Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 11 (2017) 1223 – 1230

Procedia MANUFACTURING

27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27-30 June 2017, Modena, Italy

Aspects of risk management implementation for Industry 4.0

Jiri Tupa, Jan Simota*, Frantisek Steiner

Department of Technologies and Measurement, University of West Bohemia, Univerzitní 8, 30614 Pilsen, Czech Republic

Abstract

Industry 4.0 is a comparatively new method of managing production processes. In the area of risk management, as a result of new approaches, modified frameworks, more complex IT infrastructure and so on, new types of risks may occur. In many cases, the implementation of Industry 4.0 has shown that the connections between humans, systems and objects have become a more complex, dynamic and real-time optimized network. On the other hand, there is the fact of data volume and availability enhancement in real time which causes new requirements of the infrastructure, management, technologies and so on. The aim of this paper is to conduct research on Industry 4.0 related to key aspects and presentation of a design of framework to implement risk management for the Industry 4.0 concept.

© 2017 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the scientific committee of the 27th International Conference on Flexible Automation and Intelligent Manufacturing

Keywords: Industry 4.0; risk management; implementation

1. Introduction

Industry 4.0 deals with the connection of all parts of machines via integrated data chains and operations. It was proposed in Germany with the concept of Internet + Manufacturing. The last industrial revolution was based on the use of electronics and the proliferation of information technology (IT) in manufacturing. The fourth industrial revolution, on the threshold of which we are now standing, is marked by linking sub-components of the production

* Corresponding author.
E-mail address: jsimota@ket.zcu.cz

2351-9789 © 2017 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the scientific committee of the 27th International Conference on Flexible Automation and Intelligent Manufacturing
doi:10.1016/j.promfg.2017.07.248

process via the Internet of Things (IoT). Industry 4.0 was mentioned for the first time in 2011 at the Hanover Fair and can be defined as a collective term for the technologies and concepts of a value chain organization which creates together Cyber-Physical Systems (CPS), the Internet of Things and Internet of Services, the Internet of People (IoP), and the Internet of Energy [1,2]. More than 2000 companies surveyed [3] expect to dramatically increase their overall level of digitalization. It is expected that at the end of this transformation process, successful industrial companies will become truly digital enterprises, with physical products at the core, augmented by digital interfaces and data-based, innovative services. These digital enterprises will work together with customers and suppliers in industrial digital ecosystems.

With the inescapable changes which will accompany the transformation of the industrial era there is a very high probability of new risks occurring and having a negative impact on many aspects across companies. There is also the presumption that there is a need to develop and test new approaches for risk management. This paper deals with aspects of risk management implementation for Industry 4.0.

The integration of IT and key infrastructure for the digitalization of manufacturing creates a new potential danger. Namely, the risks from the IT world may affect the industrial manufacturing process and we may find new potential manufacturing industrial risks (cyber-attack, malware, spyware, loss of data integrity or problems with the availability of information). Manufacturing and maintenance data from technical documentation and specifications may become a goal for hackers and software pirates.

There is a new kind of software criminality in the global economy, and companies may have problems with data availability and reliability. This paper discusses how to use a risk management system to minimize the potential threats and unexpected situations. In this context, the following research question (RQ) arises:

(RQ) How can we implement a risk management system according to the requirements of the implementation of Industry 4.0?

This paper aims to present a solution to this research question.

2. Literature review

The increasing number of papers on this topic is evidence that it is starting to be the subject of research at many research institutions. Countries and their governments have adopted strategies that support the implementation of the concept of Industry 4.0. For example, the Czech government approved the document ‘Initiative Industry 4.0’ and allocated support for relevant research projects. On the other hand, the practical issue is how to implement the concept of Industry 4.0. This term is often used in international conference papers and journal articles. The aim of this literature review is to present the context that brings together Industry 4.0 and risk management based on the formulated research question. International sources - Scopus, Web of Science, and ScienceDirect - have been used to search for related literature. The relevant literature has been analyzed and used to find the solution to the research question. We have focused on the keywords: Industry 4.0, Risk Management, Risk and Performance Management.

2.1. The term Industry 4.0

The concept Industry 4.0, mentioned many times as the fourth industrial revolution, depends on CPS (Cyber-Physical Systems) as its key technology and is focused on the establishment of intelligent manufacturing components, smart objects and new production processes. In future manufacturing, factories will have to cope with the need for rapid product development, flexible production, and complex environments. Within the industrial context of interconnected manufacturing plants, these systems are also referred to as CPPS (Cyber-Physical Production Systems). This broad interconnection of ICT (Information and Communication Technologies) aligns with the vision of an IoT (Internet of Things) and services. It supports a close integration along established structures for value creation. The new method of controlling production processes is the main characteristic of Industry 4.0 [4], [5].

Integration within Industry 4.0 can be divided into both vertical and horizontal. Vertical integration indicates an increasing information exchange and collaboration among different levels of the hierarchy (management, corporate planning, production scheduling) within an enterprise. Horizontal integration describes a close collaboration between multiple enterprises within the same value creation network [6].

A condition for the functionality of both forms of integration is a broad availability of efficient and affordable sensor networks (for example, radio frequency identification, RFID). Based on that, intelligent or smart objects and devices are created that allow for real-time communication between machines, working resources and application systems. Taken together, these technological developments provide the basis for implementing new manufacturing processes and business models in so-called smart factories [4],[7]. As they are able to acquire and process data, they can self-control certain tasks and interact with humans via interfaces (see Fig. 1). Figure 1 describes the Cyber-Physical System and the important levels within it. Cyber-Physical Systems (CPS) are integrations of computation, networking, and physical elements.

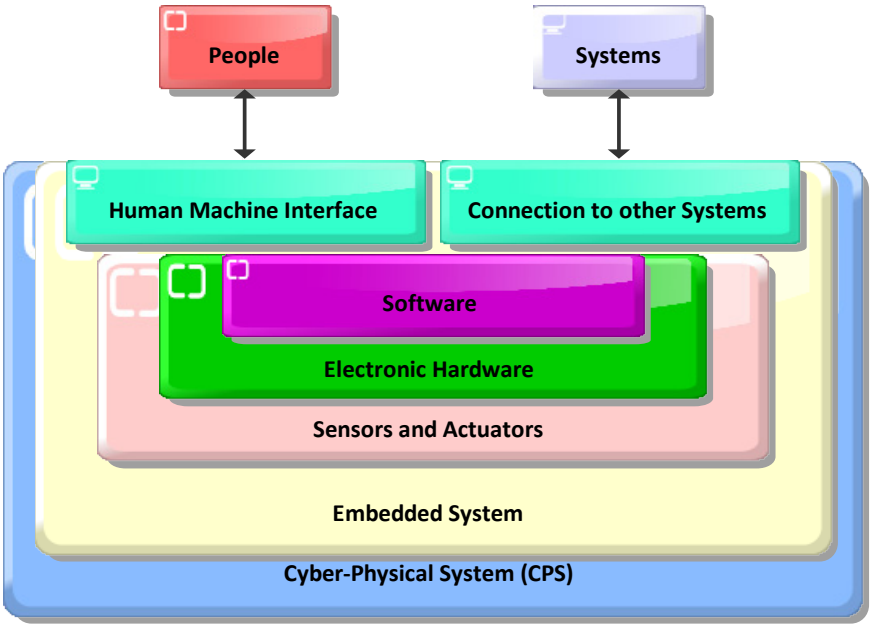


Fig. 1. Interaction of humans and machines via CPS [6] processes.

Embedded computers and networks monitor and control the physical processes, with feedback loops where physical processes affect computations and vice versa. CPS integrates the dynamics of the physical processes with those of the software and networking, providing abstractions and modelling, design, and analysis techniques for the integrated whole. Industry 4.0 also significantly influences the production environment with radical changes in the execution of operations. In contrast to conventional forecast-based production planning it enables real-time planning of production plans, along with dynamic self-optimization. Industry 4.0 also ensures the creation of better cooperation between employees and business partners.

In Germany, industries are evaluating their readiness for implementing Industry 4.0. At least 41% of German firms are aware of the theme and have started some concrete initiatives [8].

2.2. Risk management

In today's post-crisis economy, effective risk management is a critical component of any winning management strategy. Risk management is one of the nine knowledge areas propagated by the Project Management Institute (PMI) and is probably the most difficult aspect of project management. Furthermore, risk management in the project management context is a comprehensive and systematic way of identifying, analyzing and responding to risks to achieve the project objectives [9]. Risk management is a systematic process that helps organizations to understand what the risk is, who is at risk, what the current controls are for those risks and the judgements that need to be made

about whether or not such controls are adequate. If they are not adequate, then action is needed to manage the level of risk down to an acceptable and reasonable level. Nowadays, implementing a proper risk management or a safety system within organizations, especially large organizations, has become a legal requirement over and above any moral obligation to protect their employees [10].

The last few years has seen the emergence of Enterprise Risk Management (ERM), which is often denoted as a new business trend that builds on the principles of traditional risk management. It is a more structured and disciplined approach that aligns strategy, processes, people, technology and knowledge, with the purpose of evaluating and managing the uncertainties the enterprise faces as it creates value [11].

ISO 31000 represents a family of standards that seeks to provide unified and generic guidelines by means of an industry-independent risk management approach [4].

2.3. Risk management and performance

A fundamental principle of management is performance measurement. It is very important because performance measurement identifies performance gaps existing between current and desired performance and provides an indication of progress towards closing the gaps. Carefully selected Key Performance Indicators (KPI) identify precisely where to take action to improve performance [12].

The next very important indicator is the Key Risk Indicator (KRI). A lot of researchers have dealt with KRIs and the ways in which they can help to detect and reduce risk at an enterprise level (e.g. [13],[14]). With these indicators a specific risk can be monitored, and they provide a forward direction and information about risk which may or may not exist and also a warning system for future actions.

There is a gap on the issue of connecting KRIs and KPIs in all research fields. There is no systematic framework for how to effectively connect these two indicators and use them in cooperation. The idea is that in cooperation they should be able to provide useful data for improving the performance of a company (based on methodologies which are used in performance issues) and risk management overall.

3. Design of risk management framework

3.1. Risk identification

The aim of risk identification is to generate a comprehensive list of risks based on the events that might create, enhance, prevent, degrade, accelerate or delay the achievement of objectives. It is important to identify the risks associated with not pursuing an opportunity. Comprehensive identification is critical because a risk that is not identified at this stage will not be included in further risk analysis. In the manufacturing area it is possible to identify operational risk associated with:

- manufacturing process management,
- maintenance,
- the operation methods and tools used,
- material,
- human sources,
- machines and manufacturing technologies,
- machine environments.

The concept of Industry 4.0 generates new categories of risks in this area because of the increase of vulnerability and threats. The connection of cyber-space, sophisticated manufacturing of technologies and elements, and using outsourcing of services is the main factor increasing the vulnerability. An identification of new kinds of risks is presented in Table 1. This identification has suggested a framework for risk management implementation.

The results of our identification show that the majority of common risk factors in the manufacturing area are related to information security. The manufacturing technologies used - machines, robots etc. - are currently part of the Information and Communication Technologies (ICT). The important question is how to protect the manufacturing system against cyber-attacks, loss of data integrity or problems with the availability of information. The implementation of information security management systems can answer this question.

Table 1. Identification of new risks

Categories of operational risk	Risk
Manufacturing process management	Information risk associated with data losses, loss of integrity and available information.
Maintenance	Problem with availability and integrity of data for maintenance.
Operation methods and tools used	Errors data processing.
Machines and manufacturing technologies	Sensitivity and vulnerability of data—problem related to cyber-attacks.
Human sources	Low number of qualified workers
Machine environments	Attacks from Internet network, problems related to electromagnetic compatibility and electromagnetic emissions affecting manufacturing machines.

It is in the IT sector that the information security management system (ISMS) is used. Information security is mainly about confidentiality, which means that information is accessible only to those authorised to have access. But that is just part of information security. Integrity and availability are also important areas of information security. Integrity means safeguarding the accuracy and completeness of information and processing methods. Availability is ensuring that authorised users have access to information and associated assets when needed. The implementation of this standard can be a solution for manufacturing companies adopting the concept of Industry 4.0. The similarity with other ISO standards (ISO 9001, for example) is important for building a certified integrated management system based on the management of quality, information and environmental requirements. On the other hand, the standard ISMS can be effectively integrated into ERM.

3.2. Design of framework

Design of a suitable framework was the next step. The idea for this design was to combine and implement the key requirements for ERM and ISMS. This idea leads to the safe implementation of the Industry 4.0 concept in manufacturing companies. The proposed solutions help to minimize enterprise risks linked with enterprise strategy and the implementation of the certified information security system.

Table 2. Activities for implementing an integrated management system

Plan	Organisational vision and objectives	Establish policy (including ISMS policy), objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with the organisation's overall policies and objectives.
Do	Processes	Implement and operate the policy, controls, processes and procedures.
Check	Performance	Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
Act	Improvement	Take corrective and preventive actions, based on the results of the internal audit and management review or other relevant information, to achieve continual improvement of the system.

The framework for integrated implementation is described based on the Deming PDCA cycle (Plan-Do-Check-Act). This framework enables the requirements for ISMS and a quality management system to be achieved. Table 2 presents activities for implementing an integrated management system for each phase of PDCA.

The integrated system should be systematically documented, communicated, implemented and continually improved. The basic principles and processes are presented in Figure 2. The paper [15] emphasises the fact that the security policy should be extended by risk management aspects to an integrated corporate policy. Thereby, the requirements of all stakeholders, as well as legal and regulatory requirements, are considered, and appropriate corporate risk objectives and strategies are established.

The core of an implemented integrated management system must be based on the functional and effective application of business process management. This means that analysis, description and optimisation are keys to the support and management of the processes. Risk analysis is the most important step for implementation of the proposed framework. The output from that section is a catalogue of risks which should be divided into sections according to the risks included (i.e. technical risks, processes risks, planning risks).

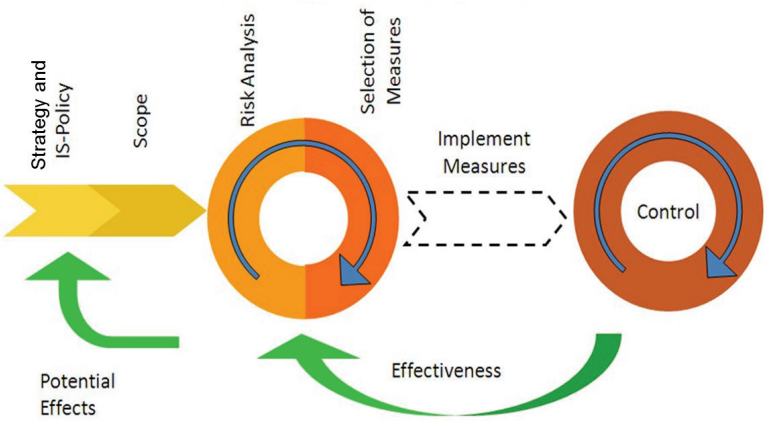


Fig. 2. Principles and processes of implementation of the designed framework [15]

3.3. Integration of performance and risk management

The establishment of business process management can help to identify risks and adopt measures from the risk treatment and business continuity plan. Thereby, the identified risk treatments and business continuity plans are suitably integrated into the manufacturing processes. The measures are implemented, maintained, tested and regularly updated to support the effectiveness of the corporate performance. Risk management must become part of the corporate culture.

The framework developed in this paper adopts principles from the fields of BPM (Business Process Management) and PPM (Process Performance Management) and combines them with elements from risk management into a novel concept. As the authors argue that risk management in smart manufacturing environments must incorporate concepts from both BPM and PPM, they proceed on the following assumptions:

- Governance of business processes and examining process risks are essential for risk management based on real-time operational data in Industry 4.0
- To investigate the performance, risk and goal attainment of processes, approaches from BPM, PPM and RM have to be integrated and combined.
- Risks have to be assessed by means of clearly defined data structures and indicators in a designated calculation scheme building upon these structures.

Due to the large volume of data that derives from processes, potential damage types and their probability of occurrence can be predicted more precisely. However, new assessment procedures might be needed in order to manage the complexity of scenarios. Also, an adaptation of the assessment criteria (for the probability of occurrence and damage) is conceivable.

As mentioned, each risk can be monitored by the KRI(s) which influenced the KPI(s) in connection with the enterprise performance. This idea is presented in Figure 3 below. The risks identified were recorded in a risk model. This model shows the important groups of identified risks and helps to classify them into categories. The different colours used in Figure 3 (to better illustrate the process) divide the risks into: operational (red) and strategic (yellow) risks. Each risk group may also have a different colour (see Figure 3) e.g. for categorization, priority or responsibility. As shown in Figure 3, each risk group can be broken down into individual risks.

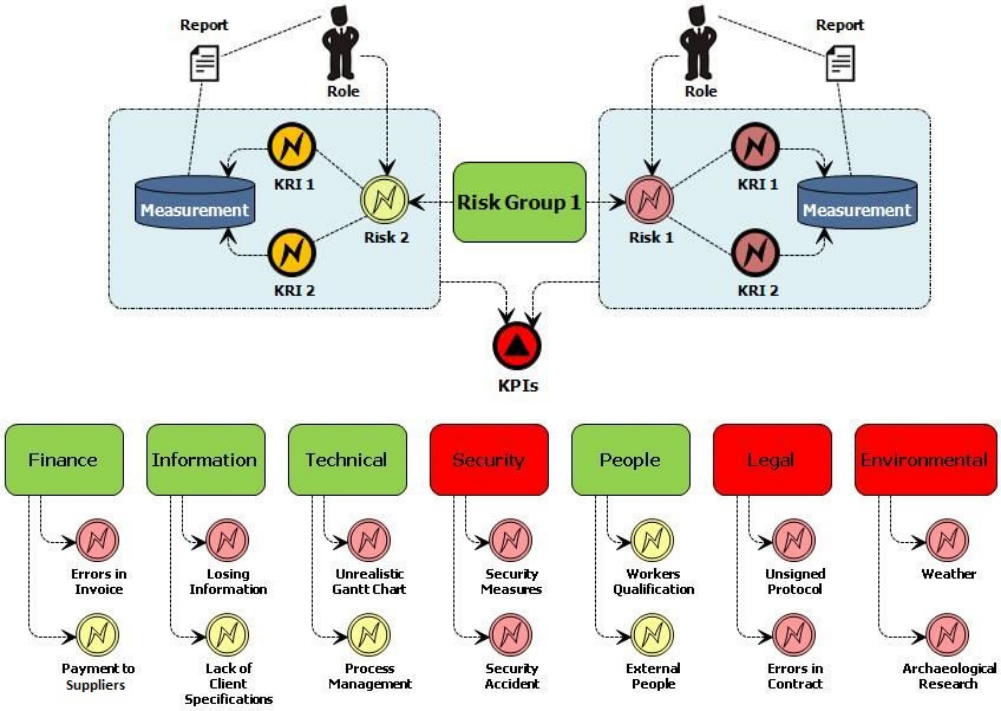


Fig 3. Model of risk groups and relationships between Risks - KRIs – KPIs.

4. Conclusion

The aim of the paper was to conduct research in risk management related to the Industry 4.0 concept and try to find all the aspects of risk management implementation involved in it. The literature review of the concept of Industry 4.0 showed that the connection of humans, objects and systems, that form dynamic, real-time optimized and self-organizing, cross-company value creation networks, can have an impact on all the processes of the company. The fact of the need for increased data volumes and availability in real time requires new infrastructures and adaptations to the handling of information.

It can be expected that new risks may occur due to the changing conditions. The results of our analysis show that the majority of common risk factors in the manufacturing area are related to information security. These risks are associated with cyber-attacks, such as the loss of data integrity etc. There is also an assumption that risks may occur more frequently in Industry 4.0. Also, the content and the running of the risk management process will change,

which is not least due to the availability of real-time data. Therefore, existing instruments and measures must be adapted.

In the case of performance, there is an expectation that a tool for the connection of Key Performance Indicators (KPI) and Key Risk Indicators (KRI) should be found in order to increase the suitability and application of risk management in relation to the performance measurement of companies.

In our opinion, there is an opportunity to find a suitable framework for the abovementioned issue in accordance with the increasing data that comes from ICT systems from manufacturing systems. It should be simpler to verify a new framework based on analyses of more relevant data for them based on the impact of Industry 4.0. This is our new aim for future research works.

Acknowledgements

This research has been supported by the Ministry of Education, Youth and Sports of the Czech Republic under the RICE – New Technologies and Concepts for Smart Industrial Systems, project No. LO1607, and by the Student Grant Agency of the University of West Bohemia in Pilsen, grant No. SGS-2015-020 “Technology and Materials Systems in Electrical Engineering”.

References

[1] M. Hermann, T. Pentek, and B. Otto, Design Principles for Industrie 4.0 Scenarios: A Literature Review, 2015.
[2] M. Lom, O. Pribyl, and M. Svitek, Industry 4.0 as a part of smart cities, in 2016 Smart Cities Symposium Prague (SCSP), 2016, pp. 1–6.
[3] 2016 Global Industry 4.0 Survey. What we mean by Industry 4.0 / Survey key findings / Blueprint for digital success.
[4] T. Niesen, C. Houy, P. Fettke, and P. Loos, Towards an Integrative Big Data Analysis Framework for Data-Driven Risk Management in Industry 4.0, in 2016 49th Hawaii International Conference on System Sciences (HICSS), 2016, pp. 5065–5074.
[5] M. Schröder, M. Indorf, and W. Kersten, Industry 4.0 and its impact on supply chain risk management, pp. 15–18, 2014.
[6] M. Brettel, N. Friederichsen, M. Keller, and M. Rosenberg, How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective, World Acad. Sci. Eng. Technol. Int. J. Mech. Aerospace, Ind. Mechatron. Manuf. Eng. 8(1) (2014) 37–44.
[7] D. Lucke, C. Constantinescu, and E. Westkämper, Smart Factory - A Step towards the Next Generation of Manufacturing, in Manufacturing Systems and Technologies for the New Frontier, London: Springer London, 2008, pp. 115–118.
[8] A. Sanders, C. Elangeswaran, and J. Wulfsberg, Industry 4.0 Implies Lean Manufacturing: Research Activities in Industry 4.0 Function as Enablers for Lean Manufacturing, J. Ind. Eng. Manag. 9(3) (2016) 23.
[9] N. Banaitiene and A. Banaitis, Risk Management in Construction Projects,” in Risk Management - Current Issues and Challenges, InTech, 2012.
[10] S. A. Malik and B. Holt, Factors that affect the adoption of Enterprise Risk Management (ERM),” OR Insight 26(4) (2013) 253–269.
[11] KPMG, Enterprise Risk Management, An emerging model for building shareholder value, 2001.
[12] A. Weber and R. Thomas, Key Performance Indicators: Measuring and Managing the Maintenance Function, 2005.
[13] The Power of Key Risk Indicators (KRIs) in Enterprise Risk Management (ERM).
[14] S. Scandizzo, Risk Mapping and Key Risk Indicators in Operational Risk Management,” Econ. Notes 34(2) (2005) 231–256
[15] M. Stoll, From Information Security Management to Enterprise Risk Management, vol. 313. Cham: Springer International Publishing, 2015.