Modeling of storage processes using Petri nets

Marina Ganzhur^{1,*}, Nikita Dyachenko¹, Andrey Gazizov¹, Arthur Otakulov¹, Dmitry Romanov¹

¹Don State Technical University, 1, Gagarin sq., 344003, Rostov on Don, Russia

Abstract. Cyber-physical systems are actively explored in the global and domestic scientific community. It is expected that cyber-physical systems will minimize human participation in the production process, as well as in many other areas of society. At the same time, the information security aspect of the interaction of elements remains insufficiently studied. The classical approach to ensuring security is aimed at counteracting a clear destructive information impact - when information security breaches have obvious signs. The risk of failure of one object of the system can lead to critical conditions. Safety modeling of managerial structures is reduced to considering the operability of the functions of the intermediate link and the interaction between objects that make decisions on the management and generating teams. By analyzing these transitions in limiting cases, it allows the use of analysis and synthesis approaches based on structural schemes and logical relationships.

1 Introduction

Active use of the term “cyber-physical system” began relatively recently. The German government launched a program to support the development of high-tech technologies High-Tech Strategy [1], which became a prerequisite for the development of a new paradigm of the production process. A distinctive feature is the relationship between the elements of the technological process: in contrast to the classical approach, human participation is minimized, moreover, human participation in some processes can be dangerous both for the successful execution of the process and for the person himself.

Compatibility implies the possibility of interaction between a person and a system using various communication protocols. In this case, all the objects involved in the production process (machines, sensors, computers, networks, etc.) are combined into a single system. Moreover, it implies the active interaction of this system with a person who does not affect the production process itself, but starts it.

To control the functioning of the enterprise during the implementation of the technological process, information technologies are used to create a virtual production model. In turn, the virtual model allows you to control the functioning of the system in real time. Decentralization implies the absence of a central computing device, which allows us to talk about organizing such systems as systems like P2P [2-3]. A general view of the organization of the interaction of elements is shown in Figure 1.

* Corresponding author: mganzhur@yandex.ru

Fig. 1. Centralized and decentralized system management models.

The information obtained on the risk is the basis for the risk management - development and optimization of organizational and technical measures for reducing risk to a predetermined value. The task of risk management is the development of action plans for the risk reduction and control, development of alternative options, as well as assessment of the effectiveness of these plans and elaboration of recommendations for taking management decisions, up to and including refusal of planned activities. The implementation of this set of risk questions is often called risk management. Thus, an outline flow chart in the field of risk most often used in the field of industrial safety is shown in Figure 2.

Fig. 2. Outline flow chart in the field of risk.

2 Modeling of the command passage

Let us consider the elementary scheme of the command passage from CL to EL with the participation of MS operators. Suppose that there is a formed command for EL which should take a certain form after passing the transformation in the operator link (for example, being encoded or supplemented with some specifics). This can be shown using the flow chart in Figure 1.3.

Fig. 3. Elementary flow chart of the command passage.

The further advancement of the command depends on MSO, since in accordance with the hierarchy of EL centralized control architecture, the closest paired link above the standing level is MSO. The following options are possible:

- a) the CLO command undergoes the required transformations in MSO and passes to ELE for execution;
- b) the CLO command reaches MSO, but then it is “lost” and does not enter ELE;
- c) the CLO command is transformed with a change in the information essence and enters ELE in a distorted form;
- d) the CLO command is delayed in CLO for more than the prescribed (normative) time and loses its information efficiency when entering ELE. Thus, the following options are possible:
 - passage of the command;
 - non-passage of the command;
 - distortion of the command;
 - unauthorized command delay.

The reasons for the results may be different. They are associated with the level of training and the psychophysiological state of operators, the state of the interacting equipment, the pursuit of destructive goals. The first reasons are the subject of a study called engineering psychology (or ergonomics). The second reason is investigated from the standpoint of reliability theory. The last reason is associated with the goals and possibilities of causing damage by the human operator, who has the goal of disrupting the correct execution (or non-execution) of the command formed by the CPE for ELE.

The possibilities (probabilities) of results depend not only on the operators, but also on their grouping (i.e. ways of including them in MS). Let us consider two ways to include unique duplicated operators in a simple MS (Fig. 1.4a, b)).

Fig. 4. Flow chart of two ways to include unique duplicated operators in the simplest MS.

If the comparison logic scheme performs addition functions of mod2, then the probability of passage of the command (if any) increases. At the same time, the probability of the appearance of an unauthorized command at the input of ELE (i.e. in case of its absence at the CLO output) remains unchanged compared to a single-operator flow chart. (Fig. 1.3)

This applies to the case when one operator is an intruder. The flow chart shown in Fig. 1.3b) allows an easy conclusion of that at such inclusion of operators of the same type, the presence of one intruder does not change both the risk of non-passage of an authorized command and the risk of appearance of an unauthorized command at any location of the intruder. Such flow chart may undergo a slight change as shown in Fig. 1.5

Fig. 5. Flow chart with logical devices for analyzing the intruder appearance.

In this case, the logical device (LD) performs the conjunction function. The risk of appearance of an unauthorized command in the presence of one intruder is reduced, and the risk of non-passage of an unauthorized command under the same conditions remains the same as for the flow chart with one operator (Fig. 1.3).

Operators can be grouped according to more complex schemes, which comprise of parallel and sequential inclusions.

3 Research

The considered schemes are determined, since based on Boolean logic and operate with the concepts of 0 - command not available and 1 - command available. However, even when describing them, there is the word “risk”, which is approximately equivalent to the concepts described in the probability space.

In order to concretize the approaches, we consider determined and stochastic models of various operators. To do this, we introduce a four-digit matrix with certain names of columns and rows. The columns contain operator inputs. The rows contain outputs.

The fields of the matrix contain the correct and erroneous probabilities of formation of outputs according to the state of inputs.

R \ S	1	0
	1	0
1	P_{11}	$1-P_{00}$
0	$1-P_{11}$	P_{00}

Fig. 6. Matrix of probability of correct and erroneous formation of outputs according to the state of inputs. Where: S is a signal (command) at the input; R is a signal (command) at the output; 0 is the absence of a signal (command);1 is the presence of a signal (command).

In Fig. 1.6, in the fields of the matrix, there are probability of the correct fulfillment of functions by the operator (P_{11} , P_{00}) and the probability of erroneous results, (P_{10} , P_{01}). Such a matrix characterizes the probabilistic approach to assessment of the operators’ activities.

If we assign the loyal values of correct actions to the probabilities, we get the matrix of an ideal operator (Fig. 1.7) or, for the opposite case (limit false actions), the matrix of an ideal intruder (Fig. 1.8)

R \ S	1	0
	1	0
1	1	0
0	0	1

Fig. 7. Matrix of an ideal operator.

R \ S	1	0
	1	0
1	0	1
0	1	0

Fig. 8. Matrix of an ideal intruder.

Transfers to limiting cases make it possible to apply analysis and synthesis approaches based on structural schemes and logical relationships. In order to construct structural schemes, the concepts of operators and units are introduced. Operators are functional elements of the management structure that receive information through one or several inputs for converting it into some output form, which is sent either for further transformations or to the output for transfer to performers. Operators can perform the following types of operations: generalization; refinement; addition; adjustment; coordination; sight aiming; conformity control; comparison; registration; decoding (decryption), etc.

Depending on the operations, for the formation of the output document (instruction for the command, guidelines, etc.), the operator may need informational materials from the system inputs or after passage of the corresponding operations from other operators. Operators in the management structure with several inputs and one output are called units by us. The functioning of the units depends on the availability of information at their inputs. If for the formation of the output information (output) of a unit during its normal operation it is necessary to have some meaningful information at all inputs, then such a unit can be called a conjunctive type unit (in accordance with the truth table, the operation of such a link is described by the conjunction function). If for the formation of the unit output information it is sufficient to have significant information at least at one input, then such a

link can be called a disjunctive link. If the conjunctive type unit (CTU) has two inputs, then the truth table for the case of its normal operation has the following form:

Input 1	Input 2	Output
0	0	0
0	1	0
1	0	0
1	1	1

The disjunctive type link (DTL) during normal operation is described by the truth table having the following form:

Input 1	Input 2	Output
0	0	0
0	1	1
1	0	1
1	1	1

In accordance with the mathematical model given earlier (Fig. 1.3), for the case when the intruder performs the function of a unit, the output information in the tables is inverted.

Note 1. In the considerations above, by default, a designation through 1 of the meaningful information is introduced (i.e., different from 0, which is associated with the absence of any information packages).

Note 2. The matrix model of the intruder in the general case can be complicated due to the asymmetric reaction of the intruder to the inputs excitation. For example, for the case of the presence of an intruder in CTU, the options described by the following tables are possible.

Table 1. The matrix model of the intruder.

Input 1	Input 2	Output
0	0	1
0	1	0
1	0	0
1	1	1
Input 1	Input 2	Output
0	0	0
0	1	1
1	0	0
1	1	1
Input 1	Input 2	Output
0	0	0

0	1	0
1	0	1
1	1	1
Input 1	Input 2	Output
0	0	0
0	1	0
1	0	0
1	1	0

The total will be $2^{2n}-1$ $2^{2n}-1$ variants (n is the number of inputs). Similar reasoning can be carried over to DTU, where deviations from normal functioning are also possible in case of two inputs 2^4-1 .

In case of three inputs, the number of possible reactions to the "intruder" increases according to the exponential law.

To simplify further considerations, we introduce the concept of an admissible and unacceptable reaction of a unit to input states. A reaction that coincides with the values of the truth table is acceptable for the case of normal functioning of this unit. Accordingly, the opposite reaction will be unacceptable. This allows passing to the dual system and will not contradict the truth, because there can be only one combination of states at a time at the unit input, which can always be associated with the permissible and unacceptable output state.

Example of a logical description of the management structure under the conditions of one intruder

Let a certain hypothetical structure be given that has two control inputs, three performing outputs and a certain structure that displays the movement and logical transformation of the command information. The vector flow chart of the investigated structure is shown in Figure 9.

Fig. 9. Vector flow chart of the investigated structure.

Inputs x_1 , x_1 are for management. Outputs x_1 , x_1 , x_1 are for performance. Unit 5 is of the disjunctive type ("DTU", and unit 6 is of the conjunctive type ("CTU"). The remaining

graph operators are single-input, and therefore perform only the functions of converting input information into its output form.

We assume that there may be no intruder in the structure (let us call it the zero state or an intruder can present, but no more than one (the number of such states will be 8).

Syndromes of system states can be displayed by the presence (let us denote it as 1) or the absence (let us denote it as 0) of command information at the performance outputs for various combinations of control commands at outputs (1 — command presence, 0 — command absence). The table of syndromes takes the following form:

Table 2. Syndrome table for outputs x_1 , x_1 , x_1 .

State of inputs x_1 , x_1	Intruder (number in the structure)								
	0	1	2	3	4	5	6	7	8
00	000	100	100	100	000	000	010	001	001
01	011	111	111	111	000	001	001	000	010
10	100	000	000	000	111	100	110	101	101
11	111	011	011	011	100	101	101	100	110

Tables of syndromes can be used to build test sequences for determining the intruder’s location

Figure 10. Length of the test sequence can be different, and in some cases it can even consist of one step. Thus, the intruder with number 6 is detected immediately in case of absence of input influences and appearance of an x_1 unauthorized signal at the output.

Fig. 10. Risk analysis tree.

4 Discussion risk analysis tree

It is believed that it is possible to minimize test checks in which, according to certain rules, the states of inputs change, and the states of outputs are analyzed. The described model is determined, but a probabilistic approach is possible too.

According to the results of the syndromes analysis, the possibility of solving several tasks can be assumed: *The first* one is related to minimization of the number of test checks for the identification of the place of violation, i.e. during the testing process there is an opportunity to submit any possible combinations to outputs in any sequence; for the combination of inputs “01”, four possible places of violation are identified within one step; another combination of “00” in one step shows the result of “0” (no violations), also in the eighth category. *Another* task may be obtaining information on the presence or violation in one of the maximum set of units for the only test combination of inputs; such a combination, with the help of which information about possible violations in five units is obtained, refers to “10”. Another test task may be the one that detects violations without special input influences on the system. In this example, such a task allows checking the sixth unit “00” only. If there is a task of minimal changes in input influences for controlling a specific unit, then this task is solved and its result will depend on which control unit is subject to verification. In the considered example, for testing units six and eight, it is

enough to change the test values at only one input from two, and for checking the fourth and seventh ones, it is also enough to change the test information at one (already another) input. If it is necessary to make sure that the solution to the task is reliable for any unit, the tests can be carried out in the way to exclude the sign or in one or more tests for the final result. In the considered example, the combination "01" with the subsequent input combination "00" identifies the fourth and seventh units as a possible place of violations, and also corresponds to the state without violations. Carrying out test combinations "00" and "11" from the set of zero, four and seven, seven are allocated if there is "000" at the input; in order to select the zero or fourth, one can use the test combination "11"; when receiving "011" at the input, which state corresponds to a working zero one, "100" is a violation in the fourth unit. Such a task is not one-valued. Other combinatorial tasks are also possible, which allow increasing the resolution of the test or the reliability of the final solution.

In case if the violations are random in nature, the task acquires a probabilistic meaning and its solutions are possible only with the use of appropriate stochastic approaches.

5 Modeling of the fuzzy hierarchical petri nets

Fuzzy hierarchical Petri nets are a bipartite directed graph. This is a combination of two types of objects, namely, positions and transitions, represented in the form of circles and rectangles, respectively. The positions may contain a marker related to the degree of confidence, looking like a value point in the range of $[0,1]$. Directed arcs connect input positions with transitions and transitions with output ones. Each transition contains a certainty factor value (μ), which is in the interval of $[0,1]$, and a threshold value (τ). The transition is triggered if $\mu > \tau$. After the transition triggering, the marker is transmitted from the input transition to the output one, with the previous calculation of the output position at the transition. The FPN structure is defined by 9 parameters.

$FPN = (P, T, I, O, D, W, U, Th, M)$, where:

$P = (p_1, p_2, \dots, p_m)$ is a finite set of positions. Each element $p_i = (p_i^I; p_i^O)$ consists of p_i^I - a direct position, and p_i^O - an inverse position; with the performance of the condition $p_i = p_i^I \cup p_i^O$;

$T = (t_1, t_2, \dots, t_n)$ is a finite set of transitions;

$I: P \times T \rightarrow [0,1]$ is an input matrix with the order $m \times n$. If the position p_i is connected by an arc with the transition t_j , then the matrix element $I_{ij} = 1$, otherwise, $I_{ij} = 0$;

$O: T \times P \rightarrow [0,1]$ is the output transition function with the order $m \times n$. If the transition t_j is connected by an arc with the position p_i , then the matrix element is $O_{ij} = 1$, otherwise, $O_{ij} = 0$;

$D = \{d_1, d_2, \dots, d_m\}$ is a set of statements $\infty: P \rightarrow [0,1]$ — a function displaying points of real values within $[0,1]$.

$\beta: P \rightarrow D$ is a function that displays approval points.

$W: P \times T \rightarrow [0,1]$ is an input function presented in the form of a matrix of size $m \times n$. In the matrix, the input value $W_{ij} \in [0,1]$ is the weight associated with the input point. For one transition, the sums of weights for all input points = 1.

$U: T \times P \rightarrow [0,1]$ is the output function presented in the form of a matrix of size $m \times n$. The input value in the matrix $U_{ij} \in [0,1]$ is equal to the value of the certainty factor (μ), which determines the transition t_j affecting its output points p_i ;

$Th: O \rightarrow [0,1]$ is the output function presented in the form of the matrix $m \times n$, the entry in the matrix $\tau_{ij} \in [0,1]$ shows the output threshold at the position p_i from the transition t_j , site $\tau_{ij} = \infty$, if this is not an output position.

M is a dynamic input signal immediately influencing the dynamic behavior of $DFPN.M = (\infty(p_1), \infty(p_2), \dots, \infty(p_m))^T$, the initial marking is indicated as θ .

The structure of the Petri net contains only fragments corresponding to the production rules P1, P2, P3, P4, P5:

P1: “IF A, THEN B” ($A \rightarrow B$) (Figure 11);

Fig. 11. An example of a Petri net formalizing the “IF A, THEN B” rule.

P2: “IF A and B and ... and C, THEN D” ($A \& B \& \dots \& C \rightarrow D$) (Figure 12);

Fig. 12. An example of a Petri net formalizing the rule "IF A and B and ... and C, THEN D".

P3: “IF A or B or ... or C, THEN D”, ($A \vee B \vee \dots \vee C \rightarrow D$) Figure 13;

Fig. 13. An example of a Petri net formalizing the rule "IF A or B or ... or C, THEN D".

P4: “IF A, THEN B and C and ... and D” ($A \rightarrow B \& C \& \dots \& D$), Figure 14;

Fig. 14. An example of a Petri net formalizing the rule “IF A, THEN B and C and ... and D”.

P5: “IF A, THEN either B or C or ... or D”, ($A \rightarrow B \vee C \vee \dots \vee D$) Figure 15;

Fig. 15. An example of a Petri net formalizing the rule “IF A, THEN either B or C or ... or D”.

For a particular case, when one transition is triggered, the following mathematical calculations are applicable to the rules P1, P2, P3 and P5 (Fig. 16):

Fig. 16. Implementation of the rule “IF A, THEN B” in the Petri net.

Here, the degree of confidence is the point $p_j = d_j$. After triggering, if $\mu > \tau$, the marker is transferred from the position p_j to p_k and the degree of confidence will be equal to the following: $d_k = d_j \times w \times \mu$.

But Figure 17 describes rule 4: If d_j then d_{k1} and d_{k2} and ... and d_{km} . Here, the transition has several outputs; the confidence of each output is estimated as $d_{ki} = d_j \times w \times \mu_i$.

Fig. 17. Implementation of the rule "IF A, THEN B and C and ... and D" in the Petri net.

But the transition of the mark to any position is unclear. For triggering of this type of transition, it is necessary to use mathematical modeling of probabilistic inference based on maximile logic, Bayes Theory, or Dempster-Schafer Theory.

According to the theory of fuzzy inference using a maximile model, the inference process is as follows. First, there is a determination of a fuzzy relation representing the knowledge output through operations of *max* and *min*.

The U ratio is calculated according to the formula and can be obtained in the form:

$$U = [\max[\min(\mu(dk_1), \min(\mu(dk_2), \dots, \min(\mu(dk_m))), \max[dk_1], \min(\mu(dk_2), \dots, \min(\mu(dk_m)], \dots, \max[dk_1], \min(\mu(dk_2), \dots, \min(\mu(dk_m))].$$

When constructing a system using a modified Petri net, the following advantages can be distinguished: a description using the rules and properties of Petri nets; no need for inverted transitions; clarity of presentation of events; It does not allow the simultaneous introduction of markers into inverse events, which allows the modeling of critical processes to eliminate the error of an incorrect marking process; provides an opportunity to obtain new conditions that can lead to negative outcomes of critical systems.

According to the results of the matrix representation of the process of fuzzy inference of knowledge according to the composition rule, which reduces risks, the construction of a fuzzy Petri net is demonstrated, which involves the use of transitions max and min. For a fuzzy Petri net, it is difficult to use the mathematical apparatus of analysis known in classical Petri nets. The transition from fuzzy Petri nets to classical ones will make it possible to realize fuzzy knowledge output to them, solve problems of analyzing the output process, which is important when solving diagnostic problems, as well as solving the problems of constructing an elemental base oriented to the tasks of knowledge output in fuzzy machines.

References

1. A. Rowstron, P. Druschel, *IFIP/ACM International Conference on Distributed Systems Platforms and Open Distributed Processing* (Springer, Heidelberg, 2011)
2. R.R. Rajkumar, I. Lee, L. Sha, J. Stankovic, *Proceedings of the 47th design automation conference* (ACM, 2010)
3. B. Radhakisan, H. Gill, The impact of control technology **12**, 161-166 (2011)
4. F. S. Hsieh, J. B. Lin, Context-aware workflow management for virtual enterprises based on coordination of agents, *Journal of Intelligent Manufacturing* (2012)
5. C.R. V'azquez, H.Y. Sutarto, R. Boel, M. Silva, *2010 IEEE Multiconference on Systems and Control* (Yokohama, 2010)
6. C. Mahulea, C. Seatzu, M.P. Cabasino, M. Silva, *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans* (2012)
7. J. J'ulvez, C. Mahulea, C.-R. V'azquez, *Hybrid Systems* **6(2)**, 806 – 817 (2012)
8. J. J'ulvez, C. Mahulea, C.R. V'azquez, *Proc. of the 7th IEEE Conf. on Automation Science and Engineering* (Trieste, 2011)
9. L. Li, D.S. Kim, *Proceedings of the 5th ACM International Conference on Ubiquitous Information Management and Communication (ICUIMC '11)* (Seoul, 2011)
10. F.S. Hsieh, C.Y. Chiang, *Computers in Industry* **62(1)**, 51–64 (2011)
11. D.V. Fatkhi, D V. Fatkhi, Information security of regions. Research and practice journal **2(7)** (2010) ISSN 1995-5731
12. A.P. Ganzhur, M.A. Ganzhur, *System analysis, management and processing of information* (Don State Technical University, Rostov-on-Don, 2013)
13. M.A. Ganzhur, A.P. Ganzhur, V.A. Fatkhi, *Mathematical and computer modeling: Proceedings of the First Research and Practice Conference* (Admiral Ushakov Maritime State University, Novorossiysk, 2014)
14. M.A. Ganzhur, D.V. Fatkhi, A.P. Ganzhur, *System analysis, management and processing of information: Proceedings of the VII International Workshop*, 84-87 (2016)

-
15. M.A. Ganzhur, A.P. Ganzhur, O.V. Smirnova, MATEC Web of Conferences **226** (2018)
<https://www.mateconferences.org/articles/mateconf/pdf/2018/85/mateconfdts201804001.pdf>