International Journal of Safety and Security Engineering
Vol. 13, No. 2, April, 2023, pp. 213-225
Journal homepage: http://iieta.org/journals/ijsse

Trust Cyber Physical Systems: Trust Degree Framework and Evaluation

Zina Oudina[1*], Makhlouf Derdour[2], Rachid Boudour[1], Ahmed Dib[1], Mohamed Amine Yakoubi[1]

[1] Computer Science Department, University of Badji Mokhtar Annaba, BO 12, Annaba 23000, Algeria
[2] Computer Science Department, University of Oum El Bouaghi, Oum El Bouaghi 04000, Algeria

Corresponding Author Email: zina.oudina@univ-annaba.org

https://doi.org/10.18280/ijsse.130204

Received: 3 January 2023
Accepted: 8 April 2023

Keywords:
Cyber-Physical System (CPS), trust degrees, trust degree framework, evaluation

ABSTRACT

Trust is the currency of every transaction and exchange and is the pillar of the trusted system concept, which is one of the needs of today and the future. Those systems ease communication and sharing with little user-side load and are used in numerous organizations, financial institutions, military scenarios, and highly confidential works. The evolution of Cyber-Physical Systems (CPS) affects people's way of life and is applied in health care, smart homes, commerce, etc. The cyber-physical system is treated as a trust system if the principles of security and safety, confidentiality, integrity, availability, and another set of properties are guaranteed. The development of CPS requires consistency in requirements management, metrics, formal test process descriptions, and computation methods. The research community is focused on how to realize a novel CPS with high confidence. In the literature, there is no clear definition of all kinds of trustworthiness metrics, and there is no classification of trustworthiness and trust metric types. There is no defined standard for trustworthiness, and there are no rules for calculating CPS trustworthiness. This paper proposes a framework for the evaluation of trust in CPS. This framework ranks the trustworthiness of CPS by degree. Trust degrees for the cyber-physical system are defined, along with a set of requirements and properties for each degree. We proposed a proprieties classification based on functionality and obligation as well as a simple mathematical formula to compute trust in the CPS, which formulates a quantitative view on the guarantee of security, trustworthiness, and trust attributes. The results of this study, which are based on the use of the proposed framework to evaluate the trust of CPS and case study, indicate that our quantitative method is more objective than existing qualitative methods.

1. INTRODUCTION

In not too distant future, an autonomous vehicle will take us around the "smart" city. May we travel by commercial plane without a pilot? Anywhere, a smart robot or a medical device might measure our vitals and send updates to our doctor. Everything will be based on the "internet of devices" or "internet of services," with internet-connected sensors and actuators scattered across our physical world and even inside our bodies. In almost the same way, in CPSs, there is a connection between heterogeneous devices via wireless networks. The communication is established via sets of sensors and actuators. Applications of CPS have been in many fields, such as aerospace, transportation, critical infrastructure, and industrial manufacturing. Why should we trust the CPS?

Cyber-physical system trustworthiness has been a key source of concern because there are no guidelines for establishing trust in the CPS. In literature, a limited contribution treated trust and trustworthiness issues from angles other than security [1]. Also, there is no clear definition of trustworthiness metrics, and there is no reclassification of those trustworthiness metrics [1]. There is no standard defined for trustworthiness. There are just suggestions for what should be taken into account, along with certain self-certification procedures [Gol Mohammadi]. There is not a generic model or framework that addresses the quantitative evaluation of trust in CPS with objectivity and ease.

In this regard, there are several types of research, but they are not systematic and do not have long-term goals. There is no work that addresses the entire issue of trust in CPS. Some of the works target the security angle; others treat the trustworthiness of CPS components, such as software, without targeting the trust computation. Some research is done in series and over a project, such as in the study [2], they provided a framework for requirements engineering and design methodologies for taking trustworthiness into account during the design phase of the CPS. They provided design techniques, architectures, and detailed service specifications for systems that balance trust and trustworthiness. They proposed a conceptual model of design-time end-to-end trustworthiness evaluation, that used the end-to-end trustworthiness calculator (E2E TW calculator), composed of (the workflow converter, formula builder, trustworthiness report, and trustworthiness profile builder). The process of computation in the study [2] is so long and related to provided metrics values from software developers, may be used for certified product only. Also, the set of metrics is very limited.

A trust-based secure cyber physical systems approach is proposed [3], a two tier trust oriented approach: a) Internal Trust, which contains trusted internal entities such as sensors, actuators, and communication networks, and b) External Trust, which represents the physical environment of the CPS.

Trustworthiness solutions for integrated manufacturing physical-cyber is presented in the study [4], combining dependability and cyber-security requirements and modeling the cyber-security component with a resilient systems framework. As a result, they considered that manufacturing cyber-physical systems delivered trusted services.

A layer-based security approach is presented in the study [5] based on OSI and PRM models that target the security of each layer.

In this paper, we seek to create a successful and sustainable trust evaluation. We started with a well-reasoned framework of trust degree. The theory was then supplemented with requirement descriptions and metrics definitions for each degree, as well as a practical case study demonstrating how we can incorporate the proposed degree and quantitative evaluation of the trust context.

As a methodology, we performed a systematic literature review (SLR) [6] to survey the publications in the area of security and trustworthiness of CPS. Also, we used requirements engineering (RE), which is a systematic and disciplined approach [7] for the specification and management of requirements.

The remainder of the paper is structured as follows: Sections 2 and 3 discuss the contribution, methodology, and background. Section 4 explains the proposed trust degree framework for CPS, outlines the benefits of ranking trust in degrees, and presents some arguments. Metrics are presented in Section 5. The trust evaluation is presented in Section 6 and discussion in Section 7. We conclude our work and highlight future work in Section 8.

2. CONTRIBUTION AND METHODOLOGY

The purpose of this study is to:

- Understand secured CPS, trustworthy CPS, trusted CPS.
- Propose a framework for trust CPS by ranking trust in degrees and specifying a set of requirements, and properties for each degree. This proposed framework facilitates the evaluation and computation of trust as a quality of CPS in a quantitative manner, targeting more objectivity.
- Propose a simple mathematical formula to compute trust in the CPS (which should create metrics expressing a quantitative view on the guarantee of security and trustworthiness as well as trust qualities).

This research takes into account four research questions.

- RQ1: What are the CPS's requirements for security and trustworthiness?
- RQ2: Is there a model or map for trust CPS evaluation?
- RQ3: What are the metrics that help developers evaluate the trustworthiness of CPS?
- RQ4: Which evaluation method (mathematical) can be used for the evaluation of trust in the CPS?

2.1 Contribution

This work aims to evaluate the trust of CPS. We conduct a comprehensive overview and analysis of the cyber-physical system, including its security and trustworthy aspects. We proposed a framework of trust degrees for the CPS and presented some arguments, a set of requirements in addition to the attributes of each degree, and finally, a simple mathematical formula to compute the trust of the CPS. At that stage, we don't consider how the attributes are measured or what the tools of measurement are; we focus only on how to simplify the complexity of trust CPS and how to give a simple and objective evaluation of this trustworthiness. The contributions entail the following:

- Background on CPS and some definitions, and comparison between concepts.
- Requirements set for trust in CPS.
- Proposed framework for trust degree and benefits of ranking trust according to the degree.
- The classification of metrics.
- Proposed mathematical formula for computing the trust of CPS.
- An algorithm for the computation of trust in the CPS and a case study.

2.2 Methodological contributions

In this paper, we used a combination of methods, including:

- Systematic Literature Review (SLR)
- Requirement Engineering
- Direct Content Analysis
- Case Study

2.2.1 Methodology (SLR)

The study and consolidation are based on publications regarding the security and trustworthiness of CPS. We used some digital libraries (IEEE Xplore, Springer, and Science Direct) and the following set of search sentences: "trust cyber physical system", "trustworthy cyber physical system", "secured cyber physical system", "evaluation of trust CPS". According to each database, the number of funded papers is shown in Table 1. We obtained a total of 525 papers after excluding all papers that lacked keywords (trust or trustworthy and secured). To choose the papers for review, a filtering technique based on a few criteria (inclusion and exclusion) was applied.

Table 1. Number of papers found for each search

Digital library	IEEEX plore	Springer	Science Direct
Sentence1	635	3708	8293
Sentence2	212	862	2646
Sentence3	1744	4375	8416
Sentence4	32	1446	3006

Inclusion Criteria

- Published from 2006 to 2022
- Using English
- Applied subject of" trust CPS" or "secured CPS, or "trustworthy CPS"
- Corresponded to the study's focus

Exclusion Criteria

- Paper published before 2006
- Not using English
- The topic of the paper is unrelated to "Secured" or "trusted", or" trustworthy CPS"
- Papers Papers with insufficient data for our study

We obtained 38 papers for our study. Some papers published before 2006 are referenced due to the importance of their content. The list of surveyed papers is presented in Table 2.

2.2.2 Requirement engineering

- Define the core requirements for designing trust of CPS in the engineering phase.
- Define the subset of requirements for each degree.
- Define the source of requirements.

2.2.3 Direct content analysis

- To provide high trustworthiness evidence of the proposed evaluation method.
- To prove the correctness of our proposed framework and compare it with other existing frameworks.

2.2.4 Case study

- To ensure the validity of the Trust Degree framework in a real example.
- To explain the use of the framework and the process of trust evaluation.

3. BACKGROUNDS

This section presents a CPS background and introduces three concepts: the concept of a secured system, a trustworthy system, and a trust system. Moves on the comparison of these concepts and defining the core requirements for trusted CPSs.

3.1 Cyber-physical systems

In 2006, Lee invented the term "cyber-physical systems" [8]. CPS is the fusion of computation and physical processes. Physical processes are monitored and controlled by embedded computers and networks, typically with feedback loops where computations are affected by physical processes and vice versa [9]. Wireless networks are used to connect heterogeneous devices in the CPS. The communication is established via sets of sensors and actuators. Applications of CPS have been in many fields, such as aerospace, transportation, critical infrastructure, and industrial manufacturing.

In the study [10], they surveyed many CPS architectures that depend on system requirements and application domains, such as cloud-based architecture, SOA-based architecture, multi-tier architectures, 5C-based architecture, and layered architecture. The most used architectures are built on the 5C architecture:

Connection, conversion, cyber, cognition, and configuration.

- Connection level: The point at which a device's design and behavior enable self-connection and self-sensing.
- Conversion level: By measuring data from linked devices and sensors, machines can use self-aware knowledge to anticipate future problems.
- Cyber level: Using instrumented features, each machine generates its own "twin" and creates it.
- Level of cognition: The monitored system is thoroughly understood. Both the machine's state and the choice of which jobs to prioritize to keep the process running smoothly are available. Diagnostic and decision-making processes include collaboration. the dissemination of learned information to users
- Configuration level: According to priority, the machine or production system can be configured.

Due to the complexity of CPS and its large application, the design, modeling, and testing of this system are very difficult. In the study [10], they explained that the researchers adopted model-based approaches, different methodologies and techniques, and tools for modeling cyber-physical systems. In the study [11], they surveyed and classified test methods and highlighted the testbed as the most commonly used.

3.2 Trust systems

The underlying concept of human interactions is trust, which governs social, political, and economic rules and behaviors.

The acceptance of these norms for face-to-face interaction has taken thousands of years. This interaction involves two parties: the one who is trusted and the one who is trusted by. Recently, all interactions have been conducted online and have moved at a breakneck pace.

A trusted system is one that entrusts security policies and strategies to other systems. According to Wikipedia.org, "trust" in the context of computers refers to the object upon which a user transmits data through a communication channel.

Implementing trusted system technology is one technique to improve a system's ability to fight against attackers and harmful programs. The importance of trust systems has grown to the point where they have become strategies and initiatives.

3.3 Some relevant definitions

3.3.1 Secured system

Security is a characteristic and property of systems. The system is treated as secure if the principles of confidentiality, integrity, and availability are guaranteed.

3.3.2 Trustworthy system

Most researchers rely on two characteristics to define a trustworthy system (security and safety), forgetting the other basic features.

- If a system is implemented well and complies with all security requirements, it can advance in the trust stakes ("Purdue University," 2010).
- Trustworthiness is a holistic quality that encompasses security, integrity, and accessibility in addition to accuracy, reliability, privacy, safety, and survivability.

3.3.3 Trusted system

Trust can be defined in a variety of ways, including:

- The degree to which you enforce a specific security policy.
- With a trusted system, the user feels secure using it and has faith in it to complete tasks without covertly running dangerous or unapproved programs.
- A trust system is a level-based security system that offers protection.
- Trust is a degree; actually, developing a secured system is a goal, and being trusted or trustworthy to a certain degree is a feature of the system in question.

3.4 Comparison of three concepts

A trustworthy system is made up of a combination of computer hardware, software, and procedures that are suited to carrying out their intended functions and reasonably secure from misuse and intrusion. It also enforces the relevant security policy.

Secure, trustworthy, and trusted are system qualities that differ in terms of concerns, requirements, properties, and human interaction, as mentioned in Table 3.

However, there is a link and connection in that each quality may be complementary to the other by adding characteristics and properties to it (security and safety are both required to a sufficient degree to make a trustworthy cyber-physical system, in addition to a set of attributes). A secured system's being trusted or trustworthy to a certain degree is a characteristic of the system in context.

A trustworthy system is not necessarily a "trusted system," as that term is recognized, because it should be trusted by an organization or user and meet the expectations of another party. But the inverse is correct; the system to be trusted should be trustworthy. We can conclude that secured systems are included in trustworthy systems, and the latter are included in trust systems, as mentioned in Figure 1 (source: compiled by the authors).

We expressed the relationship between a secure and trustworthy system and the trust system by inclusion (Order relation) between two sets or more, because those qualities of a system are a set of practices that include a set of requirements and properties.

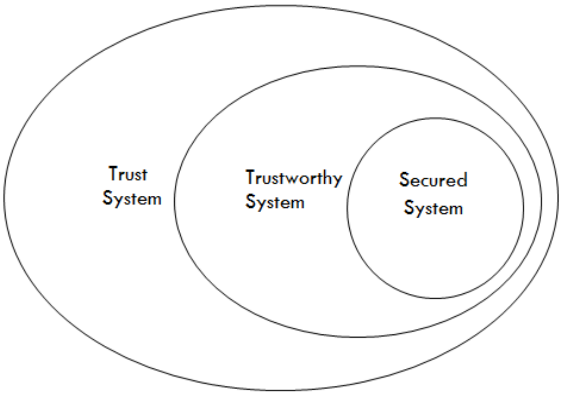

Figure 1. Trust system

3.5 Core requirements for trusted CPSs

It is vital to outline the fundamental requirements for designing trust in the CPS in the engineering phase. Our methodology for intending trust requirements is based on traditional requirements engineering (RE), which is a methodical and disciplined approach to requirements management [12, 7]. The source of requirements is based on documents. Pertinent documents are laws, standards, and mostly publications. The general stakeholders for CPSs are the law and the product user.

a) Engineering requirements: For developing a system, it is essential to identify the goals, needs, and available resources to help with a production of the system that complies with the requirements [13]. The requirements are used as a guideline for the implementation and as a reference for the verification and validation of the final product.
b) Cyber-Physical System Requirements: Understanding the goal and the available resources are the first step in designing CPS.
c) Trust (as a quality of the system) requirements:
   - CPS: The requirements of CPS should be coordinated with user requirements and organization requirements. The set of requirements consists of including all system actors and meeting the trust goals.
   - User: If the system was not developed in accordance with the user's requirements, the user will be made aware of this when using the system, which could lead to mistrust of the system and its final rejection.
   - Organization: The design of trust interacts with the use of technology to mediate trust between individuals, groups, or between artificial agents that operate as a representation of people or groups.

Table 2. List of surveyed papers

Ref	Subject
[1]	Trustworthiness attributes and metrics
[2]	Trustworthy Cyber-Physical Systems
[3]	Trust based secure cyber physical systems.
[4]	Trustworthiness requirements for manufacturing cyber-physical systems
[5]	A hierarchical security architecture for cyber-physical systems
[14]	Fundamentals of computer security technology
[15]	Security metrics: replacing fear, uncertainty, and doubt
[16]	Security content automation protocol (SCAP)
[17]	Information security and ISO 27001
[18]	Safety design concepts for statistical machine learning components
[19]	Data communication verification for safety goals
[20]	Safety standard IEC 61508
[21]	Safety management fundamentals and Annexes of ICAO safety management
[22]	Requirements engineering and management
[23]	Automation standards
[24]	security in industrial control systems
[25]	Security safety model
[26]	Cross-fertilization between safety and security engineering
[27]	Safety and security of Cyber-physical systems
[28]	Security requirements analysis
[29]	Modeling safety and security interdependencies with BDMP
[30]	The past and Future of Safety Management
[31]	Calculativeness, trust, and economic organization
[32]	Concepts and taxonomy of dependable secure computing
[33]	Aligning cyber-physical system safety and security
[34]	IT security metrics and measuring security
[35]	A survey of approaches combining safety and security for industrial control systems
[36]	Analysis of safe and secure industrial control systems
[37]	Consistency and stability of risk indicators
[38]	Safety and security risk assessment in cyber-physical systems
[39]	An analysis of software quality attributes and trustworthiness
[40]	Privacy requirements in system design
[41]	Threat modeling for security assessment in cyber-physical systems
[42]	Internetware: A software paradigm for internet computing
[43]	A trust-aware, p2p-based overlay for intrusion detection
[44]	Secure data transmission and trustworthiness judgement approaches
[45]	Trust handling framework for networks in cyber physical systems
[46]	Trust. io: protecting physical interfaces on cyber-physical systems

d) Business Requirement: The productivity of a company is increased by automating business procedures. To minimize the risks of utilizing those technologies, business processes and the software systems and services they include must be trustworthy.

Table 3. Differences between the three concepts

Systems	Requirements	Properties	Human interaction
Secure	Essential needs for security and safety satisfaction	Security, Safety	No human interaction
Trustworthy	Security and safety needs, Concern about how the system provides services that can be trusted	Security, Safety, Trustworthy properties	Potential to influence end users. Positive expectation without decision
Trusted	Security and safety, concerns about human interaction and the ability of system to be used to achieve its functional objectives effectively.	Security, Safety, Trustworthy properties, Trusted properties	Belief and satisfaction of other party Decision and evaluation by individual, guarantee that the system will work as expected

4. PROPOSED FRAMEWORK OF TRUST DEGREES FOR CPS

A trusted system, as described on Wikipedia.org, can be thought of as a level-based security system where protection is offered and managed in accordance with several levels. Since each stakeholder can have different ideas about trustworthiness and trust systems, a ranking into degrees for describing trustworthiness and trust attributes is needed.

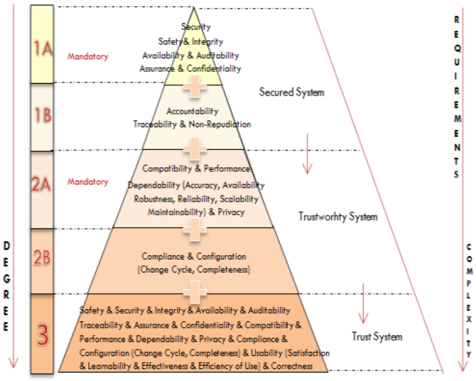
1A
Mandatory
Security
Safety& Integrity
Availability & Auditability
Assurance & Confidentiality
Secured System
1B
Accountability
Traceability & Non-Repudiation
2A
Mandatory
Compatibility & Performance
Dependability (Accuracy, Availability
Robustness, Reliability, Scalability
Maintainability) & Privacy
Trustworhty System
2B
Compliance & Configuration
(Change Cycle, Completeness)
3
Safety & Security & Integrity & Availability & Auditability
Traceability & Assurance & Confidentiality & Compatibility &
Performance & Dependability & Privacy & Compliance &
Configuration (Change Cycle, Completeness) & Usability (Satisfaction
& Learnability & Effectiveness & Efficiency of Use) & Correctness
Trust System
DEGREE
REQUIREMENTS
COMPLEXITY

Figure 2. Proposed trust degree framework

We propose a framework for classifying and ranking trust degrees based on a set of requirements and obligations in a user-centered manner. Software's trustworthiness was described by Amoroso et al. as a level of confidence that exists and satisfies a set of attributes [14].

Our framework divides the set of trust properties into three subsets; each subset is specified to constitute a base requirement for each degree, which the system should meet to be qualified as a trust system. As shown in Figure 2 (Source: compiled by the authors), from the lowest degree one to the highest degree two and three. The set of properties is defined for each degree. As we go to a higher degree, the set of properties of degree one is added to the set of properties of degree two, and so on for degree three.

Our framework is flexible and configurable; some preferred properties can be made mandatory as recommended by the stakeholders, manufacturer, or user. Trustworthiness as a system quality is a special goal that addresses the trust concerns of users. A trustworthiness goal is satisfied by trustworthiness requirements, which can be realized by more concrete trustworthiness properties. This framework will lead to the building of a generic model or map for developing trust in the CPS via property classification and highlighting the mandatory of those properties to satisfy the goal of each degree.

4.1 Degrees

4.1.1 Degree One: Secured CPS

It typically explains security issues, ways to enforce security in the system, and numerous flaws that exist.

- Degree 1A: Contains the mandatory and essential properties for secured CPS that are fixed by the organization or user.
- Degree 1B: In addition to mandatory properties, there are non-essential attributes that can characterize the CPS, and we named their preferred properties. If it is not available in CPS, it does not impact the desired level of quality.

4.1.2 Degree Two: Trustworthy CPS

Trustworthiness is a system quality that has the potential to impact end users. A trustworthy cyber-physical system is one with a sufficient level of security and safety, a collection of trustworthy properties, and a willingness to uphold the trust expectations of its users.

- Degree 2A: Contains the mandatory and essential properties for trustworthy CPS that are fixed by the organization or user.
- Degree 2B: Non-essential attributes can characterize the CPS, and we named it preferred properties for a trustworthy CPS. If it is not available in CPS, it does not impact the desired level of quality. Because our proposed framework is flexible and every stakeholder has their own trustworthy vision, some preferred properties may be mandatory for these stakeholders.

4.1.3 Degree Three: Trust CPS

Trusted CPS is when end users have positive faith in a system (the system is trusted by the user or organization). We defined trust CPS as a system that meets a set of requirements and obligated attributes and proprieties that assure the trust quality of CPS.

4.2 Method

Our method to set up a proposed framework for Trust CPS is based on: a) Requirements engineering (RE). b) Systematic analysis starts with identifying participants and gathering initial context information, then moves on to defining properties and dependencies and capturing obligations for properties at each degree.

The primary source for both steps is standard and published material and literature.

- Step1: Defining sources and extracting requirements.
- Step2: Understanding and analyzing requirements, and highlighting properties with consideration of security, trustworthiness, and trust goals.
- Step3: Filters a set of properties (secured, trustworthy, and trusted) with consideration of commodity and obligation.
- Step 4: In this step, we can start the evaluation phase.

4.3 Sources

Numerous cyber security standards have been developed to aid enterprises in better managing security risk, implement security measures that are compliant with legal and regulatory standards, and reap the benefits in terms of performance and cost [14].

Table 4. Some security and safety standards

Subject Area	Content	Ref
Security Metrics	Some theories, descriptions of security metrics, important global taxonomy classification.	[15]
Cyber Security Standards	Functional and assurance requirements for cyber security, technology environment	[16]
ISO 27001 Cyber S standards family	The interest in certification to ISO 2700. Compatibility of ISO 27001 of other MMS like ISO 9001and ISO 14001.	[17]
ISO 26262-1 Road Vehicle Functional safety Part 1: Vocabulary	A revision of edition of ISO 26262:2011 standards series of electrical and electronic (E/E) systems in road vehicles, safety lifecycle. Specific risk-based approach. Specified the requirement of ISO 26262.	[18]
ISO 26262-9 Road vehicle Functional safety Part 9: Automotive	Electrical and electronic (E/E) safety-related systems, production road vehicles. Some Hazards. A framework for E/E systems that are concerned with functional safety. determined the specifications for the Automotive Safety Integrity Level (ASIL)	[19]
IEC61508 Standard, functional safety for electrical, electronic	Described The IEC 61508 standard family. Potential hazard, IEC 61508 To describe the extent to which a system would fulfill its required safety functions, four safety integration levels (SIL) were established.	[20]
ICAO13 International Civil aviation Organization (ICAO)	Overview of safety management fundamentals and Annexes of ICAO safety management SARPs. A legal framework for controlling SMS from vendors of services. Analysis, defined criteria and properties for support safety risk management and safety assurance processes.	[21]

Standards are declarations of what must be accomplished in terms of results for security and safety in order to meet an organization's stated security and safety objectives. Even though the security and safety standards were formulated years ago, they are still applicable today because the formulation keeps pace with technological development, tools and techniques, and new goals to combat new and recent risks.

A security audit is a methodical way to evaluate security measures. During the audit, the auditor will try to locate the established policies, standards, and procedures before looking for proof that they are being followed. Some relevant standards for security and safety are presented in Table 4. Consistently reviewing and updating the security and safety standards is essential.

Policies, technologies, and threats are all subject to change, and for the standards to remain relevant, they must also adapt. If this isn't done, the standard will eventually be disregarded and deemed obsolete.

4.4 Set of requirements

For defining the trust concept, we based on an understanding and analyzing the requirements. For that reason, we divided the set of requirements into the essential parts that are related. The subset of secured requirements serves as the foundation for satisfying the essential needs for security and safety. The subset of trustworthy aspects automatically includes the needs defined in the previous subset and other added needs related to trustworthy aspects. The subset of CPS trusted requirements also includes a subset of trustworthy requirements and other needs related to trust aspects.

4.4.1 A subset of secured requirements

For the majority of fields, security requirements are based on security concerns, which are of three types:

- Confidentiality: Data and processes must be kept confidential in order to be protected from unauthorized disclosure.
- Integrity: Refers to the need for safeguards against unauthorized change of data and procedures.
- Availability: is the need that data be protected from denial of service to authorized users.

Safety and security are both required as a sufficient basis to build a trustworthy cyber-physical system. Safety is the avoidance of accidents and being protected against faults, errors, and failures (ISO 26262). Safety comprises and is related to many qualities of service and properties, the most important (Correctness, Resilience, Robustness, standard compliance. In different application domains, the safety properties may be different and adapted to their specific safety and certification requirements.

4.4.2 Subset of trustworthy requirements

The definition of trustworthiness includes both cyber security needs and system reliability criteria; the cyber-physical system delivers services that can justifiably be trusted. Traditional definitions of system dependability include requirements for operational availability, reliability, safety, and maintainability [22].

Aspects like confidentiality, integrity, availability, authenticity, and assurance of data transfers are among the cyber-security needs that authors [4] mentioned.

4.4.3 Subset of trust requirements

Concerns are about human interaction with and as part of a

CPS. It is based on a) human aspect: concern about the characteristics of CPS with respect to how they are used by humans. b) Usability: Concerns related to the ability of CPS to be used to achieve its functional objectives effectively, and to the satisfaction of users (adapted from ISO 9241-210). This degree determines whether or not the user trusts the system. Because previous degrees are directly related to system quality, it is necessary to satisfy and meet degrees one and two before proceeding to degree three, which is directly related to end user and judgment metrics.

4.5 Benefits of ranking trust in degrees

- Enhancing the quality of the system.
- Rating trust to different degrees eases the understanding of the requirements set and the needs of the final user before designing and implementing CPS.
- Enhance the CPS development and the user confidence toward producing trust system.
- Thus degree, are made as easy as possible to incorporate and integrate trustworthiness aspects into routine software engineering practice.
- Keep the time and cost, when take into consideration the necessity of developing secured, trustworthy, trusted CPS. The system's quality was evident from the start of the CPS life cycle.
- Meeting the set of trust requirements is a significant challenge. We can ensure the system and user requirements by focusing only on the obligation, which reduces development complexity and minimizes obstacles (if we only need secured CPS, we try to satisfy only the first degree requirement).

4.6 Arguments for rating trust according to degrees

4.6.1 Degree one (secured CPS)

- The International Society of Automation (ISA) mentioned the urgent need of designing safety and security for CPS, via standards ISA84 (IEC 61511) [23] and ISA99 (IEC 62443) [24]. Our proposed degree obligates security and safety for the early development phases of CPS; that builds the pillar for trust in CPS.
- Due to the CPS's complexity and integrity, the line between safety and security is becoming blurred, and researchers have proposed the need of collaboration between security and safety [25, 26].
- Safety and security are well merged together in this degree, providing a stable foundation for an impregnable CPS, whereas insufficient alignment may result in wasteful development and partially protected systems.
- Security and safety are the two key properties of a trust CPS. Careful, responsible, risk-guided engineering produces both safety and security [27].
- Security should be applied in CPS development [28].
- Trust is a key concept in the context of security [3].
- Still, there is a need for an approach or standard model that would support the development of secure CPS that adheres to industry standards for both safety and security [29].
- There is interdependability between safety and se- curity, and these dependencies should be considered during the CPS design phase. There are four types of interdependence: 1) conditional dependencies: Security is a prerequisite for safety, and vice versa; 2) reinforcement: safety and security countermeasures can help each other; 3) antagonism: they can undermine each other; and 4) independence: there is no relationship between safety and security [29].

Some surveyed paper for CPS security and safety are presented in Table 5.

4.6.2 Degree two (trustworthy CPS)

- Safety and security are two completely different concepts in a cyber-physical system. Both are necessary to a sufficient level to create a trustworthy CPS [30], Along with a number of attributes [4].
- Current certification and attestation processes need to be looked into to see if they could benefit from considering a wider variety of trustworthy attributes than only those related to security, as is typically the case today [1].

4.6.3 Degree three (trust CPS)

- The relationship between trust and trustworthiness notions is always influenced by the explicit or implicit reasoning processes carried out by system users while taking risk and potential repercussions into account [1].
- Trust can be defined as a degree of assurance or certainty that the other party won't engage in opportunistic behavior and will behave consistently with expectations [31].
- In the study [1], the authors came to the conclusion that software evaluation decisions made by a person or group of individuals affect software trustworthiness.
- Avizienis et al. [32] defined trustworthiness as "an assurance that the system will perform as expected".
- According to Amoroso et al., cyber-physical systems can earn users' trust if they enable confidence in meeting a specific set of needs or expectations.

Table 5. A sample of surveyed works for CPS security and safety

Ref	Subject Area	Content
[33]	Trust based security for CPS	Approach for achieving trust, consists external and internal layer of trust with respect to security for CPS
[34]	Security	IT security metrics, measuring security
[35]	Safety, Security	A survey of safety and security methods of ICS
[36]	Safety, Security	Analysis of dynamic software updating techniques, increasing the availability of IS
[37]	Safety, Risk Analysis	Assessing reliability of quantitative Risk Analysis (QRA), modeling errors and statistical errors
[38]	Safety, Security	Reviews of existing approaches of risk assessment and management, Integration

5. METRICS

There is no classification of trustworthy and trust attributes in the literature based on functionality and obligation. The CPS metrics that are divided by degrees are presented in Table 6. We propose a classification of properties based on system functionality and obligation (Table 7) and clearly define a set of judgment metrics (trust of the end user) as mentioned in Table 8.

This classification of CPS properties and quality of service eases the evaluation of metrics for each proposed trust degree and covers the most important metrics for CPS security and trustworthiness. The basics are the engineering requirements, user requirements, and organization requirements. The majority of properties' definitions are mentioned in the terminology glossary in the study [12].

Mandatory columns present the most important proprieties for each degree, such as security and safety [38] for degree one. Those columns are our proposed tool to facilitate the computation of trust in CPS and to define the threshold of computed values.

Table 6. CPS metrics

CPS degree	System metrics	Judgment metrics (trust of end users)
Secured	√	×
Trustworthy	√	×
Trusted	√	√

Table 7. System metrics

System properties	Mandatory
Availability	√
Integrity	√
Authenticity	√
Maintainability	×
Reliability	×
Safety	√
fault tolerance	√
Robustness	×
Performance	√
Timeliness	×
Configuration	×
Predictability	√
Reparability	×
Dependability	√
Security	√
Compliance	√
Auditability	√
Privacy	√
Confidentiality	√
Interoperability	×
Assurance	√

Table 8. Judgement metrics

Judgements properties	Mandatory
Usability	√
Satisfaction	√
Learnability	×
Effectiveness	√
Efficiency of Use	√
Flexible continuity	×
Level of Service	×
Accessibility	×
Correctness	√

Some mandatory properties depend on stakeholders' or users' precision and service quality and are not related to a standard or regulation, such as: Timeliness (ex: clinical chemistry analyzer Samsung LABGEO PT 10; 7 minutes is all the test it takes; in this case timeliness is mandatory and mentioned by the manufacturer). Other properties can be optional sometimes, such as configuration, predictability, reparability, and maintainability.

Some judgment metrics can be optional and not mandatory, such as accessibility, which may be customized for a special category and not allowed for everyone. Other properties, such as service level, flexibility, and learnability, are optional and are determined by the manufacturer or user.

The set of mandatory properties for trust CPS degrees is presented in Table 9. Configuration and compliance [39] are preferred properties of degree two (a trustworthy CPS).

Table 9. Set of mandatory properties for trust degrees

Degree	Proprieties	Sub-proprieties
Secured CPS	Safety [39] security [39]	fault tolerance, robustness availability, accountability, auditability, assurance, traceability, integrity, confidentiality, non-repudiation
Trustworthy CPS	Compatibility [39]	Openness
	Performance [39]	throughput, Response Time
	Dependability [39]	accuracy, availability, robustness, reliability, scalability, maintainability
	Privacy [39]	No unauthorized parties are able to access or utilize the personal data
Trusted CPS	Usability [ISO 9241-210] [39]	satisfaction, learnability, effectiveness, efficiency of use
	Correctness [39]	Determine if a system's behavior complies with the user's requirements

6. EVALUATION OF TRUST IN CPS

We look to improve the ability to control and secure CPS. We used an aspect inspired by the continuous modeling method that is often used in control via differential equations, which has been used to denote a variety of physical processes [47]. A set of discrete units and common variables, such as in the Modelica language [48], which conducts a theoretical study, stability, and security.

In our case, we use a simple equation when the combination of metrics has a shared variable for secured degree and secured metrics (X), a shared variable for trustworthy degree and trustworthy metrics (Y), and a shared variable for trust degree and trusted metrics (Z).

6.1 CPS trust equation

$$X = \sum_{i=0}^{n} Mi \qquad (1)$$

- M: Secured metrics (can be evaluated by value, or presented by percentage)
- n: Number of secured metrics
- L: Number of mandatory metrics (a set of safety and security attributes)
- L=2 (Mandatory metrics are safety and security)

$$Y = \sum_{k=0}^{m} Mk \qquad (2)$$

- M: Trustworthy metrics (can be evaluated by value or percentage)

- m: number of trustworthy metrics
- S: Number of mandatory metrics (a set of trustworthy)
- S=4 (Mandatory metrics are: privacy, dependability, performance, compatibility)

$$Z = \sum_{j=0}^{p} Mj \tag{3}$$

- M: Trustworthy metrics (can be evaluated by value or percentage)
- p: number of trusted metrics
- Q: Number of mandatory metrics (a set of trusted metrics)
- Q= 2 (Mandatory metrics are: Usability, Correctness)

$$T = \sum_{i=0}^{n} Mi + \sum_{k=0}^{m} Mk + \sum_{j=0}^{p} Mj \tag{4}$$

4.2 Determine the threshold values

There is no formal definition of trust, no mathematical formula. Calculating trust involves using statistics, or probabilities, notably in dynamic networks with rapidly changing topologies.

- X presents the secured metrics (a set of safety and security properties). L: number of mandatory metrics (set of safety and security attributes or metrics) When X = L, that means the mandatory metrics of Degree one (secured CPS) are verified. If X > L, the mandatory metrics are verified along with the expected or preferred metrics. In this case, the system is secure.
- At that point, the previous degree is considered verified, and the system has achieved degree 1 (the system is secure). Y presents the trustworthy metrics (a set of trustworthy metrics). S: Number of mandatory metrics (set of trustworthy metrics) If Y=S, that means the mandatory metrics of Degree2 are verified. If Y > S, it means that the mandatory metrics have been verified, as well as the expected or desired metrics. In this case, the system is trustworthy.
- At that point, we consider the previous degree verified and the system has achieved degree 2 (trustworthiness). Z presents the trusted metrics (a set of trusted metrics or judgment metrics). Q: Number of mandatory metrics (set of trusted metrics) If Z = Q, that means the mandatory metrics of degree 3 are verified. If Z > Q, it means that the mandatory metrics, as well as any expected or desired metrics, have been verified. In this case, the system is the trust system.
- On the assurance of security, trustworthiness, and trust qualities, we formulate a quantitative view. A number with a range of possible values; also known as a confidence interval. For that reason, we consider:

  a. To reduce uncertainty, each mandatory attribute will be evaluated as 1 if verified, and as 0 if not verified.
  b. No mandatory attribute, if verified, will get values in the range 0-1; it can get [0, 0.25, 0.50, 0.75, 1].
  c. If mandatory attributes of each degree are verified, we can consider a system trust CPS.
  d. The verification of sub-properties is considered part of its properties ‘verification. Only properties are taken into account.

4.3 Algorithm for calculating the trust in the CPS

An algorithm for calculating the trust in the CPS is presented below. For degrees two and three, we consider that the previous degree is verified.

Algorithm: Calculating trust of CPS

```
                Test Degree 1
require i=0, X=0, (k=0,Y=0),(j=0, Z=0), n= 2, L=2
for i=0,n
lire Mi
if Mi<>0 then X=X+Mi
return X    ,  if X>=L then end
return  ,“Degree1 & System is secured”
else return “System is not secured”
                Test Degree 2
require k=0,Y=0,( j=0, Z=0),m=7,S=4
for k=0,m lire Mk
if Mk>=0 then Y=Y+Mk
return Y ,    if y>=S then
return “Degree2 & System is trustworthy”
else return “System is not trustworthy”
                Test Degree 3
require j=0, Z=0, p=2,Q=2
for j=0,p lire Mj
if Mj<>0 then Z=Z+Mj
return Z   , if Z>=Q
return  “Degree3 & System is trust”
else return “System is not trust ,is trustworthy”
```

6.4 Use case

We used the Samsung smart blood analyzer LABGEO PT10 to evaluate our proposed trust degree and trust compu- tation. The latter was connected to a local PC for efficient database management and automatic software updates. The LABGEO PT10 clinical chemistry analyzer uses dry film chemistry to eliminate liquid waste. Rapid test results (7 minutes) Up to 14 analytes simultaneously using 70 L whole blood Analytical performance is comparable to the central lab mainframe [49]. The operation of LABGEO PT10 [50] is presented in Figure 3.

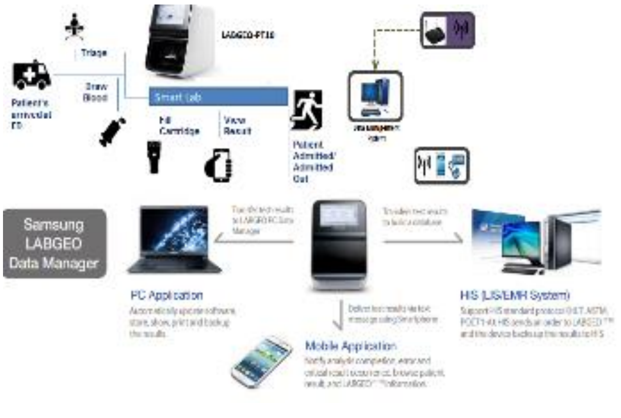

Figure 3. The operation of the Samsung smart blood analyzer LABGEO PT10

6.4.1 Metrics evaluations

a. System features

- Accuracy 95 percent: is a sub- property of dependability, is mandatory.
- Timelines = 7 minutes (response time is a sub-

property of Performance, is mandatory).

- Simple and easy, fast: efficiency of use is a sub-property of usability.

b. Secured metrics

Safety (M1) and security (M2) are positively validated. Hardware is Samsung devices (PC, smart phone, and smart medical device) are accredited and standardized. Samsung also certifies software and networks [51].

c. Trustworthy metrics

Samsung consists product quality, and at the right time to ensure customer satisfaction. Privacy (M3), dependability (M4), performance (M5), and compatibility (M6) are verified positively [44].

d. Judgments metrics

- Clinicians: Usability (M7) is the set of sub-properties (satisfaction, learnability, effectiveness, and efficiency of use). And the Correctness (M8) are verified, reference to the study (NCT02104154) [52].
- Patients: Usability (M7) is the set of sub- properties (satisfaction, effectiveness, and efficiency of use). and correctness (M8) are verified positively, with reference to the study (NCT02104154) [52].

6.4.2 Trust computation

We followed the proposed process for computing the trust of CPS, and the results are presented in Table 10.

Table 10. Trust computation

S.C.A	Components	D1	D2	D3	T	Result
		M1, M2	M3, M4 M5, M6	M7, M8		
Hard	LABGEO PT10 PC Smart phone	1+1	1+1+ 1+1	1+1	8	Trust Hard
Soft	RMS Data management System	1+1	1+1+ 1+1	1+1	8	Trust Soft
Net	VPN Router, Central Server	1+1	1+1+ 1+1	1+1	8	Trust Net

5. DISCUSSION

We noted that the use of the proposed trust degree framework for the evaluation of the Samsung smart blood analyzer LABGEO gave the expected results from the method of ranking the trust into degrees. The proposed calculation method was also simple and targeted the necessary properties of the system to qualify it as a trusted CPS such as security [40, 41] and performance [42]. The interest in the necessary and mandatory properties only for the system gave the calculation process a methodology and purpose. The expression of a quantitative view on the guarantee of security, trustworthiness, and trust attributes via number in a confidence interval reduced the uncertainty.

The three proposed trust degrees (secured, trustworthy, and trusted) have the advantage of qualifying the CPS components (hardware, software, and network) separately, as shown in Table 10.

For more evidence, we compared some existing frameworks [2, 43-46] for the evaluation of trust in CPS with our trust degree framework. We reveal some key insights:

- Most papers have treated trust as an important concept that should exist in CPS, including components and communication interfaces [46], or be globulated into security, as in the study [44].
- Trust is not treated as a system quality that should occur in CPS, and during within development process, from conception to design and implementation, they do not take into consideration the system and engineering requirements and relevant properties of CPS. Contrary in the study [2], they treated a trust as a set of properties and mentioned the requirements.
- The concept of trust has been treated as a security aspect of CPS and protection from attacks, such as malicious software [46], internet attacks [43], and eavesdropping attacks [44]. They did not consider the rest of the CPS properties, such as safety, correctness, integrity, etc.
- There is not an objective to evaluate the trust of CPS with a quantitative method.
- As application domains, the study [2] is applied for general CPS, the study [43] is applied for network, and the study [44] is applied for power grid systems. The study [45] is applied to social sciences, information systems, and distributed ad-hoc networks. The study [46] is applied for CPSs in general.
- As a limit, the study [2] is used for certified products only, and the computation process is so long. Also, the set of metrics is very limited and not classified. In the study [43], there is a lack of definition for the evaluation process. In the study [44, 46], the main objective is the security of CPS, not its trustworthiness. Also, there is a lack of trustworthiness metrics.

Advantages of our trust degree framework

- Our framework is very flexible and advantageous; it allows to compute the trust of CPS components separately, which may target hardware, software, or a network.
- Several decisions were also made in the formula composition, and we can confirm the degree of trust if it is the first degree, which targets the overall safety and security of the system or its components, or the second degree, which targets the amount of trustworthiness of the systems.
- The final degree of trust mentioned is that the system is completely trusted and has met all degrees of confidence.
- Ease and simplify the computation of trust in a quantitative manner.
- Facilitate the development of trust in the CPS from the early phases.

- Configurable, there is the option to add or remove mandatory properties based on stakeholder, user, or organizational needs.
- Applied for all CPS domains.
- Independent and not linked to the tools of propriety measurement.

As a recommendation for this proposed trust degree framework:

- The process must be integrated within industry, and most system attributes should be collected at runtime.
- The process needs to be followed for auditing and certification.

6. CONCLUSION

In this paper, we proposed a flexible framework for evaluating trust in cyber-physical systems (CPSs) based on ranking trust by degrees. We defined three trust degrees: degree one (secured CPS), degree two (trustworthy CPS), and degree three (trusted CPS). A set of trust requirements and properties are defined and divided into subsets related to each degree. We proposed a classification of properties based on system functionality, judgments, and obligations. A simple mathematical formula for computing the trust of CPS in a quantitative manner is proposed.

The most important challenges are how to achieve trust- by-design in CPS and how to develop trust in CPS from abstraction to architecture and from concept to implementation. Still, there is a need for an approach or standard model to assist in the design of safe, secure, and trustworthy CPS that are compliant with industrial CPS standards.

Our future work will cover this area and address these challenges, focusing on the integration of trust requirements in the life cycle development of CPS, which will led to the construction of trustworthiness metrics and patterns as well as reduce the effort required of process designers by creating a collection of patterns for easing the specification of trust measures.

REFERENCES

[1] Mohammadi, N.G., Paulus, G., Bishr, M., Metzger, A., Könnecke, H., Hartenstein, S., Weyer, T., Pohl, K. (2013). Trustworthiness attributes and metrics for engineering trusted internet-based software systems. In: Helfert, M., Desprez, F., Ferguson, D., Leymann, F. (eds) Cloud Computing and Services Science. CLOSER 2013. Communications in Computer and Information Science, vol 453. Springer, Cham. https://doi.org/10.1007/978-3-319-11561-0_2

[2] Nazila, G.M. (2019). Trustworthy Cyber-Physical Systems: A Systematic Framework towards Design and Evaluation of Trust and Trustworthiness. Springer Vieweg. https://doi.org/10.1007/978-3-658-27488-7

[3] Anwar, R.W., Ali, S. (2012). Trust based secure cyber physical systems. In Proc. of Workshop Proceedings: Trustworthy Cyber-Physical Systems, Tech Report Series.

[4] Babiceanu, R.F., Seker, R. (2017). Trustworthiness requirements for manufacturing cyber-physical systems. Procedia Manufacturing, 11: 973-981. https://doi.org/10.1016/j.promfg.2017.07.202

[5] Zhu, Q., Rieger, C., Başar, T. (2011). A hierarchical security architecture for cyber-physical systems. In 2011 4th International Symposium on Resilient Control Systems, Boise, ID, USA, pp. 15-20. https://doi.org/10.1109/ISRCS.2011.6016081

[6] Keele, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical Report, ver. 2.3 EBSE technical report. EBSE, Tech. Rep.

[7] Pohl, K. (2016). Requirements Engineering Fundamentals: A Study Guide for the Certified Professional for Requirements Engineering Exam-Foundation Level-IREB Compliant. Rocky Nook, Inc.

[8] Lee, E.A. (2006). Cyber-physical systems-are computing foundations adequate. In Position Paper for NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, pp. 1-9.

[9] Lee, E.A. (2008). Cyber physical systems: Design challenges. In 2008 11th IEEE Inter-national Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), Orlando, FL, USA, pp. 363-369. https://doi.org/10.1109/ISORC.2008.25

[10] Aguida, M.A., Ouchani, S., Benmalek, M. (2020). A review on cyber-physical systems: models and architectures. In 2020 IEEE 29th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Bayonne, France, pp. 275-278. https://doi.org/10.1109/WETICE49692.2020.00060

[11] Oudina, Z., Derdour, M., Bouhamed, M.M. (2022). Testing cyber-physical production system: Test methods categorization and dataset. In 2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS), Oum El Bouaghi, Algeria, pp. 1-8. https://doi.org/10.1109/PAIS56586.2022.9946868

[12] Glinz, M. (2011). A glossary of requirements engineering terminology. Standard Glossary of the Certified Professional for Requirements Engineering (CPRE) Studies and Exam, Version, 1: 56.

[13] Pressman, R.S. (2010). Interface Design. Software Engineering A Practitioner's Approach 7th, McGraw-Hill Education.

[14] Amoroso, E.G. (1994). Fundamentals of Computer Security Technology. Prentice-Hall, Inc.

[15] Jaquith, A. (2007). Security Metrics: Replacing Fear, Uncertainty, and Doubt. Pearson Education.

[16] Radack, S.M. (2010). Security Content Automation Protocol (SCAP): Helping organizations maintain and verify the security of their information systems.

[17] Governance, U.K.I.T. (2020). Information Security and ISO 27001–An Introduction UK IT Governance, Ely, UK: Green Paper.

[18] Morikawa, A., Matsubara, Y. (2020). Safety design concepts for statistical machine learning components toward accordance with functional safety standards. arXiv preprint arXiv:2008.01263. https://doi.org/10.48550/arXiv.2008.01263

[19] Gowda, J.N. (2019). ECU Inter-processor data communication end to end verification in autosar for achieving functional safety goals. INCOSE International Symposium, 29: 443-453. https://doi.org/10.1002/j.2334-5837.2019.00698.x

[20] Redmill, F., Consultancy, R. (1999). An introduction to the safety standard IEC 61508. Hazard Prevention, 35(1): 20-25.

[21] Schenkman, J. (1955). International civil aviation organization (No. BOOK). [sn].

[22] Rupp, C. (2007). Requirements-Engineering und-Management: professionelle, iterative Anforderungsanalyse für die Praxis. Hanser Verlag.

[23] I. S. of Automation, “Standards,” https://www.isa.org/intech-home/2018/july-august/departments/isa84-approves-iec-61511-moves-ahead-on-key-suppor, accessed on 1 Feb. 2022.

[24] Martins, A.G.D.S. (2020). Visualization of security in industrial control systems respecting IEC-62443. Doctoral dissertation.

[25] Stoneburner, G. (2006). Toward a unified security-safety model. Computer, 39(8): 96-97. https://doi.org/10.1109/MC.2006.283

[26] Piètre-Cambacédès, L., Bouissou, M. (2013). Cross-fertilization between safety and security engineering. Reliability Engineering & System Safety, 110: 110-126. https://doi.org/10.1016/j.ress.2012.09.011

[27] Furrer, F.J. (2022). Cyber-Physical Systems. In Safety and Security of Cyber-Physical Systems: Engineering dependable Software using Principle-based Development, pp. 9-76. Wiesbaden: Springer Fachmedien Wiesbaden.

[28] Fletcher, K.K., Liu, X. (2011). Security requirements analysis, specification, prioritization and policy development in cyber-physical systems. In 2011 Fifth International Conference on Secure Software Integration and Reliability Improvement-Companion, Jeju, Korea (South), pp. 106-113. https://doi.org/10.1109/SSIRI-C.2011.25

[29] Piètre-Cambacédès, L., Bouissou, M. (2010). Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). In 2010 IEEE International Conference on Systems, Man and Cybernetics, Istanbul, Turkey, pp. 2852-2861. https://doi.org/10.1109/ICSMC.2010.5641922

[30] Hollnagel, E. (2018). Safety-I and Safety-II: The Past and Future of Safety Management. CRC Press.

[31] Williamson, O.E. (1993). Calculativeness, trust, and economic organization. The Journal of Law and Economics, 36(1, Part 2): 453-486. https://doi.org/10.1086/467284

[32] Avizienis, A., Laprie, J.C., Randell, B., Landwehr, C. (2007). Basic Concepts and Taxonomy of Dependable Secure Computing. In A Process for Developing a Common Vocabulary in the Information Security Area, pp. 10-51. IOS Press.

[33] Sabaliauskaite, G., Mathur, A.P. (2015). Aligning cyber-physical system safety and security. In: Cardin, MA., Krob, D., Lui, P., Tan, Y., Wood, K. (eds) Complex Systems Design & Management Asia. Springer, Cham. https://doi.org/10.1007/978-3-319-12544-2_4

[34] Hayden, L. (2010). IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data. McGraw-Hill Education Group.

[35] Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. Reliability Engineering & System Safety, 139: 156-178. https://doi.org/10.1016/j.ress.2015.02.008

[36] Mugarza, I., Parra, J., Jacob, E. (2018). Analysis of existing dynamic software updating techniques for safe and secure industrial control systems. International Journal of Safety and Security Engineering, 8(1): 121-131. https://doi.org/10.2495/SAFE-V8-N1-121-131

[37] Rossi, G., Lombardi, M., Di Mascio, P. (2018). Consistency and stability of risk indicators: The case of road infrastructures. International Journal of Safety and Security Engineering, 8(1): 39-47. https://doi.org/10.2495/SAFE-V8-N1-39-47

[38] Lyu, X., Ding, Y., Yang, S.H. (2019). Safety and security risk assessment in cyber-physical systems. IET Cyber-Physical Systems: Theory & Applications, 4(3): 221-232. https://doi.org/10.1049/iet-cps.2018.5068

[39] Mohammadi, N.G., Paulus, S., Bishr, M., Metzger, A., Koennecke, H., Hartenstein, S., Pohl, K. (2013). An analysis of software quality attributes and their contribution to trustworthiness. In CLOSER, pp. 542-552. https://doi.org/10.5220/0004502705420552

[40] Kalloniatis, C., Kavakli, E., Gritzalis, S. (2008). Addressing privacy requirements in system design: The PriS method. Requirements Engineering, 13: 241-255. https://doi.org/10.1007/s00766-008-0067-3

[41] Zalewski, J., Drager, S., McKeever, W., Kornecki, A.J. (2013). Threat modeling for security assessment in cyberphysical systems. In Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, pp. 1-4. https://doi.org/10.1145/2459976.2459987

[42] Mei, H., Huang, G., Xie, T. (2012). Internetware: A software paradigm for internet computing. Computer, 45(6): 26-31. https://doi.org/10.1109/MC.2012.189

[43] Duma, C., Karresand, M., Shahmehri, N., Caronni, G. (2006). A trust-aware, p2p-based overlay for intrusion detection. In 17th International Workshop on Database and Expert Systems Applications (DEXA'06), Krakow, Poland, pp. 692-697. https://doi.org/10.1109/DEXA.2006.21

[44] Jiang, Y., Wu, S., Yang, H., Luo, H., Chen, Z., Yin, S., Kaynak, O. (2022). Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(12): 7799-7809. https://doi.org/10.1109/TSMC.2022.3164024

[45] Harlamova, M., Kirikova, M. (2018). Trust handling framework for networks in cyber physical systems of Industry 4.0. In: Zdravkovic, J., Grabis, J., Nurcan, S., Stirna, J. (eds) Perspectives in Business Informatics Research. BIR 2018. Lecture Notes in Business Information Processing, vol 330. Springer, Cham. https://doi.org/10.1007/978-3-319-99951-7_3

[46] Spensky, C., Machiry, A., Busch, M., Leach, K., Housley, R., Kruegel, C., Vigna, G. (2020). TRUST. IO: protecting physical interfaces on cyber-physical systems. In 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, pp. 1-9. https://doi.org/10.1109/CNS48642.2020.9162246

[47] Baker, C.T., Paul, C.A., Willé, D.R. (1995). Issues in the numerical solution of evolutionary delay differential equations. Advances in Computational Mathematics, 3: 171-196. https://doi.org/10.1007/BF02988625

[48] Fritzson, P. (2014). Principles of Object-Oriented Modeling and Simulation with Modelica 3.3: A Cyber-Physical Approach. John Wiley & Sons.

[49] Jeong, T.D., Lee, W., Chun, S., Min, W.K. (2013). Performance evaluation of the LABGEO PT10 point-of-

care chemistry analyzer. Journal of Laboratory Medicine and Quality Assurance, 35(2): 70-80.

[50] Samsung. labgeo.pt10e nc atalog, https//www.mediline.si/media/labgeo.pt10e nc atalog.pdf, accessed on 20 Feb.2015.

[51] Ensuring excellent quality control. https://semiconductor.samsung.com/support/quality-support/quality- management/, accessed on 12 Feb. 2022.

[52] Site: https://clinicaltrials.gov/ct2/show/NCT02104154, accessed on 1 Feb. 2001.