Advances in Reliability, Safety and Security, Part 4 – Kołowrocki, Dąbrowska (eds.)
© 2024 Polish Safety and Reliability Association, Gdynia, ISBN 978-83-68136-16-6 (printed), ISBN 978-83-68136-03-6 (electronic)

Advances in Reliability, Safety and Security

ESREL 2024
Monograph Book Series

Towards Application Of AI Algorithms In Manufacturing For Improving Productivity, Quality And Functional Safety In Life Cycle

Jan Piesik[a], Kazimierz T. Kosmowski[b]

[a]*Michelin Poland Ltd, Olsztyn, Poland*
[b]*Polish Safety and Reliability Association, Gdynia, Poland*

Abstract

The technological advances currently observed in information technology, automation and tools related to artificial intelligence (AI) broadly understood, have implications for many aspects of the activities of manufacturing companies, in particular productivity, quality assurance and functional safety. Traditional international standards are currently significantly inadequate to describe current trends and solutions. The use of machine learning-based solutions in the industry is already yielding satisfactory results in the above-mentioned domains. The new solutions, complemented by cloud-based and artificial intelligence solutions, create a large space for regulation by standards and regulations. This concerns responsible, safe and ethical AI, as well as the redefinition of functional safety, security standards, changes in corporate culture, business continuity management scenarios, the emergence of new professions, training, etc. The following article aims to present the most essential elements of the current changes in the context of improving productivity and quality while ensuring the functional safety of enterprises. The main identified directions that companies must tackle now to ensure profitability, competitiveness and safety in every aspect of their business.

Keywords: productivity, information technology, operational technology, artificial intelligence, functional safety

1. Introduction

The topic related to AI in general is so broad that in the article the authors focus on presenting only a few key aspects in relation to the issue of productivity, quality and functional safety in manufacturing companies. Competition on the market is becoming increasingly intense, and as a result, the focus on reducing costs while maintaining or even improving the quality of products and ensuring the required safety of people becomes more critical than key. To achieve this, companies are increasingly using technological achievements to win on the market through technological advantage of both products and production methods.

In this context, the idea of industry 4.0 was initiated. New approach is characterized by the convergence of Information Technology/ Operation Technology (IT/OT) systems (Yokogawa, 2021) and the integration of AI tools. IT and OT have different paths, but their joint applicability stems from the Industrial Internet of Things (IIoT). IIoT and Industry 4.0 are driving the growth of wireless sensors deployed to digitize field data. There is a lot of innovation in this field, stimulated by technological convergence and advances in miniaturization.

Today, a multitude of detection technologies are used to measure, analyse, or regulate liquids and process gases, temperature, pressure, flow, level, and electrical parameters. They have all become major IIoT data sources. Sensing devices are the basis of an IT/OT platform and reflect the vital signs of a factory, as sensor data is used to inform and improve the operational performance of the plant. This is also a challenge for functional safety solutions as there are new threats related to IT infrastructure, and OT solutions were developed based on the hierarchical system of the ISA-95 standard.

New rapidly developing digital technologies also require faster adaptation, keeping up with competencies, knowing how to exploit their advantages and avoiding risks. Functional safety remains in the background of the changes taking place here, however, here too, technological development forces rapid changes in solutions as well as methods and standards.

The second chapter will present the current problems and challenges, which significantly facilitates the use of AI tools, but also generates new threats. The third chapter is the presentation of the achieved results of productivity and quality improvement through the use of tools with implemented machine learning algorithms. The fourth chapter describes the challenges of AI development and implementation in industrial plants. In the fifth section, the authors outline the essential components that will ensure increased productivity and quality while maintaining functional safety in an industry.

2. Current challenges

2.1. Productivity in the industrial sector

This part of the article addresses the complex and interrelated challenges faced by industrial systems in the realms of productivity, quality, and functional safety. In the ever-evolving landscape of technology and industry, businesses encounter multifaceted issues that necessitate a comprehensive understanding and innovative solutions for sustainable operations. Below are presented the current challenges within each domain and explores their interconnected nature, acknowledging the critical role each plays in shaping the overall performance of industrial processes. Industrial productivity faces challenges in adapting to evolving workforce dynamics, particularly with the increased prevalence of remote work. Supply chain disruptions, compounded by global complexities, pose threats to timely resource availability. Furthermore, the integration of modern technologies into existing workflows introduces complexities that demand careful management to avoid disruptions.

Technological advantage is associated with a change in the architecture of control systems and the integration of IT with OT. The global process industry is increasingly connected, networked, and integrated. For industry automation, this has led to a shift from the traditional ISA-95 automation model to a cloud-based digital platform, or the IIoT technology stack. New applications for real-time optimization, edge analytics, machine learning (ML), AI, and new sensors are creating opportunities for innovation and automation across layers. But it also imposes new requirements in terms of integration architecture. The challenges linked to the integration of IT and OT systems are being addressed through the rise of unification and standardization efforts. Today, IIoT and Industry 4.0 hold great promise for consolidating the traditional control hierarchy while applying large-scale cloud computing to industrial processes. The vision of application integration, from the control room to the meeting room, is getting significantly closer to reality with digital transformation (DX). Under DX, distributed control system (DCS) and Supervisory Control And Data Acquisition (SCADA) systems should also support web services, IIoT, and cloud-based connectivity, such as Open Platform Communications United Architecture (OPC UA) or message queue telemetry transport (MQTT), as well as computer connectivity such as Simple Network Management Protocol (SNMP) or Internet Control Message Protocol (ICMP) to monitor IT assets. A consequence of the development and implementation of the aforementioned techniques is the explosive growth of data. Their processing and processing with existing tools do not work due to several aspects, the most important of which are excessive cost and inadequate speed. As a result, there has been a rapid development of artificial intelligence (AI), which increasingly responds to the needs of enterprises.

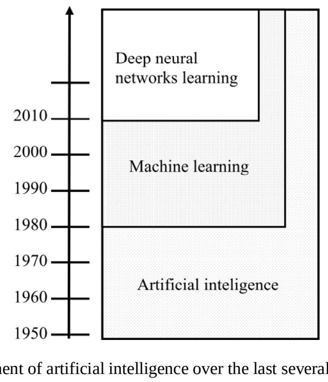

Fig. 1. The development of artificial intelligence over the last several decades (based on own study).

It should be mentioned that artificial intelligence is not a new technology AI research area can be considered to have begun during World War II with the works of von Neuman. With progress in computer techniques and increase of the calculation speed, from the beginning of ’80s, a second stage of artificial intelligence development – machine learning has been observed. Its essence is the use of algorithms to analyse data, infer from it and then determine or predict things that were requested. The algorithmic approach over the years included decision tree learning, reinforcement learning, Bayesian learning and other methods. The last decade brings more sophisticated tools with special processors dedicated for deep neural network (DNN) algorithms; the evolution of this approach is shown in Figure 1. And it is in the last decade that there has been a significant increase in the use of AI technology in industry. AI solutions used in industry bring with them new challenges related to the correct selection of data and the analysis of the obtained results. Incorrectly selected and prepared data generate incorrect or difficult to interpret results, which often resulted in abandoning the use of AI technology.

2.2. Quality of products

Quality assurance remains a persistent challenge as industries strive to maintain consistent product quality across diverse production runs. The dynamic regulatory landscape adds an additional layer of complexity, requiring businesses to navigate evolving standards while upholding high-quality benchmarks. Ensuring the quality of components and materials sourced from suppliers remains a critical aspect of overall product quality. Here, as in the case of productivity, existing methods have become insufficient and new digital tools are increasingly being used.

2.3. Functional safety aspects

Functional safety in industrial systems confronts challenges arising from the escalating complexity of modern systems. The integration of digital technologies introduces cybersecurity concerns, demanding robust measures to safeguard against potential threats (Kosmowski et al., 2022). Achieving functional safety often necessitates effective collaboration across diverse disciplines, emphasizing the need for streamlined communication and coordination. The objective of functional safety is freedom from unacceptable risk of physical injury or damage to the health of people either directly or indirectly (through damage to property or to the environment) by the proper implementation of one or more automatic protection functions (called safety functions).

Modern machines and installations are commonly equipped with electrical, electronic and programmable electronic control systems. That reduces the cost of machines, adds many new functions, and reduces people engagement in the direct production process. On the other hand, it creates some previously unknown safety threats (Sliwinski et al., 2018) This problem was noticed by specialists and international regulatory organisations which affect the founding of international standards (e.g. IEC 61508, IEC 62061, ISO 13849. Looking through the perspective of Industry 4.0 and the idea of lean manufacturing, a crucial element is an appropriate safety level. In addition, the operation of devices in the network, frequent modification of software, remote access, information exchange at various levels of the control and management makes that the entire infrastructure is vulnerable to cyber threats especially SCS. As shown by quite frequent cases of cyber-attacks, the problem is no longer just a matter of thought, but has become real and can result in significant losses. Risk determination and risk management are included in life cycle of functional safety management. The issues of cyber threats in this article are concerned with the impact on the functional safety of safety- related control systems.

The last ten years provide a huge change in the aspect of security in the industry presented above on the example of control system evolution. With the growth of infrastructure development, more and more data are sent to the company's data centre servers around the world. The tele maintenance is becoming common not only for huge enterprises but also for small companies. The services included in cloud services are becoming increasingly popular. With all benefits provided by those innovations, the risk related to security is rapidly increasing. Cyber-attacks resulting in the physical damage on industrial plants become frequent. To help enterprises manage this new risk, new methods and security standards have been created (e.g. IEC 62243, IEC TR 63074, ISO 27000 series, ISO 22301). The IEC 62443 series of standards (IEC 62443, 2018) aim is to cover the industrial automation and control (IACS) safety topics in a comprehensive and independent manner. It is suggested to use this series of standards to add security-related topics to IEC 61508 (IEC 61508, 2010). So far, however, IEC 61508 and IEC 62443 have been only loosely linked (Kosmowski, 2019). The IEC 62443 standard includes the concept of security assurance levels (SAL). The security assurance level framework helps group cybersecurity requirements to make them easier to implement. These threats are a direct result of the increase in IT solutions used from programmable logic controllers to smart sensors and programmable actuators often connected to the internet via various communication protocols including often Ethernet. These threats have been recognised by the standards authors and therefore a technical report IEC TR 63074 (IEC TR 63074) was published in year 2019, describing both security risk assessment but also security countermeasures.

3. Selected results

Below are presented selected results obtained after the implementation of the author's tool for predicting events through machine learning using the FP-Growth algorithm based on the Apriori algorithm (Figure 2). The implemented tool is one of the ways for a predictive approach in the field of defect detection and finding the causes of anomalies. It offers more capabilities than tools based on condition monitoring and is more refined than currently implemented methods based on deep neural networks. The implementation was carried out on a modern production line with a distributed control system made in accordance with the ISA 95 standard. By analysing the results of rules founded, surprisingly predictable were the proportions in which the symptoms occurred before the damage occurred. In the eight hours before the failure, 80% of the symptoms appear. It has been observed that nearly 7% of all relationships occur at the same time or remarkably close to the damage occurs. Figure 3 shows a graph of the relationship between the percentage of occurrences of symptoms and the time intervals counted from the occurrence of the symptom to the occurrence of the failure. Verification of these events has shown that certain rules should be excluded because of their resulting nature. These rules do not add value. They appear because they are the result of another rule.

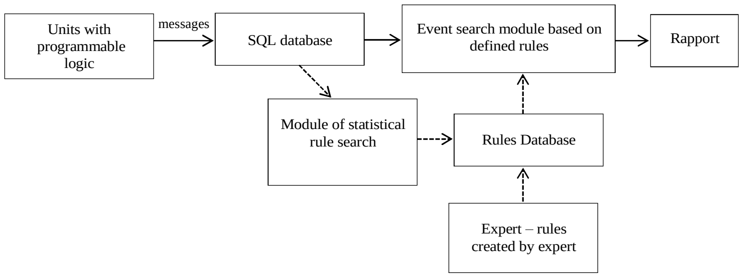

Fig. 2. General system architecture.

The main objective of this tool's implementation was to achieve an increase of the productivity indicator. The duration of the pilot implementation was six months. The analyses presented are related to this period (n+1), for comparison, the period of six months of the previous year (n) is used in the work. The OEE indicator is used as the superior indicator in many manufacturing companies and due to its cross-sectional comparison, the results of this index for the two specific time intervals were compared first. Comparing results of two following years (six first months of each year), an increase 2.1% of OEE indicator can be observed. The small decrease was observed in performance – 0.42%. It is mainly due to an increase in the speed loss rate from 1.2% to 1.51%. That regress can be explained by the work of quality personnel with new recipes as a result of new raw materials and impact of external temperature to raw materials and after on speed of process cycle.

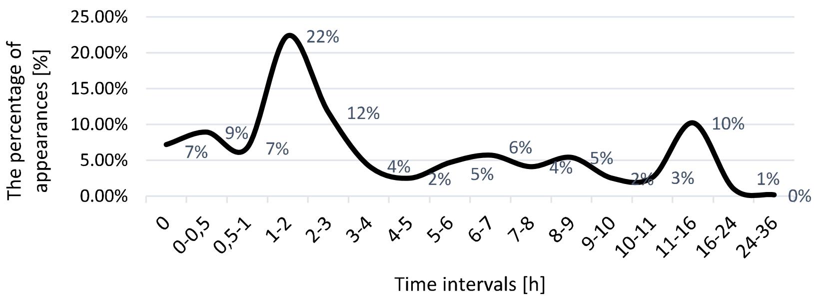

Fig. 3. Chart symptom-effect relationship broken down by time intervals.

The biggest increase was observed in the area of availability which value increased from 87.9% to 90%. As can be seen in Figure 4, there are a few components which percentage share gives that result. Unfortunately, one of the indicator components has increased its value by 0.23%. This component, named as *others*, sums the other components of losses whose single event value does not exceed 0.1% and it is impossible to qualify for any of the described codes. The progress in codes of preventive maintenance (0.08%) and modification (0.1%) has to be considered together, because the joint work of maintenance and production teams, over the increase of efficiency, caused that more work in the field of modification was carried out during the masked time of preventive maintenance, which number was also optimised (0.08%). There are also few codes that remained with almost unchanged value (change is less than 0.1%) and those are the operator error, start-up loses, set-up and machine cleaning codes. There are two more codes that are the most interesting from the point of view of this article. This is the breakdowns code which gained 2.07% and defects in the process which gained 0.35%. At the same time, they are the two most significant codes affecting the value of the availability component. Profit in the above codes was obtained thanks to the proposed tool and after as a result of modifications that eliminated the original causes, optimizing the preventive maintenance plan for repeated faults, prediction of failures and failures, and analysis of the causes of these potential failures, the experience of production and maintenance staff that reduced the duration of the downtime. Some deviations year by year are disturbed by individual failures that last more than 400 minutes. It should be remembered that one unplanned stop lasting 8 hours reduces the monthly result by over 1.1%.

Analysing the mean time to restoration (MTTR) indicator in Figure 5, it can be seen that the "calming down" of this indicator by the stability of the value over time in the year of test implementation, which proves increased preparation for repairs (knowledge of how to repair, tools) and knowledge of impending breakdown (prediction), which makes it possible to prepare the workplace still in masked time and intervention is shorter in the case of quick detection (e.g.: if we know about the high bearing temperature, it is still possible relubrication it and hold to the planned shutdown with replacing, without prediction, maintenance will react when the bearing is already damaged, and it has to be replaced immediately because it cannot continue work). What is important from the point of view of the customer's maintenance services, which is the production department, compared to the previous year (Figure 6), there has been a reduction in the fluctuations in the time load for which the maintenance operations are made. Greater stability results in fewer disturbances, more stable production, which translates into stability of quality results and improvement of production indicators - among other things, the production plan implementation coefficient.

Indicator		6 mth year n	6 mth year n+1		
Unplanned Downtime	Breakdowns	6.1%	4.03%		
	Defects in process	3.1%	2.75%		
	Preventive maintenance	1.3%	1.22%		
	Assorment exchange	0.8%	0.83%		
	Operator error	0.1%	0.11%		
	Start-up looses	0.1%	0.16%		
	Modification	0.1%	0.00%		
	Set-up	0.1%	0.13%		
	Machine cleaning	0.1%	0.17%		
	Others	0.4%	0.63%		
		Availability		**87.9%**	**90.0%**
Speed looses	Reduced speed	1.2%	1.51%	x	x
	Idling	0.2%	0.28%		
		Performance		**98.43%**	**98.01%**
	Rework	0.1%	0.1%	x	x
		Quality		**99.90%**	**99.90%**
				=	=
		OEE		**86%**	**88.1%**

Fig. 4. Percentage of OEE indicator for line A in two compared periods.

Looking at Figure 7, it can be seen that the total percentage of losses due to breakdowns is lower than the median and mean value of four following years. It also shows a certain tendency of breakdowns which cause should be seen in relation to the atmospheric conditions (temperature, humidity- indirectly influencing the raw materials) as well as the times of machinery planned downtime (human factors - holidays, etc.) and then their start-ups.

Impact of productivity improvements on product quality results. Based on the authors experience and results of chosen results of two production lines productivity and percentage of scrap graphs, it can be stated that increase of productivity influence positively the scrap reduction (Figure 8).

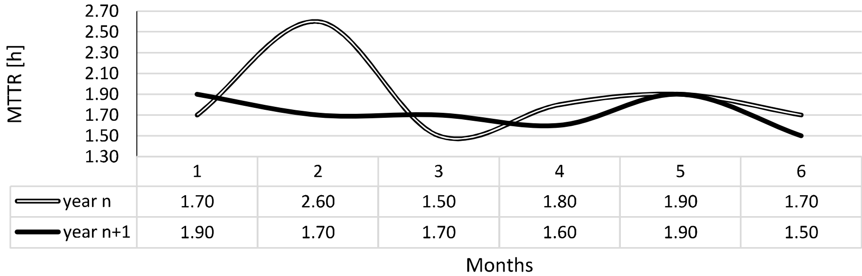

Fig. 5. *MTTR* of line A in the year of tool implementation and the previous year.

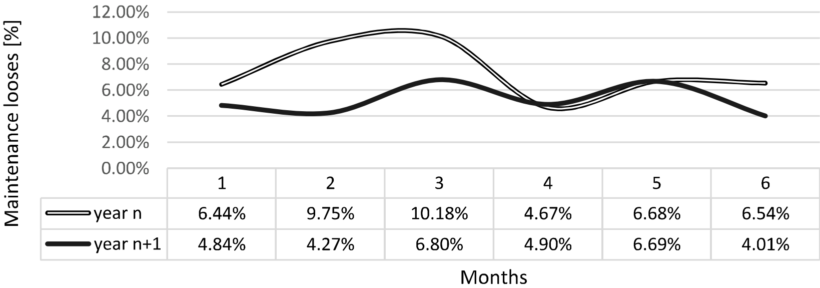

Fig. 6. Losses due to unplanned and planned maintenance activities online A in the year of tool implementation and the previous year.

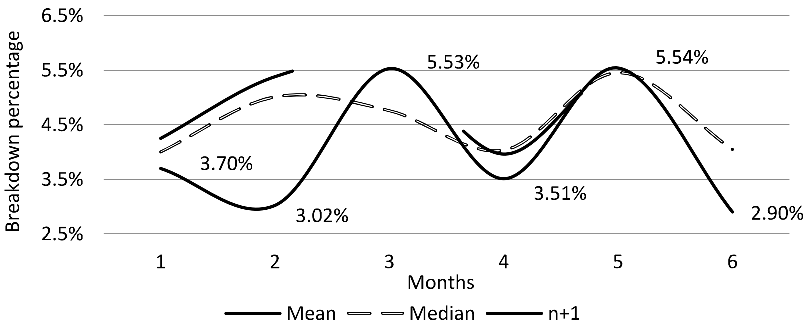

Fig. 7. Presentation of the mean and median value of breakdowns percentage in four following years (*n*-2, …, *n*+1) and breakdowns percentage in the year of test.

That is because increasing productivity decreases unplanned downtime and other MUDA losses. Some losses are inevitable due to scheduled breaks, the initiation and cessation of tasks, and waste generated during the establishment of the production process. It can be stated that focus on productivity increase, also results positively in quality.

At the current prominent level of quality and low associated losses, possible progress in this area is very challenging. Therefore, the author's efforts are concentrated on enhancing productivity, thereby indirectly impacting quality. Unfortunately, during the test implementation, it was not possible to connect the author system with any physical input of the control signal of the tested machines and devices. This was one of the restrictions provided that the author obtained permission for tests. The only possible thing was to create expert rules based on the available data that would detect functional safety abnormalities.

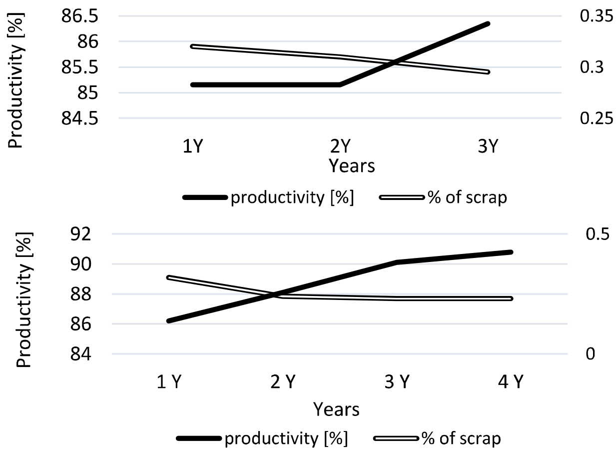

Fig. 8. Graphs of the relation between productivity and scrap percentage on sample production lines.

Despite the brief implementation period and the limited utilization of data from sensors and machines, the outcomes demonstrate significant promise. The return on investment (ROI), which represents the expenses incurred for application and implementation versus the profit gained from increased machine availability, falls within the range of 3 to 4 years—a commendable outcome for an IT tool. Swift development of this tool, coupled with the rapid deployment of the data lake tool, enables the replication of this solution in another similar plant within the enterprise. Consequently, this accelerates the ROI once more. The additional functionalities illustrated in the subsequent examples enhance the value and credibility of the proposed solution (Piesik, 2022).

4. Towards AI

Artificial intelligence has incredible potential to completely transform the manufacturing industry. This was noticed by the authors and simplified solutions are presented in Figure 9. AI in predictive maintenance can firstly use data from multiple sensors monitoring machines faster than operator and secondly, based on available historical data, develop models to predict defects or failures (Kontogiannis et al., 2023). Using predictive maintenance technology helps businesses lower maintenance costs and avoid unexpected production downtime. The detection of defects causing downtime has a direct impact on the profits of enterprises, while the detection of functional safety anomalies and the detection of cyber-attacks is difficult to calculate in terms of the rate of return on the incurred expenditure.

Interesting area of research also proposed by the authors is choice of priorities for AI - safety, security productivity, minimization of asset down-time, increasing the speed of decision making, for example: whether to stop the line now or wait until it breaks down due to timely obligations to clients and gain/ loss cost ratio, and AI in the function of information about the future failure optimizes the line parameters to avoid a drop in the quality of the products. The growing incidence of cyber-attacks targeting manufacturing companies and the ongoing development of safety systems have prompted these companies to adopt AI-based solutions. They view these solutions as a form of countermeasure and as a kind of insurance policy against potential cyber threats.

Quality control is one area where AI systems consistently outperform manual testing processes done by humans. By taking advantage of machine vision technology, artificial intelligence systems have the ability to identify deviations from the norm, as most defects are readily apparent. AI machines are also able to optimize production and figure out the root cause of a problem when there is an error (Arinez, 2020).

Due to subsequent energy crises and their effects in the form of increasing utility costs, companies are increasingly paying attention to the energy optimization of their processes, and AI tools are ideal for this role, analysing data from the processes themselves and measuring devices. By process improvement is recognized that companies can achieve sustainable production levels by enhancing processes through the implementation of AI-driven software (Mhlanga, 2023).

Manufacturing goes beyond what happens in the shop floor. This is why use of artificial intelligence systems to optimize the supply chain, focusing on forecasting demand, optimizing inventory and finding the most efficient shipping routes is very desirable. In the automation process, AI plays a crucial role in taking over tasks traditionally performed by operators, such as manually adjusting equipment settings, monitoring multiple screens for various indicators, and handling troubleshooting and system testing (McKinsey, 2024).

AI for IT operations is currently associated with AIOps, short for Artificial Intelligence for IT Operations, represents a recent trend in the IT industry designed to assist and automate various tasks within IT operational departments. Coined by company Gartner in 2016, AIOps refers to systems that integrate Big Data with artificial intelligence (AI) or machine learning (ML) to enhance processes and operational functions in the field of IT. Illustrative applications encompass performance and availability monitoring, event analysis, and automation. Existing data collection tools, in the form of Datalake creation, allow the collection of data in multiple formats from many diverse sources in one place. The next step is to analyse them using a centralized platform for operating and implementing machine learning models in enterprise applications. It also allows its users to collaborate and iterate on various AI and ML approaches using computation abstraction features. along with its supported instances on different cloud services, provides a solution to big data management that is aligned with the goals of the business (an example of such application is Dataiku platform).

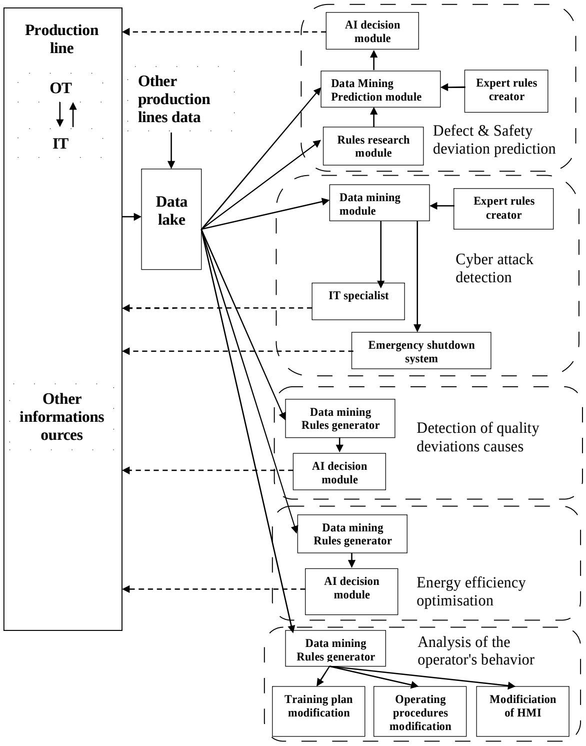

Fig. 9. Integrated concept of factory data mining and prediction supported by advanced AI (Piesik, 2020).

5. Challenges in AI usage in the manufacturing

5.1. Regulation of the law in the context of AI

Summarising what has been presented so far, the authors, based on their experience to date and analysis of literature, have chosen four major directions of challenges facing industry to effectively and safely use the unquestionable advantages of artificial intelligence in improving productivity, quality and functional safety. Due to the increasingly visible impact of AI on digital tools as well as appeals from scientists and influential personalities to regulate issues related to AI, the European Parliament took the first steps in this direction in 2017

(European Economic and Social Committee. 2017). Next step was The Draft EU Artificial Intelligence Act, proposed in April 2021, aims to establish harmonized rules for AI system development, market placement, and use, with varying requirements based on risk levels. The Act also addresses harmonization and pre-emption, seeking to prevent market fragmentation and maintain regulatory consistency across Member States (European Commission, 2021). Also, the US administration has begun the process of regularizing the development of AI. On 30 October 2023, US President issued a sweeping executive order on artificial intelligence (AI) (White House, 2023). As can be seen from the above, the legislative process has just begun, there are many issues that are unregulated. The topic is not easy to regulate due to the fact that it affects many different areas of law (i.e.: who is legally responsible for the effects of AI work, the regulation of property rights, infringement of goods, where there is a limit to plagiarism and creativity, etc) and therefore it can be assumed that this process will not be completed quickly, it will rather regulate subsequent issues in stages, and adapted to newly emerging issues.

In addition to attempts by the government and international institutions to provide a framework for AI, there are also many publications (Vyhmeister, 2023) containing key points that will allow companies to develop their own approaches to responsible AI, data use and design environments for the new agile risk management. The concept that according to the authors is one of the most interesting is the one presented by McKinsley (McKinsley, 2023). It is based on ten points and outlines key principles for the development and deployment of AI systems, emphasizing accuracy, reliability, accountability, transparency, fairness, and ethical considerations. It advocates for human-centric design with diverse perspectives, prioritizes safety and security, and underscores the importance of interpretability and documentation. Additionally, the framework highlights the need for privacy protection, careful vendor and partner selection, ongoing monitoring, and a commitment to continuous learning and development to ensure alignment with ethical, legal, and societal standards in AI applications.

5.2. Resilience of designed solutions

Uncertainty about future AI solutions resulting in adequate protection by building resilience is one of the potential success factors. A proactive resilience-based approach offers a substantial advantage when compared to conventional safety and security methodologies primarily reliant on probabilistic modelling for risk evaluation. This approach is not only beneficial for business continuity management (BCM), which predominantly focuses on restoring processes within a specified timeframe, such as the recovery time objective (RTO), but also emphasizes operational resilience measures. These measures are centred on reinstating a process before it causes intolerable harm to the business, its customers, or the market, making it an extension of conventional BCM methodology. Much more broadly this important topic is described in the article by K. Kosmowski (Kosmowski, 2023).

5.3. Process management

For enterprises to function optimally, it is essential to establish a baseline of AI governance and processes. One illustrative process is the management of an AI use-case pipeline, which involves identifying and assessing new business use cases continuously, planning their agile development, and ensuring a seamless integration into operations. Another critical aspect is the establishment of a defined development process for AI solutions, often based on the Cross-Industry Standard Process for Data Mining (CRISP-DM). This process delineates the phases of data analysis and the development of AI solutions. In the realm of manufacturing, effective operation of AI solutions requires robust data and analytical model governance. Enterprises must clearly define data ownership, access, and security parameters, as well as establish criteria for AI model performance. Additionally, considerations such as ensuring fairness, explain ability, and robustness of AI models, along with ethical and regulatory compliance, are integral components of successful AI implementation.

5.4. Organisation culture and competences

Manufacturers should foster a culture centred around data and artificial intelligence (AI). Achieving this goal involves not only educating the workforce on the capabilities and value of AI but also on its associated risks and limitations, building trust in both data and algorithms. Simultaneously, addressing workforce concerns is crucial, necessitating the creation of a compelling vision for effective collaboration between humans and machines to alleviate fears of AI displacing numerous manufacturing jobs. The impetus for this cultural shift must come from senior executives, who play a pivotal role in driving change. Their commitment should be evident through active engagement with AI methods and technologies. Moreover, they can promote innovation by endorsing a fail-fast experimentation approach for AI use cases. The increasing volume of data and the advent of modern technologies highlight the demand for individuals with specialized analytical skills in the manufacturing sector. While companies have begun hiring data scientists in recent years, they face challenges in establishing the optimal organizational structure to effectively integrate these new skills with those of traditional engineers. An

AI team should encompass new professions like data scientists, data engineers, data stewards, solution architects, and analytics translators. These resources will have to collaborate with teams from diverse manufacturing functions to collaboratively design and implement AI solutions for specific use cases.

6. Conclusions

The above article presents a certain path from the solutions currently used in the industry related to the improvement of productivity, quality and functional safety towards the dynamically developing technologies of artificial intelligence. The development of technologies related to artificial intelligence should already be considered in the category of not if, when, but how. Proper management of the change process can minimize potential losses and difficulties, and appropriate legislation can have an invaluable impact here. A process-oriented approach to risk management and technology deployment through resilience-informed design can significantly increase the competitiveness of companies that will be able to exploit it, while companies that do not adequately manage risk or do not use new technologies due to risk have a high probability of disappearing from the market. The knowledge and change of approach of the management staff is absolutely a priority here. For engineers, on the other hand, the challenge in manufacturing companies in the coming years will be even more frequent changes in technologies and tools, forcing rapid adaptation and the creation of new competencies that engineering staff must acquire to keep up with the changes. The results presented in Part 3 of this article obtained on a real industrial facility using machine learning-based tools demonstrate the potential of AI tools and their impact on productivity and quality. By using the above tool, it is also possible to ensure the expected level of functional safety, what is important is that this can be achieved without involving additional financial resources. In the current study, the authors are working on the use of DNN-based tools that further accelerate the process of data preparation, exploitation and presentation of results. This translates into real profits.

References

Arinez, J.F. et al. 2020. Artificial Intelligence in Advanced Manufacturing: Current Status and Future Outlook. Journal of Manufacturing Science and Engineering. 142, 110804, https://doi.org/10.1115/1.4047855.

European Commission. 2021. Proposal for a Regulation of the European Parliament and of the Council lying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM (2021) 206 final)

European Economic and Social Committee. 2017. Artificial Intelligence - The consequences of artificial intelligence on the (digital) single market, production, consumption, employment and society (own-initiative opinion).

IEC 61508. 2010. Functional Safety of Electrical/ Electronic / Programmable Electronic Safety- Related Systems, Parts 1–7. International Electrotechnical Commission.

IEC 62443. 2018. Security for industrial automation and control systems. Parts 1–14 (some parts in preparation). International Electrotechnical Commission.

IEC 63074. 2017. Security Aspects Related to Functional Safety of Safety-Related Control Systems. International Electrotechnical Commission.

ISO/DIS 22301. 2019. Security and Resilience –Business Continuity Management Systems – Requirements. International Organization for Standardization.

Kontogiannis, S. Gkamas, T. Pikridas, C. 2023. Deep Learning Stranded Neural Network Model for the Detection of Sensory Triggered Algorithms, 16, 202. https://doi.org/10.3390/a16040202

Kosmowski, K.T. 2023. Operational resilience regarding safety and security aspects of industrial automation and control systems. Safety and Reliability of Systems and Processes, Summer Safety and Reliability Seminar 2023, Gdynia Maritime University, DOI: 10.26408/srsp-2023, 99-116.

Kosmowski, K.T. Piesik, E. Piesik, J., Śliwiński, M. 2022. Integrated functional safety and cybersecurity evaluation in a framework for the business continuity management. Energies 15, 3610–3631.

Kosmowski, K.T. Śliwiński, M., Piesik, J. 2019. Integrated functional safety and cybersecurity analysis method for smart manufacturing systems. TASK Quarterly 23(2) 1–31.

McKinsey. 2023. Responsible AI (RAI) Principles. McKinsey & Company. (accessed 10.1.2023).

McKinsey. 2024. Adopting AI at speed and scale: The 4IR push to stay competitive. McKinsey & Company. (accessed 26.2.2024).

Mhlanga, D. 2023. Artificial Intelligence and Machine Learning for Energy Consumption and Production in Emerging Markets: A Review. Energies, 16, 745.https://doi.org/10.3390/en16020745

Piesik, J. 2022. Methods and Tools for Productivity and Safety Management in Computerized Industrial Processes. PhD Thesis.

Piesik, J., Kosmowski, K.T. 2020. Complex Predictive Solution for Computerized Processes in Tire Industry. In: Ahram, T. et al. (eds.) Human Interaction and Emerging Technologies. Springer International Publishing.

Śliwiński, M. Piesik, E. Piesik, J. 2018. Integrated functional safety and cyber security analysis. IFAC-PapersOnLine.

Vyhmeister, E. Castane, G. Östberg P.O. Thevenin S. 2023. A responsible AI framework: pipeline contextualisation. AI and Ethics 2023-3, https://doi.org/10.1007/s43681-022-00154-8. 175-197.

White House. 2023. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (14110), (accessed 11.6.2023.)

Yokogawa. 2021. IT/OT Convergence: Bringing Two Worlds Together. https://www.yokogawa.com/pl/library/resources/white-papers/itot-convergence-bringing-two-worlds-together/ (accessed 10.1.2023)