Skills for Assuring the Safe Adoption of Emerging Technology*

Matt Osborne[0000−0002−9941−4531] and Mark Nicholson[0000−0002−0954−4448]

Assuring Autonomy International Programme, Department of Computer Science, University of York, Deramore Lane, York, YO10 5GH, England
{matthew.osborne,mark.nicholson}@york.ac.uk
https://www-users.cs.york.ac.uk/mo705/

Abstract. As new and emerging technologies continue to pervade all aspects of society and commerce, we need to be confident that its adoption can and will be safe, and can be shown to be safe. A plethora of academic and grey literature considers the pitfalls and challenges to be faced by the advent of emerging technology, but offer no pragmatic steps to prepare for the safe adoption of emerging technology. The paucity of preparedness for safe adoption is underlined by the offerings of academic prospectuses - or rather the lack of offerings with regards to education and continuing professional development. Whilst we are able to highlight the challenges faced by an organisation seeking to adopt emerging technology, a substantial amount of further research is required before we can confidently recommend what competence looks like and how to provide the educational training needs associated with the safety assurance aspects of technology adoption.

Keywords: Safe Adoption · Emerging Technology · Competence.

1 Introduction

New and emerging technology continues to proliferate and pervade all aspects of society. Organisations are not immune from this proliferation. Whilst the adoption of emerging technology has the potential to realise resource, time, and cost benefits for an organisation, we must also ensure the adoption is safe - for all stakeholders. Key to the achievement of safe adoption is the establishment and management of competence. Competence is required of staff within an organisation, and this must be achieved demonstrably. To ensure competence, training needs analysis is required, followed by the provision of appropriate education and training at varying levels. For context, we first establish a definition for emerging technology.

* This work is funded by the Assuring Autonomy International Programme https://www.york.ac.uk/assuring-autonomy.

1.1 What Defines a Technology as Being 'Emerging'?

Frustrated at the lack of consensus on what constitutes an emerging technology (noting that this lack of consensus impacts the development of effective regulations - which in turn impacts the available support of the technology actually 'emerging'), Rotolo, Hicks and Martin embarked on a scientometric study to define and operationalise 'emerging technology' [21]. Their definition of emerging technology is as follows, and provides the context for this paper [21]:

"A radically novel and relatively fast-growing technology characterised by a certain degree of coherence persisting over time and with the potential to exert a considerable impact on the socio-economic domain(s) which is observed in terms of the composition of actors, institutions and patterns of interactions among those, along with the associated knowledge production processes. Its most prominent impact, however, lies in the future and so in the emergence phase is still somewhat uncertain and ambiguous".

Safety is a key emergent property which must be considered when adopting any technology, but it has significant uncertainty associated with it. Key decisions about the acceptability of safety lie with staff within an organisation. Further, mitigation of potential safety events is placed on operational staff using the technology. Emerging technology thus has a potentially large impact on the skills and associated competencies expected of staff in an organisation.

The rest of this paper is structured as follows. Section 2 considers what is needed to assure the safe adoption of emerging technology, Section 3 assesses the state of literature on what is needed to assure the safe adoption of emerging technology, and Section 4 considers what is required for effective skills management. The paper concludes in Section 5 by considering future research directions that are required to confidently assure the safe adoption of emerging technology.

2 Assuring the Safe Adoption of Emerging Technology

As new, emerging technology continues to proliferate and pervade all aspects of society, organisations are increasingly adopting such technology, but is this adoption safe?

Organisations may consider adopting emerging technology for many potential reasons, but when discussing 'technology' with respect to its safe adoption, we consider two distinct types:

- Technology adopted to improve safety
- Technology adopted to improve factors other than safety, but which may have an impact on safety nonetheless.

In considering the safe assurance of emerging technology we evaluate the challenges, the current state of literature regarding the safe adoption of emerging technology, academic and vocational training offerings, the impact on required

staff competencies and skills, and make recommendations for future research into policy and practice.

2.1 A Paradigm Shift in Safety Assurance for Emerging Technology

We are currently experiencing a steady state experience-based approach to safety assurance. The last major disrupter in safety-critical systems safety assurance was the advent of control and indication software in the 1990s. The advent of software required a re-think of recognised good practice which culminated in a plethora of Open Standards which (despite their detractors) have held firm as de facto functional safety standards (such as IEC 61508 [8], and ARP 4754A [5]). Since the advent of software, safety assurance has been predicated on the measurement and assessment of compliance/conformance with these standards, and there are no signs of any paradigmatic shift away from the processes and procedures currently described by the standards.

The advent of new, emerging technologies such as robotics and autonomous systems (RAS), and new ways of developing software (such as Machine Learning), represent a new, disruptive technology for which the existing safety standards are no longer relevant. A paradigm shift is required towards 'Responsible Innovation'. Responsible Innovation is defined by UK Research and Innovation (UKRI) as being:

> *"A process that takes the wider impacts of research and innovation into account. It aims to ensure that unintended negative impacts are avoided, that barriers to dissemination, adoption and diffusion of research and innovation are reduced, and that the positive societal and economic benefits of research and innovation are fully realised"* [22].

In a shift away from extant recognised good practice of the kind espoused by Open Standards, Responsible Innovation requires stakeholders themselves to determine and justify what 'good' looks like - and emergent technology such as RAS also implies that a new set of skills are required, including what is often referred to as 'soft skills'.

Soft skills involve the ability to undertake activities such as critical thinking, and the ability to develop alternative solutions, and judge these alternatives. We argue that the existing frameworks for managing safety competence and competencies are not fit for purpose when considering the new skills that emerging technology will necessitate, nor is there any sign that such frameworks are being reviewed/updated by stakeholders such as professional institutions.

3 The State of Literature with regards to the Safe Adoption of Emerging Technology

In this section we consider existing literature into the process of safely adopting emerging technologies, their associated competencies, and the current offerings

of educational institutions with regards to equipping the current and future workforce for the safe adoption of emerging technology.

We have considered four main types of literature in our research:

- Governmental and Organisational White papers
- Academic papers
- Grey literature (from organisations such as IOSH)
- Prospectuses of educational training providers.

These sources are considered collectively under four main themes, which are considered in turn:

1. Organisational
2. Technical
3. Regulation and Governance
4. Training, Skills, Knowledge, and Competence.

3.1 Organisational

Barwell et al [6] suggest the following checklist that an organisation could employ when considering the adoption of emerging technology. We have added to their original questions to specifically consider the *safe* adoption of emerging technology:

1. Will the technological solution provide the benefits expected?
   - Is the technological solution aiming to provide safety improvements?
   - How will the technological solution contribute to existing safety?
   -- Is the safety contribution positive or negative?
   -- Will the technology employ architectures that ensure safety?
2. Can the technological solution be integrated with the existing systems in a safe manner?
   - Can the proposed socio-technological solution be integrated effectively into the existing Safety Management System?
3. What new safety risks will a technological solution introduce into an organisation?
   - How will any new risks be managed?
4. What impact will the technological solution have on the working practices of those engaged in developing safety systems and safety assurance activities?
   - What impact will the technological solution have on competence and competencies?

3.2 Technical

As more technologies are developed/adapted for safety purposes, it is essential to unearth ways to improve the integration of technology within safety management practices [18]. A common failing when adopting emerging technologies is Systems Integration, along with an "incurable belief" that technology on its own will

yield positive results (i.e. not considering requirements on staff and staff training etc.) [6]. Further, organisations are not considering the relevance of ongoing risk measurement and assurance work as part of their training needs analysis.

New technologies such as RAS and ML change the interaction between humans and machines. They alter the ability of staff to maintain situational awareness. Thus technology change will delete elements of organisational roles, as well as adding new elements and changing others. This mix of unlearning, learning, and changing of competencies and skills is a significant challenge in terms of professional development, both initial and continuing.

3.3 Regulation and Governance

Naturally, regulation is only pertinent to regulated industries, but the act of regulation is analogous with governance for 'internal' (to the organisation) assurance needs. Emerging technology may break primary legislation under which regulation/governance personnel work, and it also poses unique issues for regulation and governance - not least when considering the competency needs of regulators and governors. Back in 2010, Downer highlighted the issues the FAA had; being wholly unable to hire and retain experts who could understand the increasingly complex technologies involved [9].

Studying the conundrum faced by the FAA, Downer noted that "High-technology regulators contend with an intractable technical problem by turning it into a more tractable social problem, such that, despite appearances to the contrary, the FAA quietly assesses the people who build aeroplanes in lieu of assessing actual aeroplanes" [9]. Emerging technology (especially novel and/or radical technology) may not be readily accepted by users nor society at large should the regulation and governance philosophy be predicated on assessing the "creditworthiness of the people who make the technological claims" (instead of the technology itself directly) [9].

There is a training/educational stepping stone capability required of staff who accept new technology into service, and they must have the ability to turn exemplar acceptance practice into policies and regulations for novel safety solutions.

The advent of emerging technology challenges the regulation and governance mechanisms used with the current compliance-based approaches, and suggests a move towards a more goal-based approach to the development of safety architectures - generating safety evidence and argumentation within a responsible innovation framework.

The current approach has been codified into standards, but emerging technology represents a step-wise progression of existing technology, and NOT an incremental change of it. The implication of this is that we will require all stakeholders (but specifically regulators) to determine:

1. What Responsible Innovation looks like in practice
2. What good adoption processes and competent staff comprise
3. Who does what (developers, safety professionals, and regulators)

4. Blockers and gap analyses for who does what (currently)
5. Possible improvements to extant regulations, policies, and processes.

There is a lack of internationally-recognised safety governance mechanisms for developing and using emerging technologies such as AI technologies in health care [16]. The use of emergent technologies such as AI (particularly in health applications) raises safety and ethical concerns that still need to be addressed by appropriate governance mechanisms [16].

However, a lack of skills, capabilities, and knowledge with local regulator workforces is a significant barrier to remediating current and future gaps in areas such as medical device regulation. It could be argued that cohesion across international regulatory frameworks could help redress the imbalance of regulatory experience and skills between nations [16].

From an employer's perspective, an inherent problem stems from the lack of certainty in regulation [13]. In considering the challenges of adopting novel therapies, Webster and Gardner bemoan the need to overcome issues of utility, novelty, cost, and skills demand - noting also that there exists the challenge of finding the right regulatory framework [25]. This is akin to the problems facing the safe adoption of RAS, for which there exists no suitable standards. Calls exist to develop compliance skills for novel development assurance.

Goyal, Howlett, and Taehagh have observed that it isn't clear from the literature *how* regulation for emerging technologies manifests [11]. Their 2021 research paper into the emergence of the EU GDPR revealed that policy-making can drive technological innovation, which then in turn requires more policy activity.

They argue there is a fine balance between innovation on one side, and oversight, accountability, and transparency on the other [11], and too little / too much regulation can be counter-productive - leading to either unsafe adoption, or the prevention of acceptable innovation in emerging technologies. To determine how effective any regulatory policy may be before its implementation is challenging [12], and the increased ambiguity in the application of a regulation can contribute to a lack of harmonisation amongst stakeholders - which can lead to the framing of the lack of harmony as a policy problem [11]. This has implications for the nature of the skills required for staff developing and implementing regulatory frameworks. Regulatory and govenance staff need reviewing, critical evaluation, and adaption skills to be effective.

3.4 Competency - Knowledge, Skills, and Behaviours

When considering the needs of organisations to educate their staff in the necessary skills for safe adoption, one must consider all the stakeholders in any education process; employers, employees, training providers, and their expectations [10]. Gajek et al cite 3 routes to process safety education [10]:

- Education institutes such as Universities
- Professional Training / OJT
- Training in governmental regulatory agencies.

They further assert that the traditional university method is not well suited to deal with the complex interactions on which safety depends, and further note that only a fraction of graduates have working knowledge of the process safety topics considered important by industrial and academic safety experts. This suggests a disconnect between academic offerings and the expectations of industry [ibid].

Experience from CPD and University-led teaching of safety at the University of York implies that this remains the case currently. It is only being made worse as new technologies become more complex, and have more capability to make decisions which have safety implications. Educating for variation of best safety assurance practices due to new technology is difficult when there is already a skills gap in industry. As new techniques and methods are generated to address the needs of decision making systems, interactions between academia and industry are required to pull these through to training needs analysis and industrial practice. The core techniques and methods, and associated skills, have not changed significantly in 20 years and this interaction is thus not a standard part of the interaction between industry and academia.

The contribution of professional institutions (such as the Institution for Engineering and Technology which publishes Codes of Practice for safety professionals), colleges and universities, and other external providers is surprisingly low, perhaps because employers consider training by universities not practical enough, and universities may not teach process safety as the lecturers have not worked in industry [10]. There remains a credibility gap between industrial practitioners and educators.

Moving away from safety specifically, Naiseh et al assert that graduates are not equipped to apply their training to real-world situations [17], and suggest that promoting the awareness of the interdisciplinary nature of new technology such as Trustworthy Autonomous Systems (TAS), is the main gap in current TAS education.

Many of the TAS experts questioned by Niaseh et al found it difficult to imagine core topics and skills before more research is undertaken, and asserted there is a serious lack of relevant studies, particularly in planning, implementing and conceptualising TAS curricula [17].

This is borne out by experience in programmes such as the Assuring Autonomy International Programme (AAIP), where we have asked demonstrator projects to provide quarterly an indication of the required knowledge, skills, and behaviours implied by their demonstrator activities. Most are unable to provide this, even when prompted and supported, however. The emerging needs for education and training does not appear to be within the current capability of development organisations. This implies that updated policies, and methods and techniques for Training Needs Analysis (TNA) are required to support innovative organisations. There is an open question as to whether developers of regulations/frameworks should have arguments and evidence of competency and training needs as an explicit certification requirement.

Workers will need skills and competencies higher up the Bloom taxonomy scale [7], which implies a need for higher level qualifications as their roles are becoming increasingly more complex, with tasks shifting from routine processes to controlling machines in real-time by incorporating analytical information given by new software [13]. Workers will also need to have digital, soft, business, and management competencies, along with mental, practical and personality skills [10].

Research cited in [13] suggests that skills generally have a"half life" of about five years, with more technical skills at just two and a half years; which poses a question as to whether professional titles such as Chartered Engineer should be formally reviewed every five years. These reviews should have appropriate criteria that ensures renewal is not a "tick-box" exercise. The professional institutions that bestow such titles (such as the Engineering Council) should therefore revisit their code of practice for competency in areas such as safety engineering and safety assurance to address the skills half-life.

Considering safety professionals specifically, Provan et al note that "Safety is a complex socio-technical discipline, and we do not have an agreed understanding of the knowledge and skill requirement for safety professionals" [20].

When considering the required education, training, skills, and knowledge, the IET and HSE provide helpful definitions for the distinction between competence and competency [1]:

Competence: The ability to undertake responsibilities and perform activities to a recognised standard on a regular basis.

Competency: A specific knowledge, understanding, skill, or personal quality that an individual may possess. The sum of an individual's competencies will make up their competence, and it is these individual competencies that are assessed in order to provide an overall indication of competence.

This concept of competency can be extended from the individual to a team of people undertaking a set of co-ordinated tasks that are aimed at some goal. The competency of a team is not merely the sum of the competencies of the individual team members because of the social interactions between the team. Team competency for safety work is particularly important as the work can be highly distributed with a number of members of the team not being under direct line management of safety managers. This is an under explored area of the skills required for safe adoption of new technologies [15], [14], [4].

What constitutes individual and team competence, however, is challenged with the advent of emerging technology, and individual competency requirements must be identified, and managed pertinent to the technology, organisation, role, and individual.

A recent UKRAS report has projected to 2030 and has asserted what skills will be required by then; noting that the rapidly-developing capabilities of technologies such as Autonomous Systems are thought to herald a new machine age

that will dwarf previous waves of innovation, in terms of the scale, speed, and scope of the disruption it creates. For example, in the specific context of RAS, what the workforce of 2030 will be required to do is to problem solve alongside the machines and technologies of 4IR [24], and increasingly act as strategic decision-makers [13].This will require human-robot co-working skills and a significant change in the soft, as well as technical, skills of individuals.

A 2017 report from Deloitte [26] frames the educational/vocational research need quite well, asking:

"How can the training system equip workers in the future to respond to automation and digitalisation? And how can it be sure it is training for the right skills while at the same time enabling those already in work to acquire new, future-oriented skills?"

The implication of increasingly complex systems and decision-making systems is that the workforce will also need to have system's understanding [26], and it will be important for organisations to find staff not only with the appropriate skills but also who are motivated, open to, and curious about acquiring new knowledge and new skills [26]. The need for acceptance by workers that skills and competency are time limited, means a clear pathway to update skills is required. Only a limited number of professions, such as the medical profession, have such cultures and pathways in place. This culture change may be a significant barrier to safe adoption in the engineering community.

We find that there is a lack of academic research with regards to how the adoption of emerging technology can be safely assured. Although some recommendations are made, the majority of uncovered literature only serves to highlight perceived issues.

Further, there appears to be a degree of consensus that universities need to continuously adapt their curricula to stay relevant for the skill requirements (of these jobs). However, University curricula are relatively slow to change with significant time lags to implementation due to the way that student engagement in changes is managed. Business and soft skills (including critical thinking and analytical skills) are as important as hard technical skills. In fact, the lack of critical thinking skills appears to be a significant barrier to industrial safe adoption of new technologies. Critical thinking and decision-making skills are vital for both AI and ML assurance roles [23].

Organisations, and training and Continuing Professional Development (CPD) providers must provide deeper and more intensive re-skilling experiences, and provide their employees relevant time for this learning as part of their change-management and future workforce's planning efforts [13].

Webster and Gardner suggest we could look to Institutional Readiness levels [25] - orthogonal levels of readiness that are designed to employ "trans-organisational expertise and participation in helping to 'ready' diverse actors to undertake more workable, doable technological innovation".

However, it will be necessary to rethink traditional learning methods to attain transferable skills such as creativity, problem-solving, critical and systems thinking, and emotional intelligence [10].

In their paper, Naiseh et al [17] make four recommendations to counter the skills issue and promote the interdisciplinary nature of TAS:

1. Increase interdisciplinary awareness
2. Prepare appropriate logistics
3. Increase diversity
4. Identify the required skills.

In summary, it is clear that the approaches to the development of both soft and hard skills required to address safety and the safe adoption of complex, emerging technologies, especially those that are safety-critical in nature, has not garnered the attention of educational institutions, development organisations, nor academia - in the same manner that the technology itself has. There is a research and policy gap in this area which needs to be addressed.

Training Providers The next question which arises is "are there any training and education providers providing appropriate soft and hard skills in this area?"

Our research suggests there is currently a lack of provision in the educational arena. The vast majority of educational institutions, vocational institutions, and CPD providers are not currently giving the safe assurance of emerging technology any consideration.

Amongst the most important challenges are the need to reskill the current workforce to work safely and effectively alongside robots, to train managers to understand and effectively deploy automation, and to ensure that, across all levels of education, people from diverse backgrounds have the requisite skills [24].

Universities need to continuously adapt their curricula to stay relevant for the skill requirements of (popular jobs/careers) [23], noting that business and soft skills (including critical thinking and analytical skills) are as important as hard technical skills. Decision-making skills are critical for both AI and ML roles [23], [19].

University Course Prospectuses Of the many educational institution prospectuses we have trawled across the UK, Europe and North America, only two institutions offer any form of education concerning safety above an initial awareness level in emerging technologies such as RAS - The University of Hertfordshire, and the University of York.

University of Hertfordshire MEng/BEng in Robotics and Artificial Technology : A review of this course's prospectus reveals the following:

– Notes it will generate an understanding and know-how of related disciplines, but doesn't expand on what these related disciplines are.

- 'Safety' is listed as a constraint that the student will identify (when investigating and defining 'the problem').
- Considers legal requirements of H&S and product safety.
- Provides knowledge and understanding of H&S and risk assessment, and risk management techniques (but this is just 1/7 of one module)
- It is not clear if any of the above are compulsory modules, however.

University of York The University of York is the only UK university to offer a Masters course in Safety Critical Systems engineering that is geared towards industrial practitioners, and is the only course that offers a formal ten credit-bearing module on the safety assurance of robotics and Autonomous systems that employ Machine Learning capabilities.

The safety assurance module is soon to be extended to a full twenty credits as the approach to assuring such technologies becomes more mature. To provide this education close links to the Assuring Autonomy International Programme [3] (sponsored by Lloyds Register) was vital. As funding bodies are key enablers of research projects which contribute significantly to the growing bodies of knowledge, we argue that funders should consider making training and education a core work package in any significant grants they make to the advancement of new technologies and their industrial impact.

However, despite our educational offerings in safety-critical systems, the University of York simply cannot cater for the numbers of postgraduate students required to support the safety professional needs of the future (nor current) workforce, as capacity is limited to twenty places a year.

The university will be providing additional capacity in this area by the 2023 commencement of the MEng course in Robotic Systems; which will again have a formal model on safety assurance. However, capacity is still limited, and cannot support the needs of the future workforce in isolation.

Overall, this shows that the market for such education provision has not become apparent to providers. Further, there is very limited knowledge and skills available amongst providers of the knowledge and skills that need to be imparted to address the educational part of competency for the safe adoption of new technologies such as RAS or Machine Learning.

4 Competence Framework

Competence frameworks exist for safety in safety critical industries (i.e. [1]), yet these frameworks are not designed against the emerging, complex technologies such as AI, ML, or RAS. As such, we have created an illustrative metamodel for a competence framework at Fig 1 which was predicated on the published work by the Institution for Engineering and Technology in the form of their Codes of Practice for both Cyber Security and Safety [2], and for the Competence of Safety-Related Systems Practitioners [1]. It can be instantiated and developed by an organisation (regardless of whether they are adopting/planning to adopt

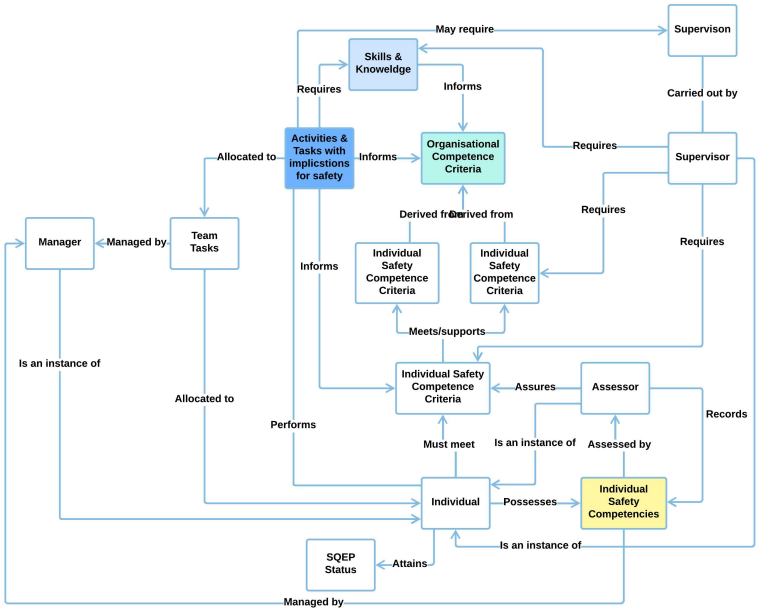

Fig. 1. A Metamodel for a Competence Framework

emerging technology). Further work will be required to extend and validate this initial proposal.

Our metamodel shows the relationships (may require, requires, informs, performs, managed by, allocated to, is an instance of, attains, assures, requires, carried out by, possesses and records) between the organisational tasks, how they define the required competence criteria, and how this competence is achieved, assured, and allocated across the organisation. This culminates in the achievement and management of individual safety competencies, and organisational competence.

This metamodel is a generic structure, and the elements of the model need to be developed for each new technology. Once the meta-model is instantiated it can be offered to any organisation wishing to safely adopt emerging technology, and facilitates the creation of a bespoke, efficient skills framework. This can then form the basis of a gap analysis for the organisation's work force. Further, it can be provided to potential education and training providers to inform their curricula development and offerings to provide initial skills and to update skills for existing staff.

5 Conclusions

Whilst a plethora of papers, guides etc. have been trawled, very little has to date been written on solving the training and education challenges associated

with emerging technology in anything but an ad hoc, individualistic manner. We have also not found any meaningful recommendations made as to how emerging technology can be safely adopted by organisations. Of the forty two artefacts that were read, only twenty had any relevant information regarding the safe adoption of emerging technology.

We are currently in a steady state of an experience-based approach to assuring safety, and this entire approach is underpinned by appeal to compliance with hard-coded, process-based practice of the type embedded in Open Standards. Such an approach is challenged by the advent of emerging technology, and a step-wise approach is needed to create the required competencies (both hard and soft skills) required of all stakeholders if we are to ensure the safe adoption of such novel technology. Not addressing the safety skills issue is a significant barrier to gaining the benefits from new technologies.

We need funders, development organisations, regulatory bodies, academia, and educational and training providers to collaborate, and start to consider their current processes, standards, and skills requirements/offerings as a matter of urgency if we are to prevent an impending skills crisis which will prevent the safe adoption of emerging technology. This collaborative work should consider how all stakeholders can combine to:

1. Increase the awareness of the training and education needs of staff involved in the safe adoption of emerging technology, and Responsible Innovation
2. Increase research into Capability Maturity and competency frameworks for safe adoption
3. Update existing safety competency frameworks and qualifications, such as Chartered Engineer, to reflect the reality of the competencies required for safe adoption of new technology
4. Increase the capacity of educational providers in this area
5. Increase the funding available to deliver pertinent soft and hard skills as a core part of professional and career development.

References

1. IET Code of Practice: Competence for Safety-Related Practitioners. The IET (2017)
2. IET Code of Practice: Cyber Security and Safety. The IET (2021)
3. AAIP: Assuring Autonomy International Programme, https://www.york.ac.uk/assuring-autonomy/
4. Alidrisi, H.M., Mohamed, S.: Developing a personal leadership competency model for safety managers: a systems thinking approach. International journal of environmental research and public health **19**(4), 2197 (2022)
5. Aerospace Recommended Practice (R) Guidelines for Development of Civil Aircraft and Systems. Standard, SAE Aerospace (2010)
6. Barwell, A., Stewart, D., Hoad, R.: Technology adoption hazards - challenges and pitfalls in adopting new technology (2020)
7. Bloom, B.: Bloom's taxonomy (1956)

8. Functional safety of electrical / electronic / programmable electronic safety related systems Parts 1-7 (2010)
9. Downer, J.: Trust and technology: the social foundations of aviation regulation. The British Journal of Sociology **61**(1), 83–106 (2010)
10. Gajek, A., Fabiano, B., Laurent, A., Jensen, N.: Process safety education of future employee 4.0 in industry 4.0. Journal of Loss Prevention in the Process Industries **75**, 104691 (2022)
11. Goyal, N., Howlett, M., Taeihagh, A.: Why and how does the regulation of emerging technologies occur? explaining the adoption of the eu general data protection regulation using the multiple streams framework. Regulation & Governance **15**(4), 1020–1034 (2021)
12. Kobos, P.H., Malczynski, L.A., La Tonya, N.W., Borns, D.J., Klise, G.T.: Timing is everything: A technology transition framework for regulatory and market readiness levels. Technological Forecasting and Social Change **137**, 211–225 (2018)
13. Leesakul, N., Oostveen, A.M., Eimontaite, I., Wilson, M.L., Hyde, R.: Workplace 4.0: Exploring the implications of technology adoption in digital manufacturing on a sustainable workforce. Sustainability **14**(6), 3311 (2022)
14. Margerison, C.: Team competencies. Team Performance Management: An International Journal (2001)
15. Miller, K.K., Riley, W., Davis, S., Hansen, H.E.: In situ simulation: a method of experiential learning to promote safety and team behavior. The Journal of perinatal & neonatal nursing **22**(2), 105–113 (2008)
16. Morley, J., Murphy, L., Mishra, A., Joshi, I., Karpathakis, K., et al.: Governing data and artificial intelligence for health care: Developing an international understanding. JMIR formative research **6**(1), e31623 (2022)
17. Naiseh, M., Bentley, C., Ramchurn, S.D.: Trustworthy autonomous systems (tas): Engaging tas experts in curriculum design. arXiv preprint arXiv:2202.07447 (2022)
18. Nnaji, C., Gambatese, J., Karakhan, A., Eseonu, C.: Influential safety technology adoption predictors in construction. Engineering, Construction and Architectural Management (2019)
19. Plummer, D., Kearney, S., Monagle, A., Collins, H., Perry, V., Moulds, A., Mroczka, M., Robertson, J., Smith, T., Trewavas, S., et al.: Skills and competency framework-supporting the development and adoption of the information management framework (imf) and the national digital twin (2021)
20. Provan, D.J., Rae, A.J., Dekker, S.W.: An ethnography of the safety professional's dilemma: Safety work or the safety of work? Safety science **117**, 276–289 (2019)
21. Rotolo, D., Hicks, D., Martin, B.R.: What is an emerging technology? Research policy **44**(10), 1827–1843 (2015)
22. UKRI: Responsible Innovation, https://www.ukri.org/about-us/policies-standards-and-data/good-research-resource-hub/responsible-innovation/
23. Verma, A., Lamsal, K., Verma, P.: An investigation of skill requirements in artificial intelligence and machine learning job advertisements. Industry and Higher Education p. 0950422221990990 (2021)
24. Waterstone, R., Charlton, P., Gibbs, D., Prescott, T.: Preparing the workforce for 2030: skills and education for robotics & autonomous systems (2021)
25. Webster, A., Gardner, J.: Aligning technology and institutional readiness: the adoption of innovation. Technology Analysis & Strategic Management **31**(10), 1229–1241 (2019)
26. Zobrist, L., Brandes, D.: What key competencies are needed in the digital age? the impact of automation on employees, companies and education (2017)