Towards an Architectural Framework and Method for Realizing Trustworthy Complex Cyber-Physical Systems

Muhammad Rusyadi Ramli*,†, Martin Törngren†

Department of Machine Design, KTH Royal Institute of Technology, Stockholm, Sweden

Abstract

Cyber-Physical Systems (CPS) are evolving to become smarter, more autonomous, connected and collaborating. Provided with unprecedented capabilities, the CPS also represent unprecedented complexity and bring new risks that go beyond classical dependability. This paper outlines a framework for complex CPS with the purposes to facilitate holistic considerations of trustworthiness and its various attributes. The framework addresses trustworthiness from both technical (e.g., safety, reliability and security, etc.) and social perspectives (e.g. w.r.t. ethics, transparency and privacy). The framework is not intended primarily to replace existing CPS frameworks, but rather to complement them by providing an approach for incorporating trustworthiness considerations as a first class citizen. The workflow for the proposed framework is presented and we briefly outline its application to two use cases in the domain of intelligent transportation systems.

Keywords

Cyber-physical systems, Trustworthiness, Trustworthiness attributes, Architectural framework, Dependability

1. Introduction

The current rapid technological advancement, including in telecommunications (e.g., 5G, edge computing), sensors and artificial intelligence (AI), are transforming cyber-physical systems (CPS) to become smarter, more autonomous, connected and collaborating, [1]. This is for example seen with the development in autonomous vehicles and manufacturing, e.g. with future industrial robots capable of more flexible collaboration with other robots and humans. Provided with unprecedented capabilities, CPS brings the potential to develop new applications that can support the sustainability efforts of the United Nations (UN) [2][3]. However, at the same time they also represent unprecedented complexity and bring new risks that go beyond classical dependability, [4].

In paving the way for such more capable and complex CPS, it is essential that trustworthiness is considered and incorporated as a first class citizen during the CPS life cycle.

Joint Proceedings of RCIS 2022 Workshops and Research Projects Track, May 17-20, 2022, Barcelona, Spain.

*Corresponding author.

† These authors contributed equally.

ramli2@kth.se (M. R. Ramli); martint@kth.se (M. Törngren)

https://www.kth.se/profile/ramli2 (M. R. Ramli); https://www.kth.se/profile/martint (M. Törngren)

With the concept of trustworthiness we refer to relations w.r.t. to a particular system; such a relation could be between technical systems (as part of their collaboration) and/or between systems and their (human) stakeholders. As such, trustworthiness naturally relates to both technical properties such as safety, reliability, availability and security, but also to social considerations such as ethics, transparency and privacy.

The Trustworthy AI guidelines [5] by the European Commission also takes such a technical and social perspective to trustworthiness. We believe that this broad view on trustworthiness is important since the services we use in the future will in many cases be controlled and managed by large scale collaborating CPS - our lives will virtually be in their hands. The corresponding risks will encompass dependability of systems in terms of for example safety and availability, but also other social implications. While the trend towards automation will continue, the CPS will strongly interact with humans at different levels, e.g., human in the loop, human on the loop)[6].

In order to realize trustworthy complex CPS, thus both technical and social perspectives must be addressed explicitly. In the following we refer to properties such as safety, security, reliability, privacy and transparency, as trustworthiness attributes (representing different facets of trustworthiness).

As CPS are provided with new capabilities and being deployed in more open environments, their complexity will increase and so will also the corresponding organizational complexity, [4]. At the same time, their socio-technical impact will also increase, necessitating that a larger number of trustworthiness attributes need to be considered for future CPS, adding to the CPS requirements. Developing future CPS will thus increasingly involve larger teams of people to be involved. The larger number of experts and aspects involved will lead to a corresponding increase in the number of viewpoints, in turn implying multiple (explicit or implicit) dependencies between the viewpoints that need to be addressed, see ISO/IEC 42010 for a description of the corresponding terminology, [7]. The increasing technical and organization complexity of CPS, bears several risks related to trustworthiness. In particular, (1) new risks related to complex CPS are likely to be underestimated, e.g. due to a lack of awareness - cmp. with the noticed limited insights into cyber-security risks, and (2) dependencies and trade-offs between trustworthiness attributes may not receive sufficient attention. For instance, cyber security nowadays becomes as important as safety in the development of connected and automated vehicles (CAVs). However, it is challenging to address safety and cybersecurity as interdependent aspects, in particular during the early development stages, due to the absence of well-established guidance[8]. As a rather likely result of (1) and (2), trustworthiness (and its attributes) may be considered rather late into the system development (or even operation), increasing the costs drastically for compensating for insufficient designs and potentially even worse, leading to system failures. Ensuring trustworthiness requires to identify and relating trustworthiness attributes to relevant aspects that some stakeholders are concerned about. These activities can be done by using reference architectures or frameworks. In particular, architectural frameworks provide a common language for all stakeholders to communicate and align their ideas [9]. Nevertheless, to the best of our knowledge, no existing framework puts forward a comprehensive view of trustworthiness, such as in the EU Trustworthy AI guidelines, thus encompassing the lenses of technical and social perspectives.

This paper outlines a framework for realizing trustworthy complex CPS. The framework takes technical and social perspectives into account, with the purposes to support holistic considerations of trustworthiness and its various attributes. The framework is not intended primarily to replace existing CPS frameworks, but rather to complement them by providing an approach for incorporating trustworthiness considerations as a first class citizen. We draw upon existing frameworks and guidelines, such as the CPS framework by the National Institute of Standards and Technologies (NIST) [10], a reference architecture for edge computing (RAMEC) [11], a reference architecture model for Industrie 4.0 (RAMI) [12], and the Ethics Guidelines for Trustworthy AI proposed by European Commission [5] in developing the framework (e.g., identifying the requirements, aspects, etc).

The development of our framework also draws upon two workshops with industry and academia, conducted as educational workshops on trustworthiness and dependability in edge-based CPS. The course modules were organized as part of the Center for Trustworthy Edge Computing Systems and Applications (TECoSA) at KTH. At the workshops, the framework was presented and discussed, and at a second workshop, the participants provided additional feedback and insights based on their own state of the art studies and case studies. Further details about this course module can be found on the TECoSA webpages[1].

The main contributions of the paper is to present a set of concepts and an approach to address trustworthiness in the context of complex CPS, leveraging architectural frameworks, and thus paving the way for a trustworthiness centered framework. Section 2 of the paper describes relevant frameworks providing a background for the work, while Section 3 presents the outline trustworthiness framework and a workflow for how to use it. Section 4 describes illustrative case studies and Section 5 provides discussions regarding the framework. Finally, Section 6 presents conclusion and future work.

2. State-of-the-art and Relevant architecture frameworks

The understanding of the importance of trustworthiness is growing but the efforts are most often siloed, with many frameworks and techniques addressing only one or a few of trustworthiness frameworks.

As already mentioned, trustworthiness should be seen in the context of relations, e.g. between humans and CPS, or between different CPS. Psychological research has shown that trust between humans and robots depends on several attributes including predictability, dependability, and faith, relating to e.g. controllability, understandability, and performance, [13]. Trustworthiness can also be studied in the context of trust between different parts of a CPS, such as in "trusted computing" [14], and in terms of fault-tolerant computing - detecting and dealing with failing components.

The recent Trustworthy AI guidelines have been criticized as being unclear in several ways, for example regarding to the relations between trustworthiness requirements such as reliable vs. ethical and regarding the intention of trustworthiness (e.g. as referring to AI algorithms and/or their developer), [15]. This supports our understanding and work in the direction of a framework to clarify such issues.

[1] www.tecosa.center.kth.se

Several so called architectural frameworks have been proposed in order to facilitate the management of complex systems. In the following we briefly highlight a few architecture frameworks of relevance to CPS and trustworthiness.

1. **NIST CPS framework:** NIST developed a framework in consultations with a larger number of stakeholders to provide common definitions and facilitate interoperability between systems in developing CPS [16]. The NIST framework describes three facets during CPS's lifetime: conceptualization, realization, and assurance. The framework then facilitates the description of these three facets through "aspects". Aspects refer to the concerns addressed by developers and operators of the CPS. The framework includes Trustworthiness as one aspect among several, focusing primarily on the technical attributes of trustworthiness as compared to the Trustworthy AI guidelines [5].
2. **RAMI 4.0:** RAMI 4.0 was proposed by the German initiative "Platform Industrie 4.0". The framework considers life cycle streams following IEC 62890, such as development and maintenance/usage type, production, and maintenance/usage instance. This stream can be seen in the x-axis of the framework. The framework also consists of several layers (y-axis) such as asset, integration, communication, information, functional, and business. The Z-axis of a framework consists of hierarchy levels following IEC 62264/61512 such as product, field device, control device, station, work centers, enterprise, and connected world. RAMI does not explicitly at a high level consider trustworthiness attributes.
3. **RAMEC:** RAMEC was proposed by the European Edge Computing Consortium. The framework was developed based on existing models such as RAMI 4.0 and the Smart Grid Architecture Model (SGAM). RAMEC addresses edge computing views in the manufacturing domain. RAMEC consists of hierarchy levels of computing continuum (z-axis), layers (x-axis), and cross-layer concern (y-axis). RAMEC highlights security as part of one of the cross-layer concerns.

Unlike existing architectural frameworks mentioned above, the framework we outline aims to put "trustworthiness" attributes as the first-class citizen when developing, maintaining, and operating complex CPS. The details about our proposed framework is explained in the next section.

3. Outlining a proposed trustworthiness framework

Complex CPS development, maintenance, and operation require the involvement of many stakeholders with different expertise. Complex CPS also consists of diverse technologies, components and structures, which are influencing each-other when integrated to provide the intended capabilities. Dealing with "trustworthy" complex CPS imposes several new challenges; requirements stemming from individual trustworthiness attributes need to be identified and it is moreover necessary to identify the dependencies between trustworthiness attributes. Such attributes may have partially conflicting goals in the first place, such as the classical trade-off between safety and availability, but may also result in mechanisms (designed into the CPS) that share the same resources and that may conflict during operation. For example, cybersecurity mechanisms such as authentication and encryption will take time to perform, impacting real-time performance, which in term may also be necessary for certain safety functions.

Given a particular CPS, our trustworthiness framework provides a set of questions as follows:

1. What attributes of trustworthiness are relevant for this CPS and given that trustworthiness is about relations - which relations are of concern? Answers to this question would help in identifying high-level requirements on trustworthiness.
2. What relationships, dependencies and trade offs exist between, (i) trustworthiness attributes in terms of their goals, (ii) how the attributes relate to different system aspects such as data, functions and computations, and, (iii) what dependencies exist between attributes due to their relationships with aspects - such as shared resources in a computing system. Answers to these questions would help in identifying traceability from attributes to the system aspects, and trade-offs between attributes relating to system design decisions.
3. What roles and processes are needed to address trustworthiness attributes? Finally, this question will help in identifying what needs to be done to ensure trustworthiness of a CPS during its life-cycle in terms of roles (e.g. a cybersecurity manager, functional safety manager, cybersecurity and safety architect), and processes.

As shown in Figure 1, our proposed framework was developed and inspired by existing framework models that have been developed, such as the NIST CPS framework, RAMI 4.0, and RAMEC. The core idea of the proposed framework is to provide vocabulary that describes and supports the understanding of trustworthy complex CPS during its whole life cycle. The proposed framework is not intended to replace the existing frameworks fully but can be positioned as a complement to the existing frameworks. For this reason, the proposed framework comprises the following concepts: trustworthiness attributes, levels, aspects, and lifecycle. Each concept is briefly explained as follows:

3.1. Attributes

The brief overview above highlights potential problems that may hinder the development, maintenance, and operation of trustworthy complex CPS. One of the main reasons is that determining proper trustworthiness attributes that can satisfy all stakeholders' requirements is challenging without architectural framework guidance.

Complex CPS will typically come to incorporate more and more AI, operating at higher levels of automation. This implies that ethical guidelines of AI becomes a new consideration and requirement for CPS. Hence, the proposed framework aims to cover trustworthiness attributes regarding the quality of the systems and the ethical requirements of complex CPS. These attributes include quality, availability, reliability, resilience, robustness, security and privacy, safety, sustainability which all refer to the quality of system requirements. The proposed framework includes transparency/explainability/auditability, fairness, and respect for human autonomy for ethical requirements.

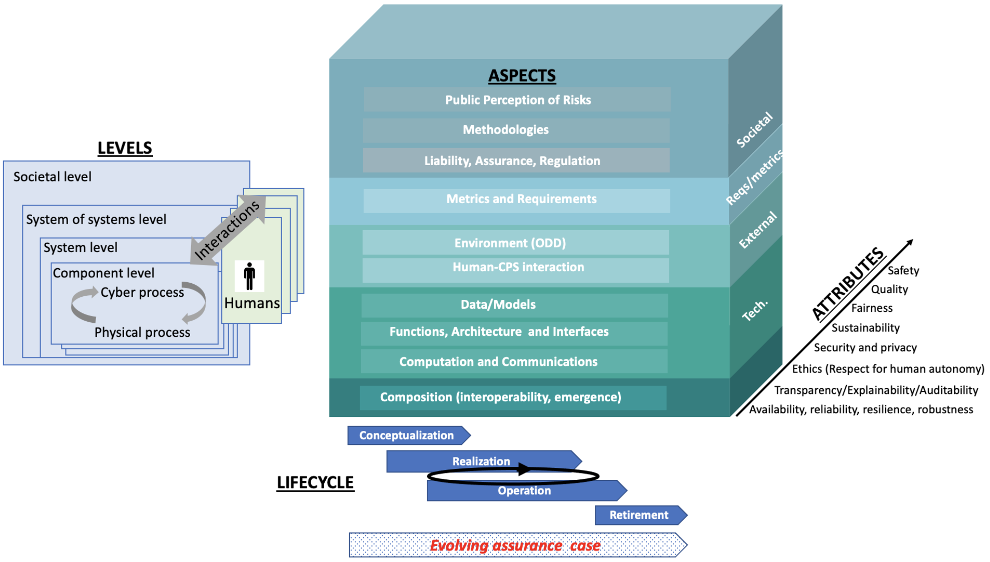

Figure 1: The proposed trustworthiness framework

3.2. Levels

Similar to the conceptual model of CPS in the NIST CPS framework, the proposed framework considers "levels" to highlight the potential interactions of devices and systems in a system of systems. Moreover, the proposed framework added a societal level to highlight possible interactions of mentioned system levels in society.

3.3. Aspects

Aspects refer to the characteristics of a system that one or some of its stakeholders are concerned about. In our proposed framework, we took the aspects from NIST CPS framework and add other relevant aspects that we identified from our workshop discussions. Then, we grouped each aspect based on their concerns such as societal, requirements/metrics, external, composition, and technological.

3.4. Lifecycle

Lifecycle refers to the view on systems engineering activities such as conceptualization, realization, operation, and retirement of the complex CPS. It also specifically includes all activities needed over the CPS life-cycle to provide trustworthiness assurance.

3.5. Applying the framework

The framework can be used to address the questions elaborated on page five. For this purpose, we propose a workflow to guide stakeholders in using the framework, see Figure 2. The workflow

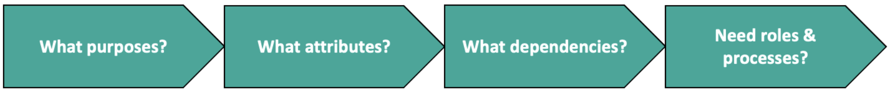

Figure 2: Workflow for the proposed framework application

consists of four steps, each step addressing the corresponding question. The detailed explanation of the workflow is as follows:

1. **Identifying the System of Interest (SoI), its context and stakeholders:** The workflow begins with identifying the purpose of the system (this could be an existing system or a system to be developed). Identifying the system in its context including key stakeholders, is essential in all types of systems analysis - in particular for establishing the concerns (and viewpoints) of the stakeholders. Existing architectural frameworks serve as a reference regarding relevant viewpoints - and thus for the SoI aspects. Having established the SoI, its context, and stakeholders, with their concerns, provides a basis for further dealing with trustworthiness (the following steps).
2. **Attributes identification:** This step is intended to address the question (1) - identifying the trustworthiness attributes. One important way to get insight into this question is to identify interactions and relations between humans (different stakeholders) and the SoI, and between key SoI (CPS) components. Further, to assess the corresponding risks per trustworthiness attribute, established attribute specific techniques should be applied, such as hazard and risk analysis (for safety), threat and risk analysis (cyber-security), and for example the AI ethics method called ECCOLA [17] (for ethical considerations). The result of step 1 is an identification of trustworthiness attributes and their risks for the given SoI in its context. In doing this analysis, the levels of interest for a given SoI has to be identified. It is common practice always consider also the next "upper system" in order to capture non-intended or emergent effects; for example, what might seem as a benign risk at the level of e.g. a machine, might appear as a more critical risk at the level of human-machine interaction.
3. **Dependencies identification:** This step addresses question (2) - identifying the relationships, dependencies, and trade-offs between attributes and aspects. Several systems engineering methods can assist in this step. For example, methods for architecture tradeoff analysis method (ATAM) with the cost benefit analysis method (CBAM) [18] have as one purpose to identify trade-off points between quality attributes and could as such be used to identify dependencies and trade offs related to trustworthiness attributes. Existing relevant architectural frameworks may also give some guidance regarding dependencies between aspects.
4. **Roles and processes identification:** This step is intended to address question (3). In particular, after identifying the trustworthiness attributes, and their dependencies concerning the levels and aspects, the last step is concerned with how to address them during in a coordinated way during the life-cycle of the SoI. Systems engineering and life cycle processes (ISO 15288) [19] as well as attribute specific standards (e.g. for cybersecurity and safety) can be used to identify the roles and processes to address trustworthiness

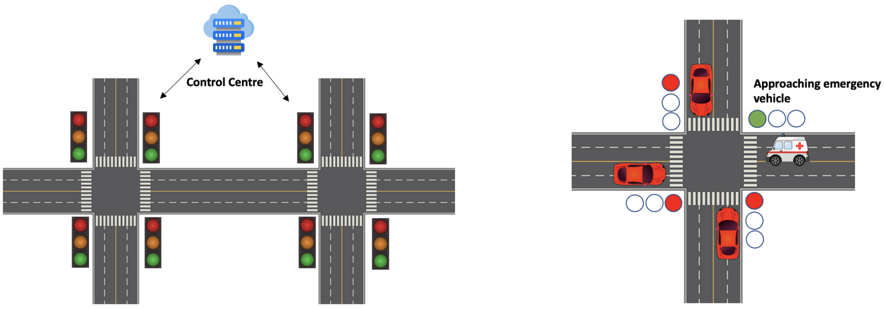

Figure 3: (Left) smart intersection analytic system (Right) smart intersection vehicular coordination system

attributes. The life-cycle stages require specific emphasis on trustworthiness including system concepts/requirements, development, assurance/certification and operational safety management. An interesting aspect of particular concern is the "certification" or approval of future highly automated CPS (compare with automated vehicles) and the need for new methodologies and research in this direction. Similarly, safety management of operational systems becomes especially important for new systems with new risks and the potential for emergent behavior, emphasizing the need for data collection and reporting of incidents (e.g. near misses) and accidents.

4. Case studies and evaluation

This paper considers smart intersections of intelligent transportation systems (ITS) to evaluate the proposed framework. As depicted in Figure 3, there are two smart intersections systems, but they have been designed for different purposes. Figure 3 (Left) shows smart intersection for data gathering and handling traffic congestion, and Figure 3 (Right) illustrates smart intersection for prioritizing emergency vehicles. Consequently, since they have different purposes, the stakeholders, aspects, and trustworthiness attributes to realize them also differ. We have applied the framework to these case studies. Given the limited space in this short paper, we briefly elaborate on these two case studies in the following and point out some experiences related to the trustworthiness framework.

4.1. Case one: Smart intersections for traffic congestion

Traffic congestion occurs as the number of vehicles increases. Intersections play an essential role in handling traffic congestion. We assume each traffic light has roadside unit (RSU), providing traffic lights with sensing, networking, computation and storage capabilities. As shown in Figure 3(Left), traffic information is gathered in each traffic light and offloaded to the control center. The control center then calculates the green time for each phase at the intersection based on the collected information from traffic lights, and moreover collects data about traffic behavior and road conditions, for example using cameras, for longer term analysis of e.g. road scenarios.

4.2. Case two: Smart intersections for emergency vehicle

The arrival time for emergency vehicles such as police cars, ambulances, and fire trucks should be minimal. Similar to case one, intersections also play a vital role in handling them. In this short case study, we assume that vehicles can communicate to the RSUs (using some appropriate communication protocol). The messages sent by a vehicle include vehicle type (e.g., emergency or ordinary) and the directions. Based on the gathered information, RSUs can distinguish vehicle types, be aware of the future direction of the emergency vehicle, and can therefore give precedence to the emergency vehicle's direction. After the emergency vehicle has passed the intersection, the scheduling traffic system can return to normal mode.

4.3. Reflections based on case studies

In general, both of case studies involve exchange and sharing of information between vehicles and a smart infrastructure. Based on the description of both case studies above, we can identify that the purpose of case one is for traffic analytics and case two for vehicular coordination. With respect to Step 1 of the framework, both systems represent collaborating systems (also referred to as systems of systems - SoS). As such, extra emphasis has to be placed on identifying the boarders of the SoI (the SoS) and its stakeholders, including their responsibilities. Referring to Step 2, the smart intersection system of case one relies on data to be gathered continuously (e.g. from vehicles and road side units with sensors), and stores the data in the control center for analytic purposes. Given the focus on data gathering and analytics, case study one becomes subject to privacy concerns and GDPR restrictions. If the traffic lights malfunction, this could also impact traffic conditions, both in terms of delays and safety. On the contrary, case study two deals time-critical control, and is thus highly safety critical, in turn resulting in derived requirements on real-time performance and reliable error detection. As for step 3, the relationships, dependencies, and trade-offs between attributes, for example, security, fairness, and privacy (for case one) and safety, security, and availability (for case two) need to be analyzed. For example, there could be potential trade-offs between safety and availability, particularly for case two when the malfunction occurs. The operator then needs to shut down the system. However, this situation could lead to traffic congestion and traffic collisions. In addition, the hackers can take this opportunity to access and steal the data. As discussed for Step 4, we would here briefly highlight the need for certification and safety management for the RSUs, in particular for Case study two.

5. Discussion

This section summarizes feedback we obtained through the workshops including through the discussions at these workshops. The need to provide a common and consistent language was highlighted. Should one for example use the terms viewpoints, aspects or facets (as somewhat synonymous)? For communication purposes it is essential to define and clarify terms and use them consistently.

What would make the framework useful? One of the participants said that the framework would be useful if it could provide insight into other's viewpoints. We believe that this is a a very relevant point; given the multiple stakeholders and corresponding viewpoints involved with complex CPS. In the case of the proposed trustworthiness framework, we address that through the trustworthiness attributes and their relations to aspects.

At one of the workshops, trustworthiness as referring to relations was intensively discussed. It was identified that "trust" is naturally seen differently concerning Human-CPS vs. CPS - CPS, and that the corresponding trust aspects are typically addressed by different scientific communities and practitioners (e.g. human-machine interaction/psychology vs. e.g. computer/-communication engineering).

Trustworthiness potentially encompasses a very large number of attributes, and a complex CPS will also have many aspects - clearly mirroring some of the inherent complexity in CPS. One of the discussions treated this topic; how detailed and how exhaustive should a framework be with respect to attributes and aspects? We believe that a trustworthiness framework needs to be comprehensive. At the same time, there is a need to organize the multitude of aspects and attributes. If hierarchical ways or organizing them, or levels of abstraction, could be used, this would reduce the cognitive complexity and facilitate framework use. This represents a topic for future work.

6. Conclusion and Future Work

This paper has proposed a framework, which views complex CPS through the lens of trustworthiness and its multiple attributes. We believe that this is important today as new systems are pushed onto the market on business grounds, many times without legal frameworks, standards and guidelines in place. We hope that the proposed framework through its guided questions, and supported by existing architecture frameworks, processes and methods, can help to position trustworthiness as a first class citizen. There are several potential directions for further work including, more detailed evaluation through in-depth case studies, further interactions with experts and systems engineers, and the development of more elaborated guidelines for how to use the framework. There is also room for more work on organizing the framework in to facilitate complexity management (hierarchies, abstraction). including potential tool support.

Acknowledgments

The research has been carried out as part of the Vinnova Competence Center for Trustworthy Edge Computing Systems and Applications at KTH Royal Institute of Technology, and was in addition supported by the InSecTT ECSEL Joint Undertaking (JU) project, under grant agreement No 876038 (see www.insectt.eu for a full acknowledgement and disclaimers). The document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains. We also acknowledge useful discussions from the workshop participants at the TECoSA workshops and with Fredrik Asplund, KTH.

References

[1] Y. Zhou, F. R. Yu, J. Chen, Y. Kuo, Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities, IEEE Communications Surveys Tutorials 22 (2020) 389–425.

[2] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, S. K. S. Gupta, Ensuring safety, security, and sustainability of mission-critical cyber–physical systems, Proceedings of the IEEE 100 (2012) 283–299.

[3] U. N. Economic, S. Council, Sustainable development, 2019.

[4] M. Törngren, Cyber-physical systems have far-reaching implications, HiPEAC Vision 2021 (2021). URL: https://doi.org/10.5281/zenodo.4710500. doi:10.5281/zenodo.4710500.

[5] High-Level Expert Group on AI of European Commission, Ethics guidelines for trustworthy ai, 2019. URL: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[6] F.-Y. Wang, The emergence of intelligent enterprises: From cps to cpss, IEEE Intelligent Systems 25 (2010) 85–88.

[7] I. O. for Standardization, ISO/IEC/IEEE 42010:2011 - Systems and software engineering — Architecture description, Technical Report, Geneva, CH, 2011.

[8] C. Schwarzl, N. Marko, H. Martin, V. Expósito Jiménez, J. Castella Triginer, B. Winkler, R. Bramberger, Safety and security co-engineering for highly automated vehicles, e & i Elektrotechnik und Informationstechnik 138 (2021) 469–479.

[9] R. Cloutier, G. Muller, D. Verma, R. Nilchiani, E. Hole, M. Bone, The concept of reference architectures, Syst. Eng. 13 (2010) 14–27.

[10] E. Griffor, C. Greer, D. Wollman, M. Burns, Framework for cyber-physical systems: Volume 1, overview, 2017.

[11] A. Willner, V. Gowtham, Toward a reference architecture model for industrial edge computing, IEEE Communications Standards Magazine 4 (2020) 42–48.

[12] M. Hankel, B. Rexroth, The reference architectural model industrie 4.0 (rami 4.0), ZVEI 2 (2015) 4–9.

[13] K. E. Schaefer, J. Y. C. Chen, J. L. Szalma, P. A. Hancock, A meta-analysis of factors influencing the development of trust in automation: Implications for understanding autonomy in future systems, Human Factors 58 (2016) 377–400.

[14] Z. Huanguo, L. Jie, J. Gang, Z. Zhiqiang, Y. Fajiang, Y. Fei, Development of trusted computing research, Wuhan University Journal of Natural Sciences 11 (2006) 1407–1413.

[15] AlgorithmWatch, Trustworthy ai' is not an appropriate framework, 2019. URL: https://algorithmwatch.org/en/trustworthy-ai-is-not-an-appropriate-framework/.

[16] T. H. Nguyen, M. Bundas, T. C. Son, M. Balduccini, K. C. Garwood, E. R. Griffor, Specifying and reasoning about cps through the lens of the nist cps framework, 2022.

[17] V. Vakkuri, K.-K. Kemell, M. Jantunen, E. Halme, P. Abrahamsson, Eccola — a method for implementing ethically aligned ai systems, Journal of Systems and Software 182 (2021) 111067.

[18] R. L. Nord, M. R. Barbacci, P. Clements, R. Kazman, M. Klein, Integrating the Architecture Tradeoff Analysis Method (ATAM) with the cost benefit analysis method (CBAM), Technical Report, Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, 2003.

[19] E. Freund, Iso/iec 15288: 2002, systems engineering-system life-cycle processes, Software Quality Professional 8 (2005) 42.