Creation of Physical Models for Cyber-Physical Systems

Nataliya D. Pankratova(✉)

Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
natalidmp@gmail.com

Abstract. Creation of physical models for cyber-physical systems (CPSs) with consideration of the concept, features and properties of CFS is proposed. The model is based on the general problem of multi-factor risks, the margin of permissible risk, the forecast of the destabilizing dynamics of risk factors, principles, hypotheses, and axioms that are directly related to the analysis of abnormal situations, accidents and disasters. This model is the foundation of the complex technical systems (CTS) functioning. The communication with computational systems and different types of sensors is implemented online in real time. Joint actions of CTS components determine the properties and special features of the mode of functioning of a complex system at any moment of time. A case of the proposed model implementation is given at the example of a real complex technical system.

Keywords: Model · Multifactor risks · Margin of permissible risk · Reliability · Forecast · Safety · Computational systems · Abnormal situations

1 Introduction

Today's cyber-physical systems have not received an unambiguous and generally accepted definition, since these systems are simultaneously located at the intersection of several fields of activities. Their main common feature is the interaction between physical and computational processes, complexity, uncertainty, and connection with the Internet of things. Thus, we can assume that a cyber-physical system is an elaborate system of computational and physical elements that constantly receives data from the environment.

It is taken into account that a CPS is an elaborate system consisting of various natural objects, artificial subsystems and controllers which allow representing of such alliance as a single whole. A CPS ensures close communication and coordination between computational and physical resources, which demand the creation of two types of models. On the one hand, these are engineering models, and on the other, computer models. This paper focuses on the engineering model in which computational elements interact with sensors, providing for monitoring of the performance and maintenance of the technical system. This model is the foundation of the CTS operation. An attempt was made to improve the quality of the survivability and safety of CTS operation with the account of the concept, features and properties of cyber-physical systems. The CTS information platform includes a model in the form of a set of principles, hypotheses,

D. G. Arseniev et al. (Eds.): CPS&C 2019, LNNS 95, pp. 55–63, 2020.
https://doi.org/10.1007/978-3-030-34983-7_6

axioms, methods and techniques; a system of sensors at critical points of a physical system that is providing for the data in the course of operation, and a computational system that brings all data into a unified format; data analysis software that allows to perform the further control of physical elements.

2 Review of the Literature

In cyber-physical systems, computing elements interact with sensors that monitor cyber-physical indicators and with actuators that introduce changes to the cyber-physical environment. The cyber-physical systems carry out computational procedures inside their distributed structure, they include "smart nodes" and make it possible to reconfigure flows in the network depending on the conditions. Thus, cyber-physical systems are distributed systems with the possibility of intelligent processing and reconfiguration of flows at the account of intelligent control [1].

An overview of some history that for more than 40 years (since 197, has been connected with the development of cyber-physics systems, with computers that interact directly with the physical world, was considered in [2]. The recent explosion of the interest in, hype up, and fear of artificial intelligence (AI), data science, machine learning, and robotics have focused a spotlight on software engineers. Business magnate Elon Musk called for regulations and the President of Russia Vladimir Putin declared that the domination in the world will come as a result of AI mastering. Are software engineers responsible for these outcomes? The author of [3] claims that software engineers have less control over their designs than they, most likely, realize. Instead, software technologies are evolving in a Darwinian way or, more precisely, they are co-evolving with the human culture.

One of the biggest challenges in the cyber-physical system (CPS) design is its intrinsic complexity, heterogeneity, and multidisciplinary nature. Emerging distributed CPSs integrate a wide range of heterogeneous aspects, such as physical dynamics, control, machine learning, and error handling. Furthermore, system components are often distributed over multiple physical locations, hardware platforms and communication networks. While model-based design (MBD) has tremendously improved the design process, CPS design remains a difficult task. Models are meant to improve understanding of a system, yet this quality is often lost when models become too complicated. In the paper [4] it was shown how to use aspect-oriented (AO) modeling techniques in MBD, as a systematic way to segregate domains of expertise and cross-cutting concerns within the model.

The role of modeling in the engineering of cyber-physical systems is considered in Reference [5]. It is argued that the role that models play in engineering is different from the role they play in science, and that this difference should invite us to use a different class of models, where simplicity and clarity of the semantics dominate over accuracy and detail. It is argued that determinism in models that are used for engineering is a valuable property and should be preserved whenever possible, regardless of whether the system under modeling is deterministic. There are three classes of fundamental limits on modeling, that is chaotic behavior, the inability of computers to numerically handle a continuum, and the incompleteness of determinism.

The paper [6] is about a better design of cyber-physical systems (CPSs) using better models. Deterministic models have historically proven to be extremely useful and arguably form the basis of the industrial revolution, as well as the digital and IT revolutions. Key deterministic models that have proven to be successful include differential equations, synchronous digital logic and single-threaded imperative programs. Cyber-physical systems, however, combine these models in such a way that determinism is not preserved. Two projects show that deterministic CPS models with exact physical realizations are possible and practical. A new system science that is jointly physical and computational is proposed [7]. In the author's understanding, the embedded computers and networks monitor and control physical processes, usually with feedback loops where physical processes affect computations and vice versa. The integrated simulation tool using a simulator of computer architecture is presented in Reference [8]. In this paper, the simulating computer architecture has many potential use cases as a cyber-physical system, including simulation of side channels and software-in-the-loop modeling and simulation.

The future development of the society is associated with the creation of the Internet of Things, which will allow creating dynamic networks consisting of billions and trillions of such things communicating among themselves. This will ensure a fusion of the digital and physical worlds, for which applications, services, middleware components and end devices are things [9].

The existing diagnosing technologies are oriented at the exposure of failures at early stages, before the appearance of serious malfunctioning in a certain place and class [10–12]. The approach for diagnosing the technical state of a system before a failure, taking into account uncertainties related to the time of the fault, its location and class is considered in [13]. The issues of designing and creating complex anthropogenic systems which satisfy the required level of guaranteed quality (reliability, durability and safety) under conditions of incompleteness of the original information for forecasting technical systems' conditions are investigated in Reference [14].

3 Model of Survivability and Safety of CTS Functioning

The proposed model is based in the replacement of a typical principle of the operability detection turning into the inoperability state based on the detection of failures, malfunctioning, and faults of an object by a qualitatively new principle. The essence of the proposed principle is timely identification and elimination of the causes of undesirable events occurrences and prevention of the transition from normal to an abnormal mode. The strategy of this principle is based on the system analysis of multifactor risks of abnormal situations, a credible estimation of the margin of the permissible risk for different modes of operation of a CTS, and a forecast of the main indicators of operability of an object during the assigned operating period [15].

We shall formulate the main problem of the system analysis of multifactor risks in generalized form [16]. The M_0 set of risk factors ρ_q is known from the data of testing a complex system of arbitrary nature and other a priori information

$$M_0 = \{\rho_q \,|\, q = \overline{1, n_0}\}.$$

Each risk factor $\rho_q \in M_0$ is characterized by a set L_q of attributes l_{qj}:

$$L_q = \{l_{qj} \,|\, q \in N_0; \quad j = \overline{1, n_q}\}, \quad N_0 = [1,\ n_0].$$

Each attribute $l_{qj} \in L_q$ is defined by the information vector

$$I_{qj} = \{x_{qj} \,|\, x_{qj} = \langle x_{qjp} \,|\, p = \overline{1, n_{qj}}\rangle; \quad x_{qjp} \in H_{qjp}; \quad q \in N_0; \quad j \in N_q\},$$

$$H_{qjp} = \left\{x_{qjp} \,|\, x^-_{qjp} \le x_{qjp} \le x^+_{qjp}\right\}; \quad N_q = \left[1,\ n_q\right].$$

Based on I_{qj} sets, the information vector is formed for each risk factor ρ_q.

$$I_q = \{I_{qj} \,|\, q \in N_0; \quad j = \overline{1, n_q}\},$$

$$I_q = \{x_{qj} \,|\, x_{qj} = \langle x_{qjp} \,|\, p = \overline{1, n_{qj}}\rangle; \quad x_{qjp} \in H_{qjp}; \quad q \in N_0; \quad j = \overline{1, n_q}\}.$$

The set M_0 corresponds to a definite, a priori predicted set S_0 of risk situations. In the functioning of a CTS, new risk factors affect it and are revealed, and the properties and indicators of a priori known risk factors $\rho_q \in M_0$ are changed. This results in quantitative and qualitative changes in the set of risk factors that determine the necessity to form a sequence of embedded sets of the form

$$\begin{gathered} M_0 \subset M_1 \subset \ldots \subset M_\tau \subset \ldots, \\ S_0 \subset S_1 \subset \ldots \subset S_\tau \subset \ldots, \end{gathered} \tag{1}$$

where M_τ, S_τ are sets of risk factors and risk situations respectively at the moment $T_\tau \in T^{\pm}$, and $T^{\pm}$ is an assigned or predicted period of functioning of a CTS. Sets M_τ, S_τ are defined as

$$M_\tau = \left\{\rho^\tau_q \,|\, q \in \overline{1, n_\tau}\right\}, \quad S_\tau = \{S^\tau_k \,|\, k \in \overline{1, K_\tau}\}.$$

Each situation $S^\tau_k \in S_\tau$ is characterized by set $M^\tau_k \in M_\tau$ of risk factors ρ^τ_{qk}.

$$M^\tau_k = \left\{\rho^\tau_{q\,k} \,|\, q_k \in \overline{1, n^\tau_k}\right\}.$$

Each factor $\rho^\tau_{qk} \in M^\tau_k$ is characterized by set L^τ_{qk} of attributes $l^\tau_{q_k j_k}$:

$$L^\tau_{q\,k} = \left\{l^\tau_{q_k j_k} \,|\, q_k \in N^\tau_k; \quad j = \overline{1, n^\tau_{q\,k}}\right\}, \quad N^\tau_k = \left[1,\ n^\tau_k\right].$$

Each attribute $l^{\tau}_{q_k j_k} \in l^{\tau}_{q_k j_k}$ is revealed based on the information obtained and processed by a diagnostic system. Information at the moment of measurement T_τ is characterized by its incompleteness, uncertainty and inaccuracy.

In the process of controlling CTS functioning on a true scale of the set moments of time T_τ or with a certain time interval $\tilde{T}_\tau \in T^{\pm}_{\tau}$, $T^{\pm}_{\tau} = \left\{\tilde{T}_\tau \,|\, T_\tau < \tilde{T}_\tau < T_{\tau+1}\right\}$, it is required to carry out a multifactor estimation of risk of any situation $S^{\tau}_{k} \in S_\tau$ and, based on the obtained results, to form and implement a decision on preventing and/or minimizing undesired consequences before the critical moment T_{cr} comes.

In the general case, risk factors ρ_q include the following parameters: risk degrees η_i as the probability of occurrence of undesirable consequences of the impact of any risk factors at any moment of time $T_i \in T^{\pm}$ in the process of CTS functioning; risk level W_i as the size of damage caused by the influence of any risk factors at any point in time $T_i \in T^{\pm}$ and the margin of permissible risk T_0 as the duration of complex system functioning period in a certain mode, when the risk degree and risk level will not exceed the a priori assigned permissible values under the possible influence of risk factors.

We point out a number of fundamentally important peculiarities of the formulated problem [17]:

- sets of risk factors and sets of situations are largely unlimited;
- a threshold restriction of time for decision forming is a top priority;
- the problem is not completely formalized;
- indicators of a multifactor risk estimation are not determinate;
- criteria of a multipurpose risk minimization are not determinate;
- the set of risk situations in principle cannot be a complete group of random events.

Indeed, the problem is presented in a generalized statement that gives the decision-maker certain freedom in adapting it to practical needs in a specific subject domain by the concrete definition of the aforementioned indicators and criteria. Based on the decomposition principle, the general problem of an analysis of the multifactor risk is represented as a sequence of the following system of coordinated, informationally interconnected problems [15]:

- System multifactor classification of revealed and predicted risk situations;
- System multifactor recognition of revealed and predicted risk situations;
- System multicriterion ranking of situations;
- Multipurpose risk minimization of a predicted set of abnormal situations;
- Rational multipurpose optimization of the informedness level in recognition of abnormal situations in the process of complex system functioning;
- Rational coordination of the margin of permissible risk of a predicted set of abnormal situations;
- Determination of a level of rational informedness under the threshold time limitation in the process of complex system functioning;
- System estimation of margin of permissible risk under the dynamics of abnormal mode.

4 Survivability and Safety of Ambulance Operations

Substantial Statement of the Problem. The work of an ambulance which moves in the operational mode, i.e., with a patient on board, is considered. Patient's life is supported by the medical equipment, which is powered from the ambulance's onboard electrical system. The charging current is limited at the level that corresponds to the power extracted from the generator, that is equal to 200 W. The ambulance must travel a distance of 70 km with a particular velocity profile determined by the situation on the road.

It is required to ensure the supply of the electric power for the medical equipment, which is located in the main cabin. Since the motion occurs at night, additional internal and external illumination needs to be provided.

Depending on the speed, the transmission ratio changes, therefore, the frequency of the crankshaft rotation of the main internal combustion engine (ICE1) changes too. In the beginning of the trip, there are 47 L of fuel in the tank. Both engines (ICE1 and ICE 2) are supplied from the same tank. In a normal situation, the car would safely drive the patient for 11,700 s (3 h and 15 min). In this case, the battery voltage does not drop below 11.85 V. At the end of the trip, there are 4.1 L of fuel left in the tank.

The transition into an abnormal mode is caused by the malfunction of the charger, i.e., the voltage sensor RB. It is assumed that the sensor gives out false information that the battery is fully charged. Since no recharging of RB is being made, then with the lapse of time, the battery gets discharged and, consequently, the voltage of the on-board network is also getting decrease during the generator outages (when switching gears, ICE1 idling). Due to the deep discharge, the mode is occurred when the RB output voltage is not enough to maintain the medical equipment operability, and this is an emergency situation.

Recognition of an Abnormal Situation. The recognition of an abnormal situation occurs in accordance with prescribed critical values.

- For the voltage in the on-board network: the abnormal voltage amounts to 11.7 V, while the emergency one is 10.5 V.
- For the amount of fuel: the abnormal value is 21, and the emergency value is 11.
- For the voltage in the rechargeable battery: in the abnormal situation, it is 11.5 V. This way, in the case of the decrease of the function value below one of the set values, the operation of the ambulance goes into an abnormal mode of functioning.

Critical Variables

- Board voltage (depending on the parameters of the RB, generator's condition and load current). If the board voltage drops below the trip level of medical equipment, this could lead right into an emergency.

- Fuel level. Depends on the power, which is taken from the main engine (in proportion to the rotation speed). Decline below a certain point can lead to an abnormal (when you can call another car equipment from an RB) or emergency mode (when the car had to make a stop for a long time without charging).
- Voltage RB (depending on the generator's condition, the total electricity consumption).

The diagnostics unit, which is the basis for ensuring the survivability and safety of complex technical objects functioning, is developed as an information platform for engineering diagnostics [15, 18]; it contains the following modules:

- acquisition and processing of the initial information during the CTO operation;
- recovery of functional dependences (FDs) from the empirical discrete samples;
- quantization of the discrete numerical values;
- identification of sensor failures;
- timely diagnosis of abnormal situations;
- forecast of non-stationary processes;
- generation of the process of engineering diagnostics.

Some results of an ambulance functioning during the first 7000 s are shown in Fig. 1 as diagrams of voltage distribution in the onboard network; the amount of fuel in the tank; and the rechargeable battery voltage. The transition into an abnormal mode happens due to the failure of the battery voltage sensor. The voltage sensor outputs false information to the RB. So far, as long as the battery recharging is not implemented, the battery is discharged with the lapse of time and, consequently, the voltage in the on-board network within 6500–7400 s. is also decreasing and transits into abnormal mode. When the voltage of the on-board network is lower than 11.7 V, the situation becomes abnormal. After lowering the level below 10.5 V, the equipment of the ambulance is turned off and the situation goes into an accident case. The fuel level, which depends on the capacity of the internal combustion engine, is also reduced. The driver stops the car, incorporates a backup generator and troubleshoots the charger. The situation transfers into a normal mode. The period of emergency situation amounts to 120 s: from the moment when the equipment is switched off to the start of the backup generator. After troubleshooting, the driver restarts the motion, without disconnecting the backup oscillator.

At any time of the program operation, the user has the ability to look at the operator's scoreboard, which displays a series of indicators that reflects the state of the CEO of the ambulance functioning. These indicators include: readings of the sensors of the accumulator battery voltage, amount of fuel in the tank, voltage of the on-board network, the state of the system, the risk of damage, causes of the abnormal or emergency mode, as well as the readings of indicator of the danger level for the system operation and possible failures of sensors.

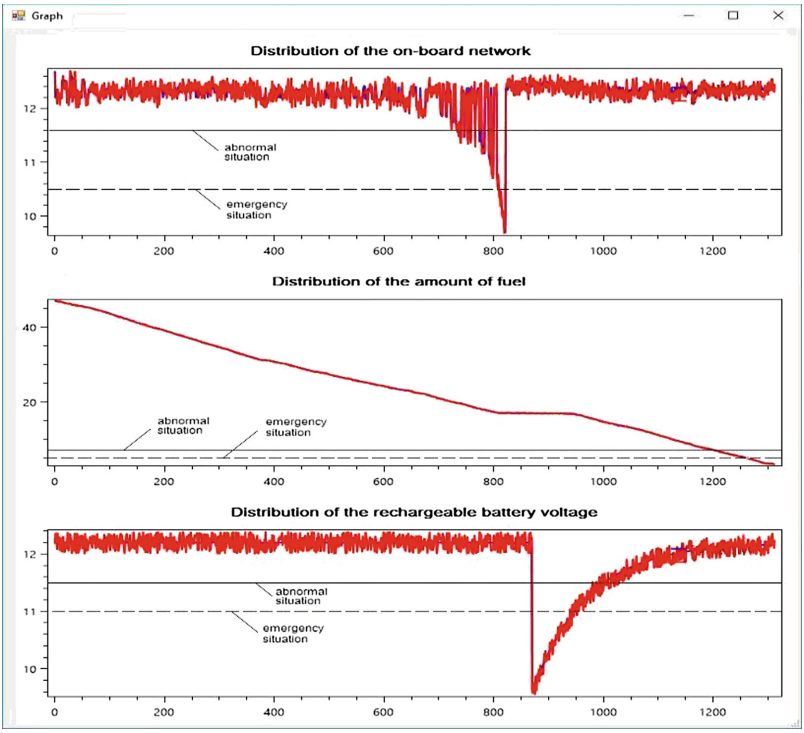

Fig. 1. Voltage distribution of the on-board network, the amount of fuel in the tank, the rechargeable battery voltage in accordance of time *t* sec

5 Conclusion

The proposed strategy of systemic coordination of survivability and safety for technical systems' operation is one of the physical models of a cyber-physical system. The proposed strategy for the operation of the CTS ensures survivability and safety of the system thanks to the timely detection of abnormal situations, assessment of their degree and level of risk, and determination of the margin of acceptable risk in the process of forming decisions on operational actions. Combining a number of similar models into a single network will allow to carry out a rational distribution of the required resources among different consumers online. To solve this problem, it is necessary to develop computational processes, take into account the heterogenity of the data obtained from various applications and devices, develop models and methods for collecting, storing and processing large data, analyze the results obtained from the timely made decisions.

References

1. Tsvetkov, V.Y.: Cyber physical systems. Int. J. Appl. Fundam. Res. **6**(1), 64–65 (2017)
2. Lee, E.A.: Modeling in Engineering and Science. Commun. ACM **62**(1), 35–36 (2019). Viewpoint
3. Lee, E.A.: Is it a smart design or evolution? Commun. ACM **61**(9), 34–36 (2018). Viewpoint
4. Akkaya, I., Derler, P., Emoto, S., Lee, E.A.: Systems engineering for industrial cyber-physical systems using aspects. IEEE Proc. **104**(5), 997–1012 (2016)
5. Lee, E.A.: Fundamental limits of cyber-physical systems modeling. ACM Trans. Cyber Phys. Syst. **1**(1), 3 (2016)
6. Lee, E.A.: The Past, present, and future of cyber-physical systems: a focus on models. Sensors **15**(3), 4837–4869 (2015)
7. Lee, E.A.: Cyber-physical systems – are computing foundations adequate? In: Position Paper for NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, Austin, TX (2006)
8. Kim, H., Wasicek, A., Lee, E.A.: An integrated simulation tool for computer architecture and cyber-physical systems. In: Design, Modeling, and Evaluation of Cyber Physical Systems. Lecture Notes in Computer Science. LNCS, vol. 11267 (2019)
9. Chernyak, L.: The Internet of Things: new challenges and new technologies. Open Syst. DBMS **4**, 14–18 (2013)
10. Huang, S.-R., Huang, K.-H., Chao, K.-H., Chiang, W.-T.: Fault analysis and diagnosis system for induction motors. Comput. Electr. Eng. **54**, 195–209 (2016)
11. Pennacchi, P., Vania, A.: Diagnostics of a crack in a load coupling of a gas turbine using the machine model and the analysis of the shaft vibrations. Int. J. Mech. Syst. Sign. Process. **22** (5), 1157–1178 (2008)
12. Chao, K., Chiang, W., Huang, S., Huang, K.: Fault analysis and diagnosis system for induction motors. Comput. Electr. Eng. **54**, 195–209 (2016)
13. Kulik, A.S., Luchenko, O.A., Firsov, S.N.: Algorithmic providing of the diagnostics modules and restore functionality satellite orientation and stabilization system. Int. J. Radio Electron. Inform. Control **1**, 112–122 (2012)
14. Kotelnikov, V.G., Lepesh, G.V., Martyschenko, L.A.: System analysis of quality and reliability of complex anthropogenic complexes. Int. J. Tech. Technol. Probl. Serv. **4**(2), 35–41 (2013)
15. Pankratova, N.D.: System strategy for guaranteed safety of complex engineering systems. Int. J. Cybern. Syst. Anal. **46**(2), 243–251 (2010)
16. Zgurovsky, M.Z., Pankratova, N.D.: System Analysis: Theory and Applications. Springer, Heidelberg (2007)
17. Pankratova, N.D.: The integrated system of safety and survivability complex technical objects operation in conditions of uncertainty and multifactor risks. In: Proceedings of conference IEEE, Kyiv, Ukraine, no. 50, pp. 1135–1140 (2017)
18. Pankratova, N.D., Radjuk, A.N.: Guaranteed safety operation of complex engineering systems. In: Continuous and Distributed System, Theory and Application, pp. 313–326. Springer (2014)