what competencies and skills are required to use AI in a risk-aware manner responsibly.

The EU AI Law 2024 states, "employees should have necessary skills & knowledge on how to use AI technologies such that the company can prove risks such as discrimination, incorrect decisions or data misuse are minimised. From 2025, companies must prove that they have the necessary AI expertise to meet legal requirements". However, it is not detailed as to how organisations are expected to carry out the practicalities. This is a problem until there is some detail regarding the safe application of AI.

The UK MoD guidance JSP 936 states that, "All roles associated with AI development & use *should* be analysed for appropriate competency requirements. Appropriate training & supervision must be provided to all staff until sufficient competence is acquired"

We recommend that organisations adopting AI should review competency requirements and assess how they can build that knowledge into their organisation prior to adopting AI.

2 Engineering and design

The ISC framework states, "Engineering and design is about applying the hierarchy of controls in the design of equipment and safety systems. This includes the concept of inherently safer design as a starting point [37]. This area also includes design across the entire life cycle of the asset and the application of robustly engineered safety systems." [37]

Regardless of incorporating a hierarchy of controls into the design, there are new complexities to consider. For example, the adoption of AI to control chemical processes also increases the number of process parameters, which in turn increases the degree of complexity [2]. We do not yet know whether high-hazard industries have the ability to cope with the complexities being introduced by AI.

An Inherently Safer Design incorporates four pillars: (i) minimise, (ii) substitute, (iii) moderate, and (iv) simplify [30]. Our research [1], [28] so far has revealed many benefits of adopting AI from a business perspective; however, it is yet to prove any safety assurance claims. The main reasons which lead to this gap in research are, firstly, due to the availability of information from industry. Autonomous systems have not been in use long enough to provide substantial failure data for researchers to analyse. This lack of real-world data is an important factor, as it presents an opportunity for industry and academics to develop viable solutions to reduce risk and provide assurance before a major accident. Secondly, there is a lack of tools and techniques

to assess the assurance claims created by new technology. As Khan et al say [2], “Process system complexity continues to evolve in a manner demanding more sophisticated methods to assess and manage process safety.”

At this stage, we have to ask if we, as chemical engineers, are going against the grain by adding more complexity to engineering design, where the aim has been the Kletz engineering concept of an Inherently Safer Design [6], [31].

If we do not have the ability to assess an algorithm, how can we prove that we understand what can go wrong? This is the reality of AI model algorithms. We can focus more on architecture, data set validations and failure rate acceptance criteria for the AI, but we will never truly know about the emergent behaviours of the AI.

Based on what we know so far, organisations are faced with the question of whether adopting AI to control chemical processes at this stage is a risk they are willing to accept. We continue this line of thought in part 4, when discussing assurance.

3 Systems and procedures

As stated on the ISC website, “Systems and Procedures define how an organisation undertakes all manner of business activities. Consistent approach to decisions from governance to job tasks”. [37]

The benefits of using AI to speed up routine workflows were discussed during the previous two Hazards Conferences (Hazards 33 and Hazards 34). For example, presentations were given on using AI-HazOp by C. Nicholls and A. Keddie, utilising technology such as big data to collect and collate data and enhancing monitoring and reporting capabilities by HPCL Mittal Energy.

Despite the widely discussed benefits, there are some challenges that should be acknowledged. The topics from the presentations at the Hazards conferences lay the foundation for us to discuss the challenges around technology and infrastructure within this section.

The first issue regarding the technology is its impact on security. Recent cyberattacks on well-established and trusted companies such as Marks & Spencer and COOP [17] have raised concerns for all. On high-hazard sites, the stakes would be extremely high if a malicious party were to exploit security vulnerabilities. Therefore, we ask the following questions: What would be the security considerations for something as simple as AI used for production scheduling, to more complex uses such as controlling a chemical process? Does the organisation have the skill set to ensure the cybersecurity of an AI?

The second challenging area is around data quality. For example, using AI for data entry or scheduling production can be beneficial in that it reduces human error, results are achieved quickly, and decision-making is streamlined. However, we should consider the accuracy of the data and whether we can rely on it. Are the decisions being made transparent so they can be interpreted?

Lastly, the infrastructure necessary to utilise AI effectively should be considered. Architecture is a significant design aspect when implementing AI. For example, computing power, data storage, network considerations, memory requirements, data privacy, access, reliability, maintenance, and additional tools and platforms for the AI.

In theory, the implementation of AI in systems and procedures shows promise, but upon closer examination, we find several key considerations that need to be addressed. It is advisable, from a process safety perspective, that adopting AI for systems and procedures should undergo a management of change process. As well as reviewing the requirements under ISO/IEC 42001 Artificial Intelligence Management Systems (AIMS).

4 Assurance

The ISC website defines assurance as “a programme for the systematic monitoring and evaluation of all aspects of a business. Inspection, testing, monitoring, verification, and audit.” [37]

The UK government published guidance, Introduction to AI assurance, in February 2024, which provides details on aspects to incorporate if you adopt AI and how organisations are required to assure their AI.

We summarise the key points from the Introduction to AI assurance guidance for an organisation to consider.

- Firstly, the AI must incorporate existing regulations, for example, the UK COMAH Regulations would be key for the chemical industry.
- Secondly, organisations should consider training and upskilling their employees to deal with AI effectively.
- Third, it is essential to review internal governance and risk management frameworks to cope with AI effectively.
- The final aspect is to stay up to date on new regulatory guidance on AI, data protection, cybersecurity, and other relevant areas [32].

We note that the UK Introduction to AI assurance lacks technical guidance and practical implementation methods; instead, it outlines key concepts that organisations should focus on to provide AI assurance.

The use of AI in our plants and processes, when AI is a complex system, requires an organisation to assure the AI. Whether organisations are using AI or considering its use, we encourage you to incorporate assurance in the design stages. The UK government's Introduction to AI assurance guidance provides an introduction to essential concepts for organisations to consider. Still, it falls short as it lacks practical application steps for high-hazard industries. There are also other standards, such as ISO/IEC TR 5469:2024 Artificial intelligence — Functional safety and AI systems, and ISO/IEC TR 23894:2023 Information technology — Artificial intelligence — Guidance on risk management. It remains unclear how organisations are expected to demonstrate the effective implementation of these concepts. However, the UK’s guidance on AI assurance does point the reader to ISO/IEC/IEEE standards for data bias.

Guidance without details on implementation ultimately means that it's up to the chemical industry to determine how to implement AI safely whilst adhering to existing regulations. However, at this stage, AI creates issues for compliance, as we are unable to know if your use is compliant.

5 Human factors

The ISC framework states, “Human factors explores the interaction between the human and their performance, the job and the organisation. This goes beyond only ergonomics and explores other aspects of the interaction.” [37]

AI technologies will change the role of humans working in organisations, including those involved in high-hazard industries. Kirwan 2025 [33] states, “Since AI will inevitably push the boundaries of traditional human-automation interaction, there is a need to revisit Human Factors to meet the challenges of future human-AI interaction design.”

Kirwan 2025 provides a background via a visual evolution of human factors and AI technology depicted in Figure 1. Kirwan 2025 states that, “Human Factors need to be reviewed, and updated in the context of AI”. As Figure 1 shows, a great deal of work has been conducted in the field of human factors, as depicted by the timeline showing the Parallel Evolution of AI in the lower section and Human Factors in the upper section [16]. Initially, the concept of AI was to replicate human capabilities; however, due to increased computing power, the design focus changed to surpassing human capabilities. Likewise, human factors have always focused on human work and interaction with machines.

Currently, human operators on a chemical plant with automation have a clear understanding of the actions taking place and their reasons. They are also able to intervene as they are trained to understand the logic behind the control system and the

process. Whereas a chemical plant with autonomous functionality has opaque decisions, and a human operator could be left guessing as to why the control system has made certain decisions. The dynamic between the human operator and the AI is uncertain; for example, would the human be expected to take over from the AI in an emergency, and how would the human gain the necessary data to make decisions in an emergency from a black box?

Human control may shift to a basic role of checking that the AI is operational, rather than a more engaged and informed monitoring role. This poses challenges, which involve deciphering the AI's decisions as well as knowing when and how to intervene. There are other predicaments, such as short timeframes for decision-making, issues with maintaining vigilance, and the necessity for real-time situational awareness about the system's perceptions and planning. Additionally, it raises questions about how safety-critical interventions may be affected.

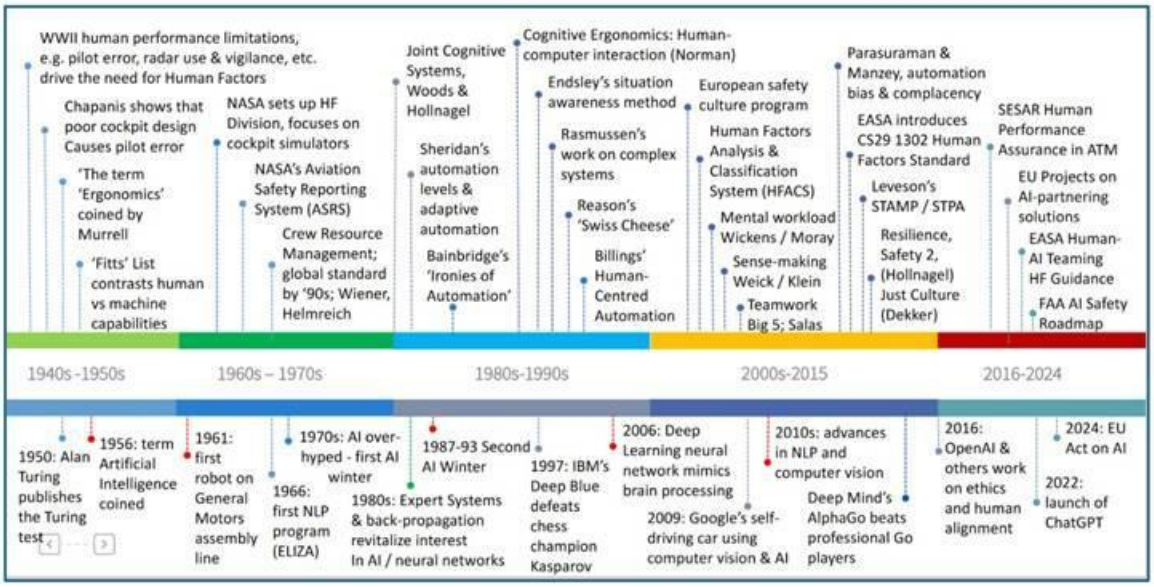


Figure 1 Timeline of Parallel Evolution of AI (lower section) and Human Factors (upper section), from Kirwan 2025 [16]

6 Culture

The ISC framework states, "Culture is the most commonly defined as 'the way we do things around here. This quote was first used by Bower in 1966. Understanding and shaping 'the way we do things" shapes people's attitudes about safety and how they do their tasks." [37]

Safety culture is a broad topic with socio-technical aspects that can significantly impact an organisation's culture. Bisbey et al 2021 [34] describe safety culture as being part of the larger organisational culture and its impacts on employees are linked to their attitudes and behaviours.

The long-term impact of adopting AI in high-hazard industries is simply unknown at the moment. Instead, we focus on what we know about current enablers of safety culture, such as responsibility and accountability [34]. Organisations have had to understand human factors and human behaviour to understand how best to affect safety culture in a positive manner [35]. High-hazard industries adopting AI should now consider the impact on existing humans and their subsequent reactions towards the new technology, especially if their job roles are going to change.

Farrow 2024 [36] raises the aspect of how accountability can be constructive when it avoids blame, especially in high-risk environments. We ask the question of the new dynamics between humans and AI in the context of who would be responsible when something goes wrong. We recognise that it may be impossible to answer this question as the technology may be opaque due to its nature. The opaqueness and lack of transparency would impact any incident investigation. However, this question of responsibility and accountability when things go wrong is important to address, as it can significantly impact the organisation's culture.

Conclusions

This paper assesses the implications of AI on Process Safety by assessing the ISC Process Safety Framework. However, not all answers are readily available at the moment due to the newness of the technology in the industry; we encourage further research to be carried out and shared among peers.

To summarise, some key issues impacting process safety efforts are workforce skill levels, whether through deskilling or evolving skill requirements. Data challenges are significant and poorly understood, including issues like data inaccuracies and insufficient data. The most critical point is the difficulty in understanding the AI decision-making process.

The critical message to industry is that we need to start discussing responsible innovation and the impact of a regulatory void. Responsible innovation using AI should be able to meet current regulations. In contrast, irresponsible innovation in this context is using technology about which we have no operational knowledge, or the subsequent consequences of it, without regard for current regulations. From a process safety perspective, this indicates a lack of precaution and foresight. We should not wait for a major accident before we begin to learn.

Regulators like the UK's HSE are already adapting their approach to AI. They are asking organisations first to provide transparency and explainability, to take accountability for AI-driven decisions and lastly have appropriate risk assessments for AI systems. The practicalities of this are unknown, particularly whether compliance with regulations such as COMAH can be achieved, given the difficulties in demonstrating ALARP when using AI.

Further to this, we recommend and encourage organisations to start building AI knowledge, carry out organisational assessments of their data to check if it's ready, ensure they choose the right technology, understand how the technology works, what its functions are, and most importantly, study the unintended interactions, especially as these may result in serious consequences. Consider starting small with a pilot project and incorporating human oversight at all stages of the AI adoption process.

Lastly, for organisations adopting AI, it is necessary to consider whether there is a need to review their Process Safety Management systems and procedures with respect to the impact of accepting a level of risk that is not computable at this stage.

References

[1] Jogia, Vira, Alexander, Rob and Garnett, Philip, "Ambiguous terminology for advanced control systems can impact the perception of risk," *Institution of Chemical Engineers*, 2023, [Online]. Available: https://eprints.whiterose.ac.uk/204898/1/HAZ33_111_JOGIA_v3_final_submission.pdf

[2] F. Khan, P. Amyotte, and S. Adedigba, "Process safety concerns in process system digitalization," *Educ. Chem. Eng.*, vol. 34, pp. 33–46, Jan. 2021.

[3] J. Lee, I. Cameron, and M. Hassall, "Information needs and challenges in future process safety," *Digital Chemical Engineering*, vol. 3, p. 100017, Jun. 2022.

[4] R. Arunthavanathan, Z. Sajid, F. Khan, and E. Pistikopoulos, "Artificial intelligence – Human intelligence conflict and its impact on process system safety," *Digital Chemical Engineering*, vol. 11, p. 100151, Jun. 2024.

[5] S. Rathnayaka, F. Khan, and P. Amyotte, "Risk-based process plant design considering inherent safety," *Saf. Sci.*, vol. 70, pp. 438–464, Dec. 2014.

[6] F. I. Khan and P. R. Amyotte, "How to make inherent safety practice a reality," *Can. J. Chem. Eng.*, vol. 81, no. 1, pp. 2–16, May 2008.

[7] F. Khan, S. Rathnayaka, and S. Ahmed, "Methods and models in process safety and risk management: Past, present and future," *Process Saf. Environ. Prot.*, vol. 98, pp. 116–147, Nov. 2015.

[8] S. Vaidya, P. Ambad, and S. Bhosle, "Industry 4.0 – A Glimpse," *Procedia Manufacturing*, vol. 20, pp. 233–238, Jan. 2018.

[9] M. Dotoli, A. Fay, M. Miśkowicz, and C. Seatzu, "A Survey on Advanced Control Approaches in Factory Automation," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 394–399, Jan. 2015.

[10] A. Napoleone, A. Pozzetti, M. Macchi, and R. Andersen, "Time to be responsive in the process industry: a literature-based analysis of trends of change, solutions and challenges," *Prod. Plan. Control*, pp. 1–14, Jul. 2021.

[11] P. S.-L. Jämsä-Jounela, "FUTURE TRENDS IN PROCESS AUTOMATION," *IFAC Proceedings Volumes*, vol. 40, no. 1, pp. 1–10, Jan. 2007.

[12] S. von Delft and Y. Zhao, "Business models in process industries: Emerging trends and future research," *Technovation*, vol. 105, p. 102195, Jul. 2021.

[13] Centre for Chemical Process Safety, *Guidelines for Risk Based Process Safety*. in 1st edition (26 April 2007). Wiley Interscience, 2007.

[14] C. D. Nwankwo, S. C. Theophilus, and A. O. Arewa, "A comparative analysis of process safety management (PSM) systems in the process industry," *J. Loss Prev. Process Indust.*, vol. 66, p. 104171, Jul. 2020.

[15] P. Candidate Ehab Elhosary, O. Moselhi, and C. Bucur, "Evaluation of AI-assisted HAZOP Software Tools", [Online]. Available: https://www.icheme.org/media/27631/hazards-34-paper-175-elhosary-revised.pdf

[16] A. Kopbayev, F. Khan, M. Yang, and S. Z. Halim, "Fault detection and diagnosis to enhance safety in digitalized process system," *Comput. Chem. Eng.*, vol. 158, 2022, doi: 10.1016/j.compchemeng.2021.107609.

[17] M. Sakthivanitha1, S. Silvia Priscila2, Praveen B.M., "E-commerce security: An overview of AI driven threat / anomaly detection," *Int. J. Eng. Trends Technol.*, vol. 73, no. 6, Jun. 2025, doi: 10.14445/22315381/ijett-v73i6p114.

[18] Baker, "The B.P. U.S. Refineries Independent Safety Review Panel," Jan. 2007. [Online]. Available: https://www.csb.gov/assets/1/20/baker_panel_report1.pdf?13842

[19] D. Nordberg, “Filling empty vessels: accountability, responsibility, and corporate leadership,” *Strat. Lead..*, vol. 52, no. 5/6, pp. 41–56, Dec. 2024.

[20] B. Brożek and B. Janik, “Can artificial intelligences be moral agents?,” *New Ideas Psychol.*, vol. 54, pp. 101–106, Aug. 2019.

[21] G. Allen, “Understanding AI Technology,” Apr. 2020, [Online]. Available: https://apps.dtic.mil/sti/tr/pdf/AD1099286.pdf

[22] “JSP 936 V1.1 Dependable Artificial Intelligence (AI) in Defence Part 1: Directive,” Nov. 2024. [Online]. Available: https://assets.publishing.service.gov.uk/media/6735fc89f6920bfb5abc7b62/JSP936_Part1.pdf

[23] CAA, “CAP2970 CAA’s Strategy for AI Building Trust in AI 5 Principles for AI and Autonomy,” Feb. 2024. [Online]. Available: https://www.caa.co.uk/our-work/publications/documents/content/cap2970/

[24] I. 8800:2024 H. ai/catalog/standards/iso/f, “ISO/PAS 8800 Road vehicles — Safety and artificial intelligence,” Dec. 2024. [Online]. Available: https://cdn.standards.iteh.ai/samples/83303/0c6743b68df0446ca9872168dbbf2e19/ISO-PAS-8800-2024.pdf

[25] Matthias Schinner, Andr´e Calero Valdez(B), Elisabeth Noll, Anne Kathrin Schaar, Peter Letmathe, and Martina Ziefle, “Industrie 4.0’ and an Aging Workforce– A Discussion from a Psychological and a Managerial Perspective,” in *Human Aspects of IT for the Aged Population. Applications, Services and Contexts*, in Lecture notes in computer science. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 151–170.

[26] E. J. Murray, “A proposed method for assessing knowledge loss risk with departing personnel,” *VINE: The journal of information and knowledge management systems*, vol. 44, no. 2, pp. 185–209, Jan. 2014.

[27] S. M. Saleem, E. Tsui, R. Cheong, and S.-T. E. W. K., “Critical areas of knowledge loss when employees leave in the oil and gas industry,” *Journal of Knowledge Management*, vol. 22, no. 7, pp. 1573–1590, Jan. 2018.

[28] Jogia, Vira, Alexander, Rob and Garnett, Philip, “Skills and expertise required by chemical engineers to adopt new technologies,” 2024, [Online]. Available: https://eprints.whiterose.ac.uk/id/eprint/227316/1/HAZ34_150_Skills_Expertise_Required_By_Chemical_Engineers_To_Adopt_New_Technologies_Final_version.pdf

[29] C. Joe, P. Yoong, and K. Patel, “Knowledge loss when older experts leave knowledge-intensive organisations,” *Journal of Knowledge Management*, vol. 17, no. 6, pp. 913–927, Jan. 2013.

[30] G. Gómez, S. Rodríguez, J. Cadena, and F. Muñoz, “Kletz’s legacy for developing countries: Simple systems based on inherently safer design,” *J. Loss Prev. Process Indust.*, vol. 25, no. 5, pp. 843–847, Sep. 2012.

[31] J. Li, F. Goerlandt, and G. Reniers, “Trevor Kletz’s scholarly legacy: A co-citation analysis,” *J. Loss Prev. Process Indust.*, vol. 66, p. 104166, Jul. 2020.

[32] “Introduction to AI assurance,” Department for Science, Innovation & Technology, Feb. 2024. [Online]. Available: https://assets.publishing.service.gov.uk/media/65ccf508c96cf3000c6a37a1/Introduction_to_AI_Assurance.pdf

[33] B. Kirwan, “Human Factors requirements for human-AI teaming in aviation,” *Future Transportation*, vol. 5, no. 2, p. 42, Apr. 2025.

[34] T. M. Bisbey, M. P. Kilcullen, E. J. Thomas, M. J. Ottosen, K. Tsao, and E. Salas, “Safety Culture: An Integration of Existing Models and a Framework for Understanding Its Development,” *Hum. Factors*, vol. 63, no. 1, pp. 88–110, Feb. 2021.

[35] M. M. Abu-Khader, “Impact of Human Behaviour on Process Safety Management in Developing Countries,” *Process Saf. Environ. Prot.*, vol. 82, no. 6, pp. 431–437, Nov. 2004.

[36] K. Farrow, “Blame culture: The line between blame and accountability in policing,” *Polic. J. Policy Pract.*, vol. 18, p. aae034, Jan. 2024.

[37] “Framework” https://www.icheme.org/knowledge-networks/knowledge-resources/safety-centre/framework/ 12/08/2025