ISSN 2658-5014 (Print)
2021. Т. 3, № 3 (7). С. 23–29
СИИТ
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
ISSN 2686-7044 (Online)
http://siit.ugatu.su

УДК 004.056

# ASPECTS OF INDUSTRIAL CPS CRITICAL FOR RISK ASSESSMENT METHODS

**T. FABARISOV[1], G. SIEDEL[2], S. VOCK[3], A. MOROZOV[4]**

[1, 4] {first.last}@ias.uni-stuttgart.de, [2, 3] {first.last}@baua.bund.de

[1, 4] Universität Stuttgart, Stuttgart, Germany
[2, 3] Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Dresden, Germany

*Поступила в редакцию 20 сентября 2021 г.*

**Abstract.** A Cyber-Physical System (CPS) is an advanced mechatronic system or a system of distributed and networked mechatronic systems with sophisticated software parts and complex communication protocols. Classical risk assessment methods exploit several well-known methods for evaluating the dependability and resilience properties of technical systems. However, CPS are structurally and behaviorally more complex, distributed, and autonomous, and their components are of heterogeneous nature. Therefore, it is necessary to revisit the classical risk analysis methods and extend them with the most promising advanced approaches. As a first step, we conduct a systematic literature review to evaluate the applicability of risk assessment methods for Industrial CPS. This method is started through formulating the research questions that are ought to be answered. In this paper we are focusing on the first research question, namely: Which aspects of Industrial CPS need to be covered by risk assessment methods? Answering this research question would be the main pre-requisite for the inclusion of a publication presenting a risk assessment methodology into the subsequent reviewing and quality assessment process of the systematic literature review. To strengthen our understanding of important CPS properties, we are not only considering the definitions, but also the academic research focus. Using the bibliographic visualization tool Vosviewer, we are illustrating the most important aspects of CPS.

**Keywords:** Cyber-Physical System; risk assessment; risk models; systematic literature review; model-based methods; Industrial CPS.

## INTRODUCTION

Cyber-Physical Systems (CPS) are advanced interconnected systems that are one key characteristic of the emerging trend towards Industry 4.0 in automation engineering. As with any industrial production system, risk analysis is one of the key challenges of the design of CPS. Classical risk analysis exploits several well-known methods for evaluating the dependability and resilience properties of production systems. However, Industry 4.0 implies that the Industrial CPS (sometimes also called Cyber-Physical Production Systems, or CPPS) are more complex from a structural and behavioral points of view and consist of distributed heterogeneous components [10]. Classical methods cannot adequately describe sophisticated failure scenarios of modern highly dynamic, autonomous, and adaptive Industrial CPS. That is particularly true for Artificial Intelligence, especially Deep Learning, being employed for more broad types of safety-critical applications within systems. It is necessary then to revisit the classical Risk Assessment Methods (RAM) and extend them with the most promising advanced techniques that cover increased complexity.

*This study is completed in the framework of the BAuA F 2497 project.*

As such, it is necessary to evaluate the applicability of modern model-based RAMs for the analysis of Industrial CPS. For that, we are conducting a Systematic Literature Review (SLR) [1]. First, the Research Questions that the SLR addresses are presented. As with any attempt at systematic reviewing of scientific research papers, the prereview activities are of greatest importance. This article is focusing on the precondition for the evaluation of a methods applicability. Namely, what aspects of Industrial CPS need to be addressed by RAMs.

**RESEARCH QUESTIONS FOR SLR**

First, we start with the overview of the Research Questions (RQ) that the planned SLR is sought to answer:

1. *Which aspects of Industrial CPS need to be covered by RAMs?* In this paper, we are focusing on this main RQ. Before starting to evaluate whether a paper is suitable for further consideration and should be accepted, it is necessary to come up with a general idea of what exactly these RAMs should be capable of covering. We want to accept methods capable of covering aspects specific for Industrial CPS. These aspects should reflect the challenges for the straightforward application of modern RAMs to the risk modeling and assessment of CPS.

2. *What kind of RAMs can be applied for the risk analysis of CPS?* After establishing the critical CPS aspects, we will utilize the SLR method to evaluate which existing RAMs are suitable for the analysis of CPS. One possible situation that may arise during the literature review is that different methodologies are partially covering some of the aspects. Or even, they could be applied partially with limitations to a given type of CPS. That closely leads us to the third RQ.

3. *How can the different RAMs be combined for a more effective Risk Analysis?* After evaluating single methods, we will focus on the combined risk analysis. Each RAM is designed for a particular task. Event Trees can describe failure modes, Fault Trees describe logical combinations of component failures, Markov Chains help to model risks of the dynamic system, etc. By integrating various RAMs, it could be possible to cover multiple challenging aspects of CPS. However different methods have different computation complexity. For instance, static methods such as ETA or FTA employ effective computation methods based on Binary Decision. In contrast, Markov Chain-based methods suffer from the so-called state space explosion problem. The real challenge is the intelligent combination of these methods. For example, classical probabilistic risk analysis methods usually combine Event Trees, Fault Trees, and Bayesian Network. In our recent paper, we have proposed an effective combination of PMC, ETA, and FTA [2]. In our SLR we will seek combinable methods suitable for industrial CPS systems. That would assume interfaces between chosen RAMs and an evaluation of their exchangeability.

4. To evaluate how well and to what extent it is possible to apply RAMs, it is necessary to find *which metrics/criteria to use for applicability evaluation.* The applicability criteria would be derived from the inherent CPS properties. Possible criteria could include RAMs advantages and drawbacks, such as its industrial maturity, available tools that realize these methods and their benchmarks, the required input data that should be feed from the system, the sensitivity of the methods to uncertainties. For the combination of RAMs, it could also include its comprehensibility and computational complexity.

5. *Where to get input data to feed the Risk Analysis methods?* This RQ is closely related to the previous one. There are multiple guiding references available that provide the necessary insight. However, the aspects of complex CPS might dictate specific requirements which will require a new methodology for automatic access point allocation.

6. *In which phase can the Risk Analysis methods be applied?* Different types of RAMs are applicable for different phases of system development. Simulative methodologies such as model-based Fault Injection or Software/Hardware-in-the-Loop may help to cover edge cases with various failure modes. But they cannot be applied to earlier design phases. On the other hand, analytical methods such as Fault Tree Analysis or Markov Chains could be applied on a much earlier design phase, where the cost of possible system design changes would not be as drastic as with a simulative approach.

Upon completing these RQs, we would be able to pinpoint *whether there is any major gap in RAMs that should be covered.* Even when we succeed in the identification of the RAM-combination that is suitable for CPS RA, it might be that some of the aspects are not covered to the required extent and an extension of selected RAMs is therefore needed.

## ASPECTS OF INDUSTRIAL CPS

Cyber-Physical Systems (CPS) are an integral part and a key component of Industry 4.0 [3, 4]. Lass [4] points out that the literature does not provide a comprehensive clarification of terms or a conclusive definition for CPS. However, he also emphasizes that there is a fundamentally consistent understanding with different emphasis on the aspects of CPS and their combination. As it is described in the previous section, covering these aspects would be the main prerequisite for the inclusion of a publication presenting a risk assessment methodology into the subsequent reviewing and quality assessment process of the SLR.

CPS connect the physical world with the digital by integrating the processes of both [5, 6]. In this regard, they are based on mechatronic systems, which combine mechanics, electronics, and information technology. CPS in turn are more complex mechatronic systems with extended inherent aspects [7–9]. The emphasis on these aspects differs, as described by Lass [4], depending on the publication and industry. The special properties which make up Cyber-Physical Systems can be summarized into four groups.

### ASPECT GROUP 1

The first area is the integration of heterogenous hardware components and sophisticated software. There is a consensus in professional publications about sensors and actuators as core components of a CPS [7, 9–12]. Sensors allow the collection of data from the physical world into the digital one with the goal of further processing. Actuators allow the CPS to implement digital decision making in the physical world and trigger processes. Several authors emphasize the particularly high software content as a characteristic of CPS [8, 10]. Another key characteristic of CPS that makes them more complex than mechatronic systems is that they can cooperate. A CPS may in this way form more complex behavioral and structural operation modes and develop higher dimensional state spaces. Due to this fact, a software part of CPS may be more prone to hazardous data errors caused by edge case situations and unexpected inputs.

### ASPECT GROUP 2

The second aspect group is the network structure and data processing capability. These aspects cause complex communication protocols, data pipelines, the need for interoperability and generally advanced structural and dynamic complexity. Connectedness is an essential property that defines CPS [5, 7, 9, 10, 13]. In this context, the systems can be networked locally, but also globally through the Internet [7, 13]. CPS can not only collect data internally and process it independently, but also exchange it among each other [5, 13, 14]. Networked CPS can use globally available data and services [7] and make data available globally [14]. Interconnected CPS are referred to in the literature as “Cyber-Physical Systems of Systems” (CPSoS) or “Cyber-Physical Production Systems” (CPPS). The former term refers to rather large, distributed systems of CPS [10], the latter refers to the coupling of individual CPS into a consolidated plant [4], which then represents an independent intelligent unit of an enterprise [15]. The term CPPS is mainly focused on industrial production systems. Extensive communication technologies on different system levels are necessary for the data exchange of the CPS [8, 13]. Standardization of the communication of networked systems is a central challenge for the future [4].

### ASPECT GROUP 3

Several authors include human-machine interfaces (HMI) among the essential characteristics of a CPS [7, 11]. CPS with extensive HMI result in human-in-the-loop systems, where humans can be considered and modeled as part of the CPS via its communication interfaces [8]. Presence of a human requires taking into consideration human interactions as well which is a further open challenge. As the authors shows in ([16], p. 19), “Current CPS have yet to integrate the Human component in order to achieve an Internet of All”.

**ASPECT GROUP 4**

The third property area is the autonomy and self-control of the CPS [5, 6, 14]. Self-control is a combination of structural self-organization of instrumentation and control technology [17], for which autonomy is a prerequisite. Self-control is expressed in the abilities of independent local information processing, decision making and execution [4, 17]. Information processing and decision making are enabled by sensory data collection and communication with other CPS [4]. By means of actuators, CPS can trigger actions autonomously [5, 9]. Several authors define “embedded” or integrated systems as a characteristic of CPS [6, 10, 18]. Embedded systems are computers that are integrated into a functional context and are often specifically adapted to a particular application. Thus, from a technical point of view, these support the functional autonomy of the CPS, although they could be assigned to Aspect group 1 as well. The extent to which machine learning methods or other AI methods are central parts of CPS can only be partially determined based on these definitions. Even if autonomy and self-control could be identified as an important property area, its characterization is not consistent. The self-control of CPS can in principle be achieved by either classical control mechanisms or artificial intelligence. However, the extending software proportion, data usage and autonomy indicate the upcoming usage of learning and knowledge-based systems.

The fact that CPS become autonomous and networked (Aspects 2 and 4) indicate increasing decentralization, which enables a particularly high mutability and robustness of production sys-tems [4]. Bolbot [10] even distinguishes between autonomous CPS and networked CPSoS as indi-vidual types of CPS. The extent of autonomy as well as decentralization of CPS differ strongly and can be expressed in indices and measures [4]. Besides or contrary to the decentralization into separate autonomous CPS, Langmann et al. [19] point out a second trend: the shift of centralized control to the cloud.

To strengthen our understanding of important CPS properties, we wanted to not only consider definitions, but also the academic research focus. To achieve that, a sample of 1666 papers about Industrial CPS was derived from Scopus database [20] based on the following search string:

*( TITLE ( cyber AND physical AND system* OR cyber-physical AND system* OR cyber-physisch* AND system* OR cyber-physisch* AND system* OR CPS) AND ( TITLE ( industr* OR production* OR produktion* OR factory OR factories OR manu-fact* OR fabrik OR fabrication OR mill* OR plant* ) OR KEY ( industr* OR production* OR produktion* OR factory OR facto-ries OR manufact* OR fabrik OR fabrication OR mill* OR plant* ) ) ) AND ( LIMIT-TO ( LANGUAGE,"English" ) OR LIMIT-TO ( LANGUAGE,"German" ) )*

It is noticeable that the term “Cyber-Physical System” is relatively new, with the oldest identified paper being from 2007. In the past few years, CPS enjoyed rapidly increasing attention, as can be observed in Fig. 1.

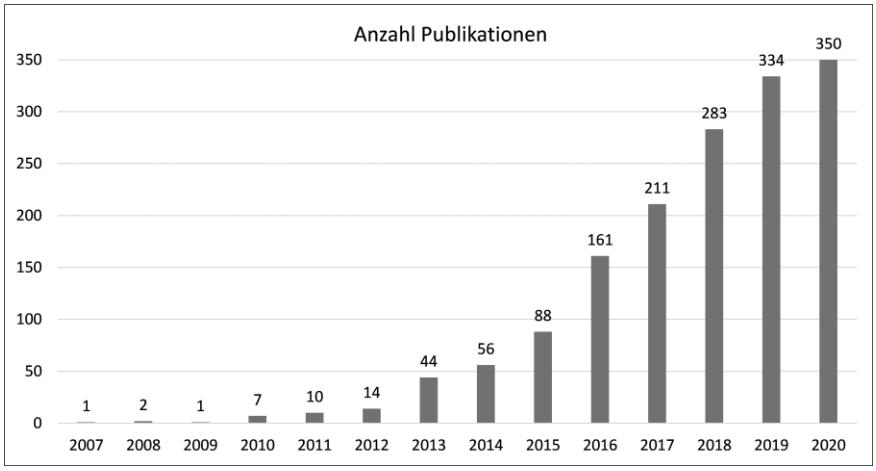


**Fig. 1.** Distribution of identified CPS papers by year

Using the bibliographic visualization tool Vosviewer [21], we intended to illustrate the most important aspects of CPS within these papers. Therefore, we created a so called co-occurrence-map shown in Fig. 2. It displays terms with more than 10 occurrences within title or keywords of the papers, with larger points and labels indicating more occurrences. The tool arranges those terms next to each other that occur together in the same papers frequently. We manually adjusted the map by summarizing very similar terms (marked "sum.") and by filtering for terms only which are relevant for understanding CPS properties in research focus. In the map, related terms are clustered and colored similarly.

While the red cluster in the co-occurrence-map includes terms from multiple fields, it contains "embedded systems", which is the most frequently used property, showing its academic relevance. A term from the red cluster yet to be mentioned in our aspect groups is "real time systems". Real-time is a requirement even exceeding the property of CPS being 'simply' highly dynamic. The dark blue cluster includes publications, where controllers as parts of CPS are in the research focus. The bright blue cluster relates to security aspects and is significantly large. This indicates that network security systems and real-time-monitoring systems for anomaly/fault/attack detection are frequently investigated in the context of CPS. The orange cluster is related to big data and network aspects. Cloud computing and digital storage also play a role. This underlines the claim that properties like extensive data usage and distributed, interconnected agents should be part of the CPS definition. The green cluster shows techniques and applications of artificial intelligence in CPS, especially learning algorithms. The purple cluster includes terms directly related to HMI, among others "decision support systems" "human computer interaction" as well as "virtual"- and "augmented reality".

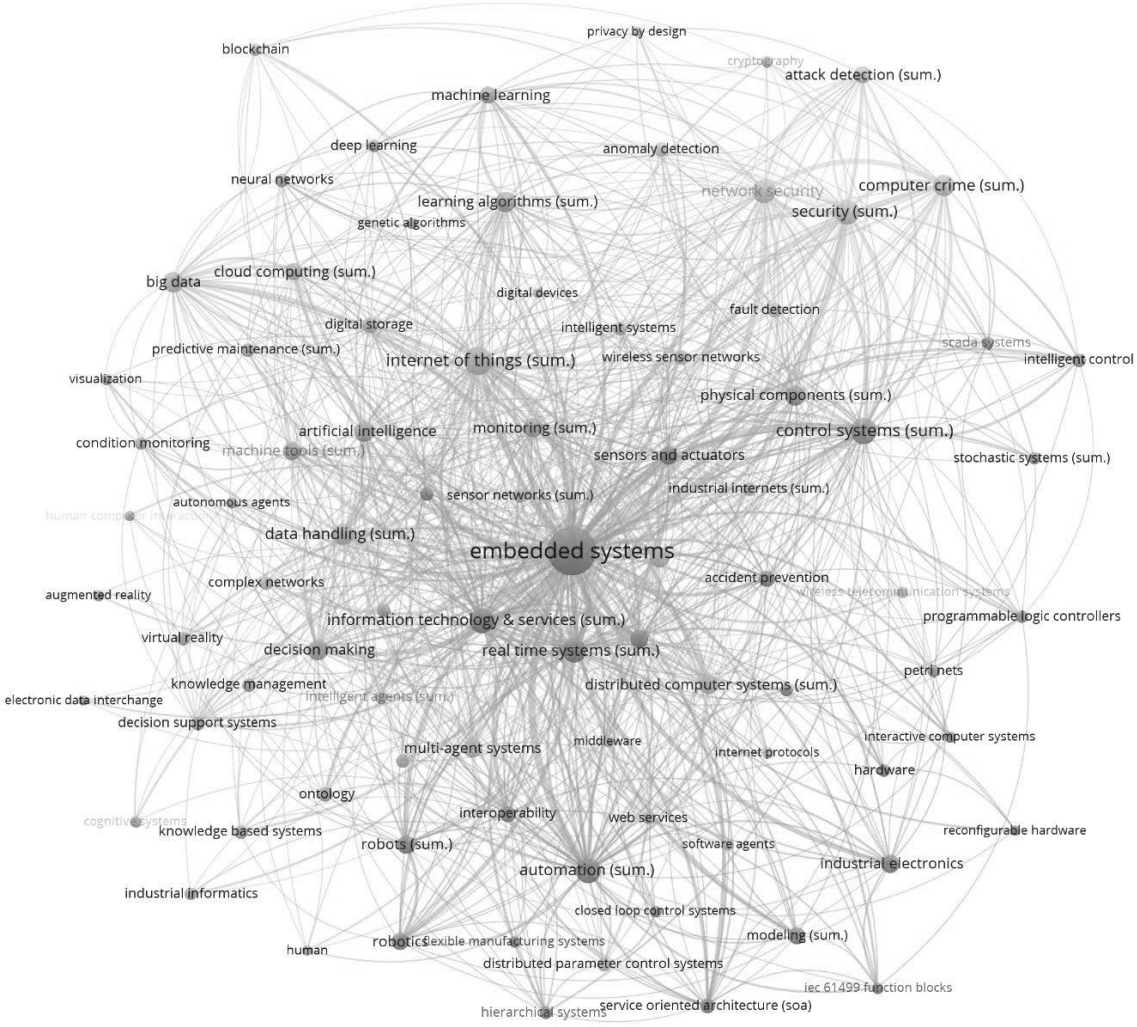


**Fig. 2.** Vosviewer Co-occurrence map illustrating most frequently used terms from title and keywords of academic publication about industrial CPS

In summary, the map supports the aspect groups proposed before. At the same time the visualization of the currently most frequent research terms indicates in which direction the most important aspects of CPS might further develop. These directions could add to the currently defined aspect groups. From the size of the clusters, compared with the current definition, it can be concluded, that particularly the topics related to security, AI and HMI will be of growing importance.

## CONCLUSION

In this article we presented an overview of the properties of Cyber-Physical Systems that make the application of classical risk assessment methods complicated. To tackle this problem, we are planning to perform a systematic literature review. We therefore provided an overview to the Research Questions for the review that will be focused on applicability evaluation of the RAMs and their combinations to modern Industrial CPS. In this paper, we particularly addressed our first research question: From established definitions as well as utilizing the bibliographic visualization tool Vosviewer, we illustrated the most important aspects of CPS within the publications.

## REFERENCES

1. **Systematic** literature reviews in software engineering - a systematic literature review / B. Kitchenham, et al. // Information and software technology. 2009. Vol. 51, no. 1. Pp.7-15.

2. **Morozov A., Diaconeasa M. A., Steurer M.** A Hybrid Methodology for Model-Based Probabilistic Resilience Evaluation of Dynamic Systems // ASME International Mechanical Engineering Congress and Exposition. 2020. Vol. 84669. Pp. V014T14A024.

3. **Recommendations** for implementing the strategic initiative / H. Kagermann, et al. // INDUSTRIE 4.0: Securing the future of German manufacturing industry; final report of the Industrie 4.0 Working Group. Forschungsunion, 2013. 87 p.

4. **Lass S**. Nutzenvalidierung cyber-physischer Systeme in komplexen Fabrikumgebunge // Ein hybrides Simulationskonzept für Industrie 4.0. Berlin: Gito, 2018. 321 p.

5. **Huber D., Kaiser T**. Wie das Internet der Dinge neue Geschäftsmodelle ermöglicht // Industrie 4.0. Wiesbaden: Springer Vieweg, 2017. Pp. 17-27.

6. **BMWi**, Erschließen der Potenziale der Anwendung von "Industrie 4.0" im Mittelstand // F.I.u.Z. Erarbeitet von agiplan GmbH, 2015.

7. **Cyber**-physische systeme / W. G. Drossel, et al. // Digitalisierung. Berlin, Heidelberg: Springer Vieweg, 2018. Pp. 197-222.

8. **Industry 4.0:** Emerging challenges for dependability analysis / A. Morozov, et al. // Industry 4.0. 2019. Vol. 4, Iss. 5. Pp. 206-209.

9. **Die** neue Rolle des Mitarbeiters in der digitalen Fabrik der Zukunft / A. Richter, et al. // Industrie 4.0. Wiesbaden: Springer Vieweg, 2017. Pp. 117-131.

10. **Vulnerabilities** and safety assurance methods in Cyber-Physical Systems: A comprehensive review / V. Bolbot, et al. // Reliability Engineering & System Safety. 2019. Vol. 182. Pp. 179-193.

11. **Bracht U., Geckler D., Wenze S**. Digitale Fabrik: Methoden und Praxisbeispiele. Berlin: Springer, 2011. Pp. 160-161.

12. **Kagermann H., Wahlster W., Helbig J**. Umsetzungsempfehlungen für das zukunftsprojekt industrie 4.0 // Abschlussbericht des Arbeitskreises Industrie. 2013. Vol. 4, Iss. 5. Pp. 1-9.

13. **Sauer O.** Lösungsbausteine für herstellerunabhängige, standardisierte Schnittstellen in der Produktion / T. Schulz (ed.) // Industrie 4.0 - Potenziale erkennen und umsetzen. Würzburg: Vogel Business Media, 2017. Pp. 87-108.

14. **Evolution** from mechatronics to cyber physical systems: An educational point of view / R. Plateaux, et al. // 2016 11th France-Japan & 9th Europe-Asia Congress on Mechatronics (MECATRONICS)/17th International Conference on Research and Education in Mechatronics (REM). 2016. Pp. 360-366.

15. **Agentenbasierte** dynamische Rekonfiguration von vernetzten intelligenten Produktionsanlagen–Evolution statt Revolution / D.Pantförder, et al. // Industrie 4.0 in Produktion, Auto-matisierung und Logistik. Wiesbaden: Springer Vieweg, 2014. Pp. 145-158.

16. **Nunes D. S., Zhang P., Silva J. S**. A survey on human-in-the-loop applications towards an internet of all // IEEE Communications Surveys & Tutorials. 2015. Vol. 17, no. 2. Pp. 944-965.

17. **Windt K.** Selbststeuerung intelligenter Objekte in der Logistik / M. Vec, M.-T. Hütt, M. A. Freund (eds.) // Selbstorganisation - ein Denksystem für Natur und Gesellschaft. Köln Weimar: Böhlau Verlag, 2006. Pp.271-316.

18. **Lee E. A.** Cyber physical systems: Design challenges // 2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC). 2008. Pp. 363-369.

19. **Langmann R., Stiller M**. Industrial Cloud–Status und Ausblick // Industrie 4.0. Wiesbaden: Springer Vieweg, 2017. Pp. 29-47.

20. **Scopus:** Content Coverage Guide // Scopus. [Электронный ресурс]. URL: https://www.elsevier.com/__ data/assets/pdf_file/0007/69451/Scopus_ContentCoverage_ Guide_WEB.pdf (дата обращения 15.09.2021). **[** Scopus: Content Coverage Guide // Scopus (2021, Sep. 15). [Online]. Available: https://www.elsevier.com/__data/assets/pdf_file/0007/ 69451/ Scopus_ContentCoverage_Guide_WEB.pdf. **]**

21. **Van Eck N. J., Waltman L**. Software survey: VOSviewer, a computer program for bibliometric mapping // Scientometrics. 2010. Vol. 84, Iss. 2. Pp. 523-538.

## ABOUT AUTHORS

**FABARISOV, Tagir,** Postgraduate student, Universität Stuttgart, Germany.

**SIEDEL, Georg,** Postgraduate student, Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Germany.

**VOCK, Silvia,** Dr. of Tech. Sci., Bundesanstalt für Arbeitsschutz und Arbeitsmedizin, Germany.

**MOROZOV, Andrey,** Jun.-Prof., Dr. of Tech. Sci., Universität Stuttgart, Germany.

**МЕТАДАННЫЕ**

**Заголовок:** Аспекты индустриальных кибер-физических систем, важных для методов оценки рисков.

**Авторы:** Т. Фабарисов[1], Г. Зиэдель[2], С. Вок[3], А. Морозов[4]

**Принадлежность:**

[1, 4] Университет Штутгарта, Штутгарт, Германия.

[2, 3] Федеральный институт Безопасности и медицины труда, Дрезден, Германия.

**Эл. адрес:** [1, 4] {first.last}@ias.uni-stuttgart.de, [2, 3] {first.last}@baua.bund.de

**Язык:** Английский.

**Источник:** СИИТ (научный журнал Уфимского государственного авиационного технического университета), т. 3, № 3 (7), стр. 23–29, 2021. ISSN 2686-7044 (онлайн), ISSN 2658-5014 (печатный вариант).

**Аннотация:** Кибер-физические системы (КФС) – усовершенствованные мехатронные системы, а также системы, состоящие из рассредоточенных мехатронных систем с сетевым взаимодействием, сложным программным обеспечением и коммуникационными протоколами коммуникации. Классические методы оценки рисков используют несколько известных способов оценки надежности и устойчивости технических систем. Однако КФС структурно и поведенчески более сложны, распределены и автономны, а их компоненты имеют неоднородную природу. Поэтому необходимо пересмотреть классические методы анализа рисков и дополнить их наиболее перспективными передовыми подходами. В качестве первого шага мы проводим систематический обзор литературы для оценки применимости методов оценки рисков для промышленных КФС. Этот метод начинается с формулирования исследовательских вопросов, на которые необходимо ответить. В данной работе мы сосредоточимся на первом вопросе, а именно: Какие аспекты промышленных КФС должны быть охвачены методами оценки риска? Ответ на этот вопрос станет основной предпосылкой для включения публикаций, представляющих методологии оценки риска для последующего рассмотрения и оценки качества в планируемом систематическом обзоре литературы. Чтобы укрепить наше понимание свойств КФС, мы рассматриваем не только определения, но и то, на что направлен фокус научных исследований, связанных с ними. Используя инструмент библиографической визуализации Vosviewer, мы иллюстрируем наиболее важные аспекты индустриальных кибер-физических систем.

**Ключевые слова:** кибер-физическая система; оценка риска; модели рисков; систематический обзор литература; методы основанные моделях; индустриальные КФС.

**Об авторах:**

**ФАБАРИСОВ Тагир,** асп. Университета Штутгарта, Штутгарт, Германия.

**ЗИЭДЕЛЬ Георг,** асп. Федерального института Безопасности и медицины труда, Дрезден, Германия.

**ВОК Сильвия,** д-р техн. наук, Федеральный институт Безопасности и медицины труда, Дрезден, Германия.

**МОРОЗОВ Андрей,** мл. проф., д-р техн. наук, Университет Штутгарта, Штутгарт, Германия. Jun.-Prof. Dr.-Ing.