Dmitro KHLAPONIN[1]

Scientific Supervisor: Petro VORONA[1]

STATE REGULATION OF CYBER-PHYSICAL SYSTEMS IN THE LEADING COUNTRIES OF THE WORLD

Summary: The article deals with the analysis of the peculiarities of the normative-legal regulation of the cyber-physical systems (CPS) functioning in the leading countries of the world, the analysis of the results of scientific research in the field of ensuring safe, reliable, resilient operation of CPS, taking into account the requirements of confidentiality. Two iterations of integration and analysis produced the following Framework elements: Domains (such as Energy, Healthcare, Infrastructure, Manufacturing, Transport etc.). Aspects (such as Functional, Business, Human, Timing, Boundaries, Composability, Lifecycle), Facets (such as conceptualization facet, realization facet and assurance facet). An important unsolved problem is the large scope of incompatible global CPS standards which should be unified to be applicable to heterogeneus CPS. Also an attention is paid to CPS certification which will confirm the requirements for reliability, security, resilience, confidentiality of CPS.

Keywords: cyberspace, cyberphysical system, CPS certification, CPS standards, internet of things

REGULACJA PAŃSTWOWA SYSTEMÓW CYBER-FIZYCZNYCH W WIODĄCYCH KRAJACH ŚWIATA

Streszczenie: Artykuł dotyczy analizy specyfiki regulacji normatywno-prawnej systemów cyber-fizycznych (CPS) funkcjonujących w wiodących krajach świata, analizy wyników badań naukowych w zakresie zapewnienia bezpieczeństwa, niezawodności oraz odpornego działania CPS, z uwzględnieniem wymogów poufności. Dwie iteracje integracji i analizy dały następujące elementy ramowe: /1/ domeny (takie jak energia, opieka zdrowotna, infrastruktura, produkcja, transport itp.), /2/ aspekty (takie jak funkcjonalność, biznes, człowiek, czas, dane, granice, cykl życia) oraz /3/ aspekty (takie jak aspekt konceptualizacji, aspekt realizacji i aspekt zapewnienia). Ważnym nierozwiązanym problemem jest szeroki zakres niekompatybilnych globalnych standardów CPS, które należy zunifikować, aby można je było zastosować do heterogenicznych CPS. Zwrócono również uwagę na certyfikację CPS, która potwierdzi wymagania dotyczące niezawodności, bezpieczeństwa, odporności oraz poufności CPS.

Słowa kluczowe: cyberprzestrzeń, system cyberfizyczny, certyfikacja CPS, standardy CPS, internet rzeczy.

[1] Institute of personnel training of the State employment Service of Ukraine, Kyiv, Ukraine, kmld.85@gmal.com

1. Introduction

Due to the rapid development of information technologies, the expansion of the provision of services in cyberspace and the expansion of the use of cyber-physical systems, there is a need to develop a unified common definition of cyber-physical systems, their main features, the need for legal regulation of the procedure for the creation and functioning of CPS in Ukraine, taking into account the experience of the leading countries of the world.

2. Analysis of recent research and publications

The issues of the creation and safe, reliable, resilient CPS functioning, taking into account the requirements of confidentiality, were explored by scientists from the USA, Germany, the United Kingdom and other countries as well as by such scientific institutions as German Academy of Science and Engineering and National Institute of Standards and Technology, US Department of Commerce.

3. Problem definition

One of the unsolved problems is the existence of numerous international CPS standards which are incompatible and are not completely applicable to heterogeneous CPS. Another issue is the need for certification to confirm the requirements of safety, security, reliability, resilience and confidentiality of CPS functioning.
The purpose of the article. To analyze the peculiarities of the normative-legal regulation of CPS functioning in the leading countries of the world, the results of scientific research in the field of ensuring safe, reliable, resilient CPS functioning, taking into account the requirements of confidentiality.

4. Statement of the main material

According to German Agenda Cyber physical systems Outlines of a new research domain Intermediary results 7th December 2010 a vertical integration of embedded systems with commercial application software opens up the door to completely new business models and has significant potential for optimization, in areas such as logistics, discrete production of goods or in process industries [1,3].
Many sectors in Europe are currently seeking out solutions that will allow them to thrive in global competition while maintaining production in a high-wage region. The most important objective is frequently even greater automation and monitoring, in order to control the business and entire value added networks in near to real time. CPS are finding broad scope for deployment here.
The as yet untapped potential of CPS will pose new technological, methodological, legal, economic and social challenges [1,4]:

1. Economic challenges, such as overcoming traditional system limitations (moving from a device to a business process) and the creation of new associated ownership

and business models. Within a large-scale CPS, services can no longer be developed and operated by a single provider, but can only function in an integrative fashion within the system infrastructure, adapted to existing technologies, services and solutions. For instance, CPS enable the creation of new, web-based services, identified as the "Internet of services", which is closely related to the "Internet of things". In [1] is emphasized that differentiated economic eco-systems will develop, in which companies occupy different roles and interact on the basis of complementary business models [1,24]. CPS offer a great opportunity to act as stimulators and receptors for new, emerging forms of business that provide individualized services – for example linking traditional services with partial or complete automation.

2. Legal challenges, such as cross-system processes and the associated security and safety issues (which can no longer be addressed locally, as it is done in current certification processes) and the resulting liability issues.
3. Methodological challenges, due to different lifecycles of the systems and requirements for clear interfaces and configuration options. The technical development of products (solutions and services) will increasingly demand a methodology that not only integrates the new application opportunities but that is also specifically oriented towards the requirements of the processes that are to be optimized (e.g. the optimization of the logistics chains, energy management, mobility concepts).
4. Social challenges, such as the growing acceptance of increasing opportunities for being supported by IT services in various processes, but also the way in which we perceive our environment and how we react to it.
5. Technological challenges such as CPS are not constructed for one specific purpose or function, but rather are open for many different services and processes, and must therefore be adaptable.

In view of their high degree of interconnection, in particular, the safety and security-related requirements of CPS represent one of the key research topics. [1,20]. "Safety and security" refers equally to the requirement that [1,20]:

- Usage and operation of the systems should not generate risks ("functional safety").
- The system should be protected against attack and unauthorized usage by external sources ("access security").
- Ensuring safety and security through verification, testing and certification.
- Implementing measures to detect and suppress attacks, risks, malfunctions (error tolerance through redundancy, fail-safe systems, self-stabilization).

As CPS directly affect physical processes, an incorrect response can have devastating effects on humans and technology, as well as it can cause significant economic losses. In many domains, such as in avionics and medical care, there are explicit approval and certification procedures that comprise documentation of an appropriate level of safety and security.

According to [1,21] a further challenge is found in the integration of new technologies, such as new hardware architectures and new communication protocols, into existing **certification processes**.

The integration of CPS into global networks makes them vulnerable to potential attacks by cyber criminals, ranging from unauthorised usage of private data, through data theft (e.g. industrial espionage) to affecting the response of CPS by manipulating

or forging data. This therefore also has an effect on safety. A key research challenge here is the creation of protocols to reliably establish the authenticity of a communication partner and the security of data transfer [1,21].

The term ***cyber-physical systems*** (CPS) is used to describe software-intensive embedded systems that are connected to services available around the world through global networks such as the Internet, and their diverse potential for development and utilization [1,5].

According to the Framework [2] National Institute of Standards and Technology (USA) in mid-2014 established Cyber Physical Systems Public Working Group (CPS PWG) to bring together a broad range of CPS experts in an open public forum to help define and shape key characteristics of CPS, so as to better manage development and implementation within multiple "smart" application domains, including smart manufacturing, transportation, energy, and healthcare. ***Cyber-physical systems (CPS)*** are smart systems that include engineered interacting networks of physical and computational components [2,13].

Two iterations of integration and analysis produced the following **Framework elements** [2,14]:

Domains. It is intended that the Framework can be applied to concrete CPS application domains, such as Advertising, Avionics, Buildings, Defence, Emergency response, Energy, Healthcare, Infrastructure, Manufacturing, Transport etc.

Aspects. Aspects are high-level groupings of cross-cutting concerns. Concerns are interests in a system relevant to one or more stakeholders. The identified aspects are listed below: Functional, Business, Human, Trustworthiness, Timing, Data, Boundaries, Composability, Lifecycle. Trustworthiness includes security, privacy, safety, reliability, and resilience.

Functional aspect includes concerns related to the ability of the CPS to effect change in the physical world; concerns related to the exchange of information internal to the CPS and between the CPS and other entities; ability of a CPS to control a property of a physical thing; concerns related to the management of CPS function.

Business aspect includes concerns related to the direct and indirect investment or monetary flow or other resources required by the CPS; concerns related to the impacts of treaties, statutes, and doctrines on a CPS, concerns related to the ability of a CPS to provide benefit or satisfaction through its operation.

Human aspect includes concerns related to the ability of CPS to be used to achieve its functional objectives effectively and to the satisfaction of users.

Aspect of trustworthiness includes the following concerns:

Privacy related to the ability of the CPS to prevent entities (people, machines) from gaining access to data stored in, created by, or transiting a CPS or its components,

Reliability related to the ability of the CPS to deliver stable and predictable performance in expected conditions.

Resilience related to the ability of the CPS to withstand instability, unexpected conditions and gracefully return to predictable performance.

Safety related to the ability of the CPS to ensure the absence of catastrophic consequences on the life, health, property, or data of CPS stakeholders and the physical environment.

Security related to the ability of the CPS to ensure that all of its processes, mechanisms, both physical and cyber, and services are afforded internal or external

protection from unintended and unauthorized access, change, damage, destruction, or use.
Integrity: guarding against improper modification or destruction of system, and includes ensuring non-repudiation and authenticity.
Availability: ensuring timely and reliable access to and use of a system.
Timing aspect includes the following concerns:

Logical time related to the order in which things happen (causal order relation) or event driven.

Synchronization, which means that all associated nodes have timing signals traceable to the same time scale with accuracies as required. There are three kinds of synchronization that might be required: time, phase, and frequency synchronization.

Time awareness includes concerns that allow time correctness by design.

Time-interval and latency generally involves requirements for time-intervals between pairs of events.

Data aspect includes the following concerns:

Data semantics related to the agreed and shared meaning(s) of data held within, generated by, and transiting a system.

Identity related to the ability to accurately recognize entities (people, machines, and data) when interacting with or being leveraged by a CPS.

Operations on data related to the ability to create/read/update/delete system data and how the integrity of CPS data and behaviors may be affected.

Data velocity related to the speed with which data operations are executed.

Data volume related to the volume or quantity of data associated with a CPS operation.

Aspect of Boundaries includes behavioral concern related to the ability to successfully operate a CPS in multiple application areas and responsibility related to the ability to identify the entity authorized to control the operation of a CPS.
Composition aspect includes the following concerns:

Adaptability related to the ability of the CPS to achieve an intended purpose in the face of changing external conditions such as the need to upgrade or otherwise reconfigure a CPS to meet new conditions, needs, or objectives.

Complexity related to our understanding of the behavior of CPS due to the richness and heterogeneity of interactions among its components, such as existence of legacy components and the variety of interfaces.

Lifecycle aspect includes the ease and reliability with which a CPS can be brought into productive use, the ease and reliability with which a CPS can be kept in working order.
Facets. Facets are views on CPS encompassing identified responsibilities in the system engineering process. They contain well-defined activities and artifacts (outputs) for addressing concerns. There are three identified facets:
The conceptualization facet captures activities related to the high-level goals, functional requirements, and organization of CPS as they pertain to what a CPS or its components should be and what they are supposed to do. It provides as its overarching output a conceptual model of the CPS.
The realization facet captures the activities surrounding the detailed engineering design, production, implementation, and operation of the desired systems.

The assurance facet deals with obtaining confidence that the CPS built in the realization facet satisfies the model developed in the conceptualization facet. Its activities include evaluating the claims, argumentation, and evidence as required to address important (and sometimes mandatory) requirements of design, policy, law, and regulation.

The CPS is said to *satisfy* the CPS Model if it satisfies or has each of the CPS Model properties. In the transportation domain, with ISO 26262 [23] examples, the high-level statement or judgement is that the CPS meets the requirements of the functional safety standard or that the processes of the organization that developed the CPS are ISO 26262 compliant.

Cyber-physical systems (CPS) are smart systems that include engineered interacting networks of physical and computational components. [2,1].

In addition to CPS, there are many words and phrases (Industrial Internet, Internet of Things (IoT), machine-to-machine (M2M), smart cities, and others) that describe similar or related systems and concepts. There is significant overlap between these concepts, in particular CPS and IoT, such that CPS and IoT are sometimes used interchangeably; therefore, the approach described in this CPS Framework should be considered to be equally applicable to IoT.

This document defines a CPS as follows: Cyber-physical systems integrate computation, communication, sensing, and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment, including human interaction. [2,5]**.**

According to **The UK Cyber Security Strategy 2011** [3] it contains the notions "cyberspace", "cyber security products", "cyber security industry" but it doesn't contain the notion "cyber-physical systems".

Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. "It includes the internet, but also the other information systems that support our businesses, infrastructure and services". [3,10].

It is emphasized in the abovementioned Strategy that "digital networks already underpin the supply of electricity and water to our homes, help organise the delivery of food and other goods to shops, and act as an essential tool for businesses across the UK" [3,10].

A conclusion can be made that the abovementioned digital networks are in some way similar to cyber-physical systems.

According to the abovementioned strategy, the following actions are aimed at ensuring safer business conduct in cyberspace:

1. Working with domestic, European, global commercial standards organisations to stimulate the development of industry-led standards and guidance that help customers to navigate the market and differentiate cyber security products.
2. Encourage industry-led standards and guidance that are understood and readily used by companies in their commercial activities.

Thus, it can be seen from this that the abovementioned Strategy focuses on the need for cooperation with relevant standards organizations to stimulate the development of sectoral standards and guidance on CPS and introduces a specific concept of cybersecurity products that are not clearly defined in the Strategy.

On the development of the UK Cyber Security Strategy 2011 Guidance "The key principles of vehicle cyber security for connected and automated vehicles" was published dated August 6, 2017 [4,17].

According to the Principle 4.1 of the abovementioned Guidance organisations, including suppliers and 3rd parties, must be able to provide assurance, such as independent validation or certification, of their security processes and products (physical, personnel and cyber).
According to the Principle 4.1 of the abovementioned Guidance organisations jointly plan for how systems will safely and securely interact with external devices, connections (including the ecosystem), services (including maintenance), operations or control centres. This may include agreeing standards and data requirements.
In Ukraine, the Decree of the President of Ukraine dated March 15, 2016 "On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 "On the Strategy of Cybersecurity of Ukraine" was issued. [5,7] Also on 05.10.2017 the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" was adopted, which will come into force on 05.09.2018. [6,3] The law contains the concept of cybersecurity, cyber attack, cyberspace, critical infrastructure objects, and others. Also, in the definition of "cyberattack", the Law refers to the concepts of communication and/or technological systems. It should be noted that the concept of "cyber security" contained in the Law is an integral part of cyber-physical systems as a condition of safe, reliable and resilient functioning, taking into account the requirements of confidentiality. Instead, the Cybersecurity Strategy and the Law do not contain the concept of cyber-physical systems, although they are increasingly used in the world in industry, energy, healthcare, transport, and there is a need for a clear formulation of the concept of cyber-physical systems and their main universal features and proper normative-legal regulation of the CPS functioning. Proceeding from this, the author suggests to introduce in the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" the concept "cyber-physical system" with such definition: **Cyber-physical system (CPS) is a smart system that includes engineered interacting networks of physical and computational components**.

5. Conclusions

As a result of the research, legislation and the results of the scientific research on cyber-physical systems of such countries as The United Kingdom, Germany, The USA and European Union were analysed.
As today in the world, all processes in the economy, industry, and infrastructure are becoming increasingly connected, cyber-physical systems are becoming more widely used as smart networked engineered interacting systems that combine physical and computational components [7, 3].
The integral part of cyber-physical systems functioning is cyber security, which ensures reliable, secure, resilient conditions of CPS functioning.
As a result of this research it can be concluded that in the German framework document on CPS as well as in the framework document of the USA the attention is paid to the need for CPS certification which will confirm the requirements for reliability, security, resilience, confidentiality of CPS.
The necessity for certification is also emphasized in Cyber-Physical European Roadmap & Strategy Research Agenda and Recommendations for Action 01.07.2013 according to which current methods and instruments for certification are not

completely applicable to CPS certification today because of their discrepancy to the requirements of modern CPS depending on the environment.
Another issue which is underlined in the German framework document on CPS and in the relevant US framework document is the adoption and application of the unified CPS standards.
In order to provide a universal definition of CPS, it is necessary to analyze the aspects of the creation of CPS. It was done thoroughly in the US Framework for Cyber-Physical Systems May 2016 Cyber Physical Systems Public Working Group.
Of particular importance is the research of various scientists and scientific institutions in the issue of trustworthiness of CPS, which includes privacy, reliability, resilience, safety and security.
There are periodic workshops at the EU level with the participation of scientists, experts, representatives of government, business, which result in important developments and practical conclusions in the field of CPS.
Nowadays numerous efforts have been made by various international organizations in the field of the establishment of standards for cyber-physical systems, in particular ISO, ITU, Industrial Internet Consortium, IoT-A and others, but the full compatibility of these standards with respect to heterogeneous CPSs is still not ensured.

REFERENCES

1. German Agenda Cyber physical systems Outlines of a new research domain Intermediary results 7th December 2010, www.acatech.de
2. Framework for Cyber-Physical Systems Release 1.0 May 2016 Cyber Physical Systems Public Working Group, www.nist.gov
3. The UK Cyber Security Strategy 2011, www.cabinetoffice.gov.uk
4. Guidance “The key principles of vehicle cyber security for connected and automated vehicles” published 6 August 2017, www.gov.uk
5. The Decree of the President of Ukraine dated March 15, 2016 "On the decision of the National Security and Defense Council of Ukraine dated January 27, 2016 “On the Strategy of Cybersecurity of Ukraine".
6. The Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine".
7. KHLAPONIN D.Y., TRUSH I.V.: Normative-legal regulation of cyber-physical systems in the leading countries of the world. Journal of Eastern European Law, 2 (p.2), 115-120.