Informational Space in the System of Smart Factory

Maria Usova, Ilya Viksnin, Alisa Vorobeva
ITMO University
St. Petersburg, Russia
mausova@corp.ifmo.ru, wixnin@cit.ifmo.ru, alice_w@mail.ru

Abstract—**The need to reduce costs level and human involvement in the production process has led to the search for new approaches to the organization of manufacturing activity. The methods used to create cyber-physical systems became the basis for the concept of Industry 4.0 and Smart Factories in particular. This article discusses the abstract object of digital production and describes the processes of information interaction of agents within it. The authors propose a model of the informational space of a Smart Factory, created on the basis of the set theory concept and discrete mathematics, considering all processes as discrete, and analyze the model from the point of view of information security.**

I. INTRODUCTION

Over the past century, society has made a powerful leap in various fields of science. In connection with the growing needs of society, it became necessary to revise approaches to the organization of manufacturing and transition to high-tech, “smart”, digital production concepts. Digital Production, or Smart Manufacturing is an information model of high-tech factory, including areas of research of new technologies and materials. Digital economy, i.e. economic activities based on digital technology is related to Digital Production. It includes e-business which methods are used on the final stages of production.

This concept is also called Industry 4.0. It is based on sensors that collect information, the Internet as a whole and cloud services in particular. Industry 4.0 concept is embodied in the military, industrial, household spheres. Now the question of ensuring the information security of this concept becomes more relevant.

In particular, the concept of a Smart Factory is based on the interaction of elements within the framework of a cyber-physical system and combines the methods of the Internet of Things (IoT), which ensure the interaction of the physical and informational levels of the system [1]. Previously published works in the field of Industry 4.0 [2-4] address issues related to determining the functioning criteria of the Smart Factory levels their functions, identifying problems that prevent the transition to a new industrial era [5-7], a number of works [8-10] contains a detailed description of models designed on the basis of the IoT.

A disadvantage of modern state of studying Industry 4.0 is a lack of mathematical descriptions of factories and, furthermore, there are no studies in which informational processes are considered. Smart Factory concept is based on Internet of Things and Internet of Services technologies, consequently, information (or informational messages) are the most essential objects of a model. The purpose was to create an informational space with features using various points of view on it.

In this paper the authors present the set-theoretic model of a smart factory as a cyber-physical system and introduce the concept of the informational space, which is used as a communication channel between system agents. The properties of informational messages constituting the information space are determined. The final part of the work is an analysis of the security of the information space of the system, in which the main vulnerabilities of the system are considered, basic models of the behavior of intruders who have a destructive impact on the system are presented.

II. SMART FACTORY SYSTEM

From the point of view of the systems theory, we will consider the factory system as closed, since communications of the elements $\{c_i\}$ are limited by the set of internal connections between agents of the system and the production planning system. The system is not scalable, the number of agent-robots involved in the production is constant. On the other hand, the system of the factory is connected with the environment by logistic system which consists of a set of autonomous cars.

This system is a set of mathematical objects in the form of the structure $< A, I, R, Pr >$. The elements of this structure are the set of objects of the system: the set of agent-robots *A*, the informational space *I*, the set of resources *R*, the set of products (products of digital production) *Pr*, agents communicate with each other using the information space *I*.

A number of agent-robots (agents) $A = \{(a_1|q_1), (a_2|q_2), \dots, (a_n|q_1)\}$ implements the assembly of the product, q_i- is a value characterizing the agent's access level elementary informational messages of the information space, $0 \leq q_i \leq 1$. Each *i*-th agent performs a set of its command function $F_i = \{f_1, f_2, \dots, f_m\}$. The set $\{F_i\}$ for each *i*-th agent forms a uniquely defined production algorithm, as a result of which a certain set of products $Pr = \{pr_1, pr_2, \dots, pr_v\}$ will be produced. The determinism of the algorithms is due to the fact that, on the other hand, the product is the result of a certain function $pr_i = f(A_i, F_i, R_i, I, t)$, which is indirectly dependent on time and a set of elementary messages of the informational space I and directly dependent on the set of initial resources $R = \{r_1, r_2, \dots, r_s\}$. And if Q is the space of digital production, then $f_{pr} : Q \to Pr$.

III. INFORMATIONAL SPACE

The informational space presented in Fig. 1, is the structure $< I, D >$:

- $I = \{i_1, i_2, \dots, i_l\}$ - a set of elementary informational messages,

- $D = \{d_1, d_2, \dots, d_l\}$, $0 \le d_i \le 1$ - a set of elements that characterize the parameters of access to the *i*-th informational message.

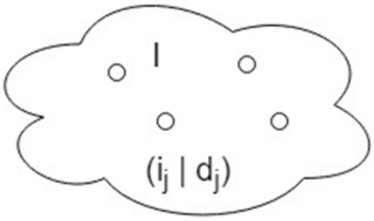

Fig.1. General view of the informational space

Informational space is represented as a set of subsets of information messages, grouped by position in space:

$$I = I_{main} \cup I_{interaction_{a,b}} \cup I_{agents} \quad (1)$$

Consider a three-dimensional representation of the informational space in the coordinates a, b, t. Axis a is the axis of agents sending informational messages, axis b is the axis of agents receiving informational messages, axis t is the axis of time:

- On the axes a and b, agents r_k are discretely displayed, where k is the sequence number of the agent.
- Time in the system is considered as a discrete value.
- The assumption that the transmission time of the information message tends to zero is introduced: $t_{transmission} \to 0$, then $t_{send} = t_{receive} = t_c$. This assumption allows us to find the transmitted message in the information space along the t axis.

The visualization of the informational space model is shown in the Fig. 2.

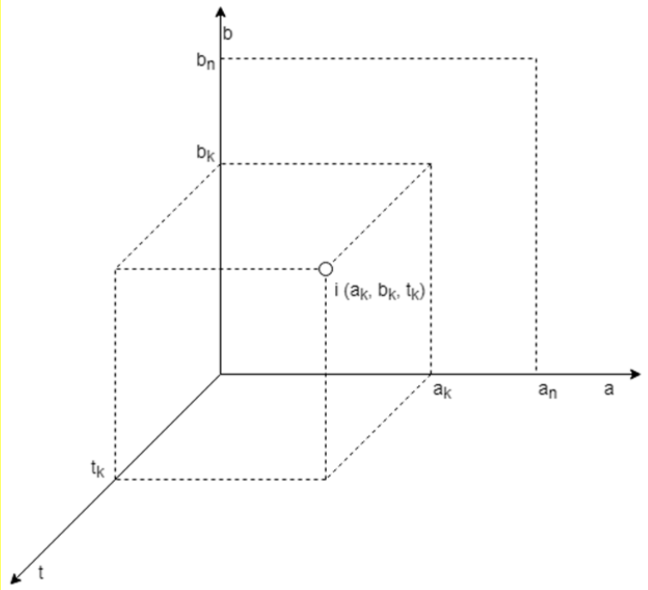

Fig. 2. Three-dimensional view of the informational space

If n is a number of agents in the system, then the axes of senders and receivers of the informational messages are limited to agents a_n, b_n.

An infinite parallelepiped limited by the straight lines $a = a_n$, $b = b_n$ is a set of informational messages $I_{interaction_{a,b}}$. The cluster defines a set of the messages transmitted between agents *a* and *b*, they are available to these agents only. In this case the access parameter *d* is defined as $d = min(d_a, d_b)$. The Fig. 2 shows the *i-th* message in space with coordinates (a_k, b_k, t_k).

The space bounded by the values $a_0 < a < a_n$, $b > b_n$, $t > 0$ is the cluster I_{main}, which is defined as a set of informational messages' sets $I_{main} = \{(\{i\}|d_k)\}$ that are grouped by the access parameter *d*, and the cluster is common for all robots: any a_i agent can access the i_k message if the $q_i \ge d_k$ condition is satisfied.

If $a = b$, then we can assume that the coordinates of the receiver-agent in the space are $b_k\ (a_k; 0; 0)$, that is, the agent sends the messages (work reports, error reports, etc.) to itself. Such messages will be called agents' own messages. The semi-infinite plane bounded by the straight lines $a_0 \le a \le a_n$, $b = 0$ is the cluster I_{agents} containing the set of the *k*-th agent's own messages $\{i_k\}$. Agent's messages access parameter is equal to agent's own access level $q_i = d_k$.

The projection of the informational space on the *aob* plane is shown in the Fig. 3.

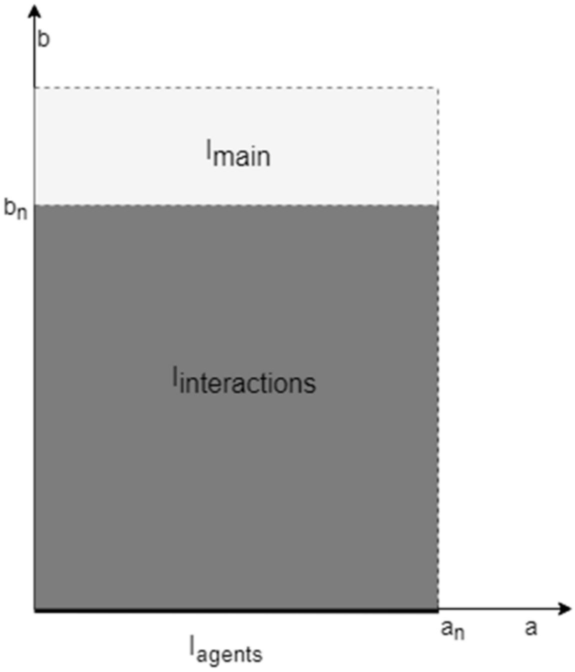

Fig.3. The projection of the informational space on the *aob* plane

The information space can also be represented as a two-dimensional *ID* space (Fig. 4). Coordinate axes are the set of elementary messages and the corresponding values of the access parameter defined for the *k*-th third-party agent. This representation may be helpful in grouping all messages by their access parameter.

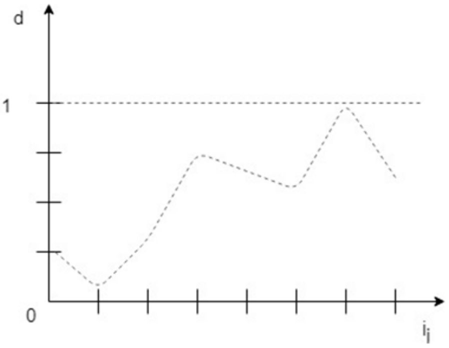

Fig. 4. Two-dimensional model of the informational space in *ID* coordinates

Summing up, it is possible to schematically show the interaction of various agents with the informational space. The agents *a*, *b*, *c* and particular clusters of the informational space are given: the public I_{main} , cluster of the messages of interacting agents *a*, *b*, and the own message clusters of agents *a*, *b* (Fig. 5).

It can be noted that agents *a*, *b* have access to all clusters of messages, except for a cluster of own informational messages of another agent. Agent *c* has access only to the I_{main} cluster, because it is an external agent relatively the process of informational interaction between agents *a*, *b*.

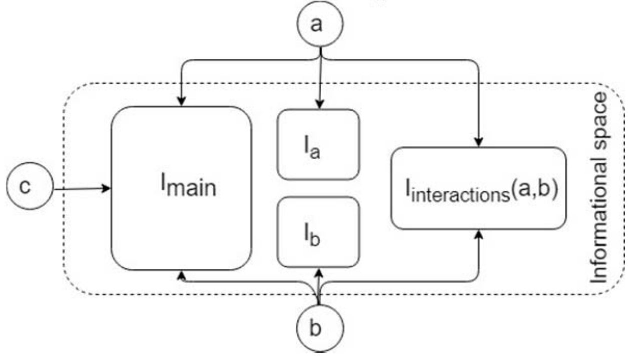

Fig. 5. Interactions between agents and clusters of the informational space.

IV. Channels of information transmission

A. General case of informational channel

In the general case, the process of informational messages' transmitting is a process that includes the sequential creation of an informational message, encoding, sending to the communication channel (informational space), sending a message from the communication channel to the receiver, decoding and checking the integrity of the decoded message by the sender agent and the receiver agent. The UML diagram describing the process of transmitting an information message is shown in the Fig.6.

The informational space, as was already described, is an intermediate in the process of informational messages transmitting and serves to record them in the permanent memory of the system. After receiving the encoded message by the information space, the following attributes are assigned to it:

- the time of creating a memory cell to store it (transmission time)
- sender-agent, receiver-agent IDs
- access level parameter

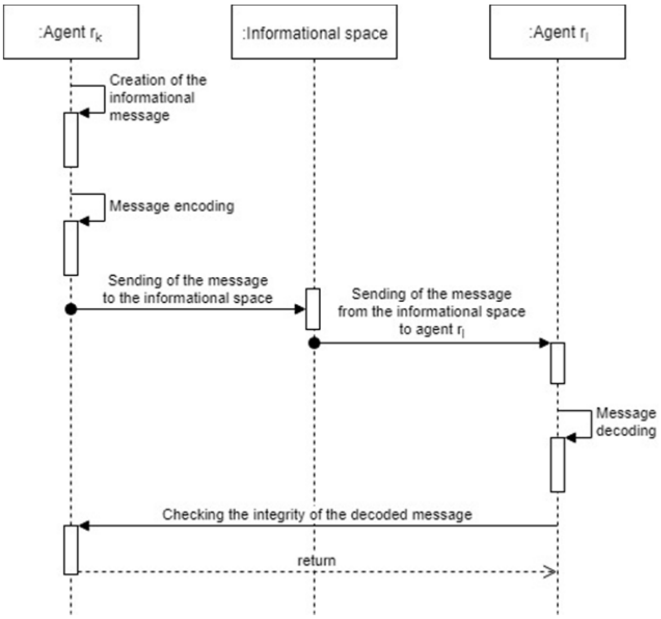
:Agent r_k
:Informational space
:Agent r_l
Creation of the informational message
Message encoding
Sending of the message to the informational space
Sending of the message from the informational space to agent r_l
Message decoding
Checking the integrity of the decoded message
return

Fig. 6. Communication process between two agents

Integrity check (checksum verification) is a mandatory step in the process of information exchange due to the fact that errors in recording, encoding and decoding messages are not excluded.

Any of the agents involved in the process of messages transmission can refer to them for the purpose of reading or exploit using the recording time of the message and the identification number of the interlocutor-agent as parameters for the search. In Section 5 all available actions of agents with messages are described. In this case, it is impossible to re-write message or change its data.

B. Informational channel of a single agent

The messages transmission using the informational space can be carried out unilaterally if $i_k \in I_{main}$ or $i_k \in I_{agents}$. The sequence diagram for these interaction options is shown in the Fig.7. We propose an interaction model which includes a process of message encoding.

C. Bandwidth

We assume that the described information transmission channel is a discrete channel without interference, characterized by a system of values $[Y, c(y), a]$ [11]. The value y takes a discrete value from the set of Y values. On Y, some numerical function $c(y)$ is given - a penalty function. The number a and the condition $c(y) \leq a$ are given. We introduce the probability distribution $P(y)$ on Y with the

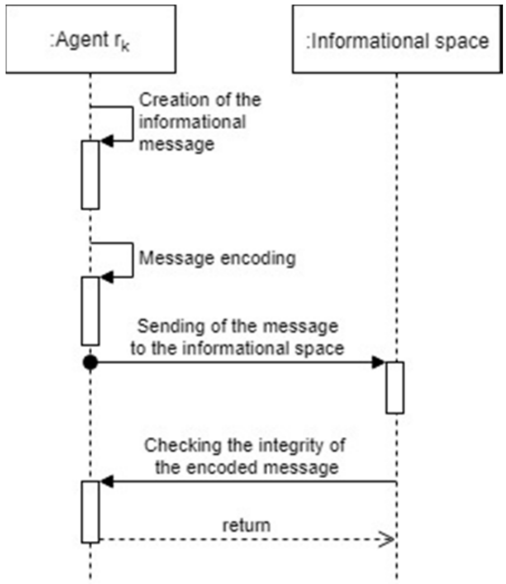
:Agent r_k
:Informational space
Creation of the informational message
Message encoding
Sending of the message to the informational space
Checking the integrity of the encoded message
return

Fig. 7. Communication process for one agent

condition for the average value:

$$\sum c(y)P(y) \leq a \quad (2)$$

Channel capacity is defined as the maximum entropy value:

$$\mathrm{C} = sup_{P(y)}H_y \quad (3)$$

The maximum value of entropy takes place at the highest of the possible costs, therefore we set:

$$C = c(y) * P(y) \quad (4)$$

The value $c(y)$ may have a physical or technical meaning. It can describe the cost of particular letters, indicate the unequal costs of recording or transmitting a single letter, or correspond to penalties for various adverse factors.

V. The properties of informational messages

A. Theoretical properties of informational messages:

1) Informational messages (IM) are discrete in time and space.

2) Nonadditiveness. Adding IM to existing ones does not increase the total amount of information by the amount of added information.

3) Nonassociativeness. Let $f_1(I) = h\ (i_1 + \cdots + i_n)$ is the first function algorithm to be executed by the agent, $f_2(I) = h(i_n + \cdots + i_1)$ is the second function algorithm, and the functions differ only in the order of summation of certain informational messages, then $f_1(I) \neq f_2(I)$ by definition of determinacy of algorithms inside the factory system

4) Obsolescence of IM. The data contained in IM may lose their relevance after a certain time.

5) Non-disappearance of IM. As part of the work, the authors introduce the assumption that a message placed in informational space cannot be deleted.

6) The invariability of information in time. Similar to property 5, an informational message in the space cannot be changed by the sender-agent, the receiver-agent, or the third-party agent.

7) Independence of the representation of informational messages for various agents, syntactically and semantically.

8) The pragmatic value of informational messages depends on the class to which the agent belongs.

9) Non-equivalence of the value and usefulness of the information contained in the IM (consequence of property 8).

B. Physical properties of informational messages

1) Memorability. Due to the fact that the messages transmitted by agents are recorded in the information space, these messages are linked to the transmission time, therefore, they are also remembered physically.

2) Transferability. Informational messages are transmitted via communication channels within the factory system.

3) From property 2 follows the ability of the IM to be copied. Let t_{copy} be the point in time at which the message will be copied, then:

$$i\left(t_{copy}, i(t_k)\right) = i(t_k) = i(t_{copy}),\ t_k \leq t_{copy} \quad (4)$$

4) Reproducibility. In the ideal case, the copied message is syntactically identical to the original (reproduced) message. In real systems, there is a possibility of copying errors.

Let a discrete message $i(l, X)$ be transmitted, where *l* is the length of the information message, $l \in N$, $X = \{(x_1|p_1), (x_2|p_2), \ldots, (x_n|p_n)\}$ - is the set of available symbols of the alphabet with the length *n* and the corresponding error probabilities of recording the letter is *p*, $0 \leq p \leq 1$. To be considered that a writing error has occurred, the number of incorrectly written characters of the message must be more than or equal to the number *m*. Message characters are written independently of each other. Then the probability of writing a message is calculated by the formula:

$$P_{error} = \sum_{k=m}^{l} P_k \quad (5)$$

C. Possible actions with messages

1) Reading. All agents possessing sufficient access rights have rights to read messages from the I_{main} cluster. Reading messages from the $I_{interaction_{a,b}}$, I_{agents} is performed by receiver-agents and sender-agents for the first, sender-agents for the second case.

2) Writing. Writing of informational messages is possible once only, rewriting an existing message is not possible.

$I_{rewrite}$ message cluster is selected, in the space of which the sender-agents have the rights to rewrite messages. This cluster includes messages containing obsolete data, the relevance of which must be maintained, for example: customer requests, actions algorithms for robots, etc.

3) Exploit. The agents who have rights to read IM have the rights to exploit the data contained in these messages. It is understood that the messages are intended for a specific group of robots in the factory system.

VI. Vulnerabilities. Destructive informational impact

A. Vulnerabilities of the informational interactions

Vulnerability is a characteristic of an informational system, the use of which may lead to the realization of a threat.

When analyzing a Smart Factory system, it is possible to say that the informational space and robots-agents are vulnerable to destructive impact, the result of which is a disruption of the functioning of the system, its stopping and theft of the information. The consequence of the destructive impact on the communication channel of agents, the syntactic integrity of information messages is compromised, which leads to a violation of semantic and pragmatic values of information. In case of direct impact on agents, agent may be disabled, transfer false information, or transfer information to third-party attacker-agents.

When considering the destructive informational impact on the described system, the following classification of possible vulnerabilities is proposed:

- Network level vulnerabilities (network protocol vulnerabilities)
- Operating System (OS) level vulnerabilities
- Database level vulnerabilities. Because of the introduced assumption of the invariability of the majority of informational messages written in the informational space, we will assume that this class of vulnerabilities is related to informational messages that can be rewritten or transmitted in real time. This class of vulnerabilities also includes the lack of backup, which can cause the stop of system functioning.
- Vulnerabilities from the point of view of physical security
- Communication vulnerabilities. These vulnerabilities include ones in cryptographic algorithms, lack of validation of input data (the robot-agent can send incorrect data), lack of validation of the data being processed (vulnerabilities that can be exploited at the stages of coding, transmission in the communication channel, decoding), the threat of uncontrolled copying messages.
- Access control vulnerabilities. In the system the mechanisms of access control to informational messages and authentication, identification of system's agents are described. The system is not scalable, because the introduction of a third-party agent is possible in case of disabling a functioning agent only.

B. Attacker's behavior patterns

An attacker - is a subject that has an impact on the informational process in order to cause its deviation from the conditions of its normal flow. Model of the attacker's behavior will be considered as an algorithm of actions, which he follows accordingly to his goal.

The attacker's goal is to achieve a certain state of an informational system or information in it. In accordance with the identified vulnerabilities of the system, it can be said that the targets of an attacker could be the malfunction or functioning stop of the system or theft of information.

The methods used to achieve the goal by an attacker are determined by his position relative to the system placement at the initial time of the attack. An attacker is considered as an external one if he is outside the system and does not have access rights to the information transmitted inside it. An internal attacker is an agent of the system. At the same time, an external attacker can implement internal threats to information security. Using the description of the attackers, their goals and vulnerabilities of the system, it is possible to describe their basic behavior patterns (behavior models).

1) Model 1:

Intruder type: external
Purpose: change the system's functioning state
Basic exploitable vulnerability: agent's OS vulnerabilities
Intermediate result of the attack: the attacker manages the actions of the agent, the ability to use access control vulnerabilities
The result of the attack: changing data in the informational space

2) Model 2a:

Intruder type: external
Purpose: theft of the information
Basic exploitable vulnerability: OS vulnerabilities, access control vulnerabilities
Intermediate result of the attack: the attacker manages the actions of the agent
The result of the attack: attacker sends informational messages outside the system to a third-party agent

3) Model 2b.

Intruder type: external
Purpose: theft of the information
Basic exploitable vulnerability: communication channel vulnerabilities
Intermediate result of the attack: the attacker «listens» to the communication channel
The result of the attack: sending informational messages outside the system to a third-party agent

Due to the non-scalability of the system (the impossibility of the functioning of more than *n* agents at the moment of time), the following strategy is implemented by making the agent disabled.

4) Model 3:

Intruder type: external
Purpose: any of the described

Basic exploitable vulnerability: agents' OS vulnerabilities, network protocol vulnerabilities, physical security vulnerabilities
Intermediate result of the attack: the selected agent has stopped functioning, the attacker is disguised as an agent using his identifiers
The result of the attack: the change of the informational messages in the information space, the false data transmission, theft of information, etc.

C. Attack consequences

A Smart Factory system is presented, it consists of 10 agents connected in series and in parallel (Fig. 7). The agents located in series get an intermediate product from the previous agents and, after their execution of their algorithm, transfer it to the next agent. Agents located in parallel perform the same functions and are interchangeable. Suppose that for the interval t one chain of agents produces n products. The value $N = k\frac{n}{t}$ will be called the production capacity of the system, where k is the number of consecutive chains of agents.

In the system shown in the Fig. 8, one of the agents (marked as gray) was attacked by a third-party violator and stopped functioning. In this case, production flows were regrouped relatively to the parallel "healthy" agent. The value of production capacity is limited on top by the amount of production that this agent can produce, then the value of production capacity will take the value $N_{reorg} = \frac{n}{t}$.

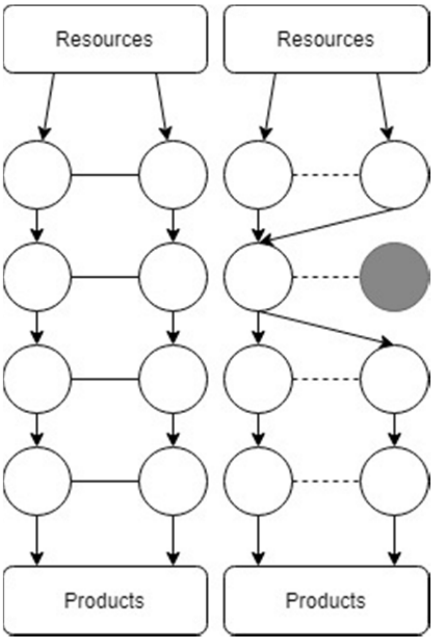

Fig. 8. System's functioning after the attack

The replacement time of the agent in the system is t_{repair}, the cost of one product is $cost$.

The amount of losses will be $COST = t_{repair} * n * cost$ of conventional units.

VII. CONCLUSION

The paper describes interactions of agents using the informational space inside Smart Factory. Properties of the informational messages were defined, and behavior patterns of attackers were presented.

The model of the informational space provides a wide spectrum of opportunities for development and implementation of new interactions methods for agents and can be a start point for developing a wider attacker model and a threat model.

We defined new tasks for the work as follows:

- Develop an information security model for Smart Factory.
- Develop a simulator and test the effectiveness and stability of the informational space model.
- More complex approach for the informational space description has to be presented.

The development of the project requires, on the one hand, a common informational space within the system to increase the speed data access (which is the solution to the problem of information accessibility), on the other - ensuring data confidentiality, which is solved by the introduction of the access rights of the system objects to informational messages. The wide spread of the concepts of digital manufacturing and Industry 4.0 arises the need to make their use safe for both companies and consumers of services and products, including ensuring the security of the data used at various stages of production.

REFERENCES

[1] H.S. Kang, et al. "Smart manufacturing: Past research, present directions, and future directions", *International Journal of Precision Engineering and Manufacturing-Green Technology,* vol. 3, pp. 111-128, 2016.

[2] S. Wang, J. Wan, D. Li and C. Zhang, "Implementing smart factory of industrie 4.0: an outlook", *International Journal of Distributed Sensor Networks*, vol. 12(1), 2016, p. 3159805.

[3] D. Zuehlke, "SmartFactory—Towards a factory-of-things", *Annual Reviews in Control*, vol. 34(1), 2010, pp. 129-138.

[4] J. Lee, "Smart factory systems", *Informatik-Spektrum*, vol. 38(3), 2015, pp. 230-235.

[5] M. Bauer, L. Jendoubi and O. Siemoneit, "Smart factory–Mobile computing in production environments", *Proceedings of the MobiSys 2004 Workshop on Applications of Mobile Embedded Systems, June* 2004.

[6] A.R. Sadeghi, C. Wachsmann and M. Waidner, "Security and privacy challenges in industrial internet of things", *Design Automation Conference (DAC), 52nd ACM/EDAC/IEEE*, 2015, pp. 1-6.

[7] K. Zhou, T. Liu and L. Zhou, "Industry 4.0: Towards future industrial opportunities and challenges", *Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference,* Aug. 2015, pp. 2147-2152.

[8] D. Lucke, C. Constantinescu and E. Westkämper, "Smart factory-a step towards the next generation of manufacturing", *Manufacturing systems and technologies for the new frontier*, 2008, pp. 115-118.

[9] S. Wang, J. Wan, D. Zhang, D. Li and C. Zhang, "Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination", *Computer Networks*, 2016, vol. *101*, pp. 158-168.

[10] D. Ivanov, A. Dolgui, B. Sokolov, F. Werner and M. Ivanova, "A dynamic model and an algorithm for short-term supply chain scheduling in the smart factory industry 4.0.", *International Journal of Production Research*, 2016, vol. *54*(2), pp. 386-402.

[11] R.L. Stratonovich, *Information Theory*. Moscow, 1975.