Chapter

Cybersecurity Risk Analysis of Industrial Automation Systems on the Basis of Cognitive Modeling Technology

Vladimir I. Vasilyev, Alexey M. Vulfin and Liliya R. Chernyakhovskaya

Abstract

The issues of procuring the cybersecurity of modern industrial systems and networks acquire special urgency because of imperfection of their protection tools and presence of vulnerabilities. International standards ISA/IEC 62443 offer the system risk-oriented approach to solve the tasks of providing the security of industrial control systems (ICS) at all stages of life cycle. But in view of high uncertainty and complexity of procedure of formalizing the factors affecting the final indices of system security, the problem of cybersecurity risk assessment remains open and requires applying new approaches based on the technology of data mining and cognitive modeling. Cognitive modeling of risk assessment using fuzzy grey cognitive maps (FGCM) allows us to take into account the uncertainty factor arising in the process of vulnerability probability assessment for each of security nodes. The interval estimates of FGCM connection weights can reflect the scatter of expert group opinions that allows us to take into account more completely the data available for risk analysis. The main stages of ICS security assessment with use of FGCM are analyzed in the chapter on the example of distributed industrial automation network. The recommendations concerning the choice of the necessary countermeasures improving the level of network security in the conditions of possible external and internal threats are considered.

Keywords: fuzzy grey cognitive map, cybersecurity risk analysis, industrial automation systems, cognitive modeling, integrity control model automation system

1. Introduction

Digital economy, cyber-physical objects, cyberspace, and Internet of Things are concepts that have firmly entered our lives in recent years. As a part of industrial revolution "Industry 4.0," the face of modern industrial enterprises, which actively use the transition to unmanned production technologies, the integration of information technologies into the most complex production processes, has dramatically changed. In this case, a distinctive feature of production is the close connection of technological networks with the corporate network, as it is necessary both for production management and for administration of industrial networks and systems. Modern technological networks, as a rule, have direct access to the Internet, for example, for maintenance and technical support of industrial automation systems by employees of organizations—contractors. Also, computers of contractors, developers, integrators, and system/network administrators connected to the technological network of the service company from the outside often have free access to the Internet.

Under such conditions, the problem of ensuring the security (cybersecurity) of industrial automation and control systems (IACS) sharply increases. In corporate networks, the object of protection is information and the problem of ensuring the confidentiality of information is primarily addressed. However, in the case of industrial automated control systems, the object of protection is already technological processes (TP), and not ensuring the confidentiality of information comes to the fore, but first of all ensuring the continuity and integrity of the TP itself. Speaking of IACS cybersecurity, the so-called digital attacks (cyber-attacks) are primarily considered associated with exposure to IACS through the control and monitoring devices—controllers, data acquisition and transmission devices, SCADA servers, workstations, telecom equipment, communication lines, etc.

The severity and relevance of IACS cybersecurity problem are confirmed by statistics of recent years, showing a sharp increase in the number of the targeted attacks on industrial networks and systems, as well as an increase in the scale of consequences of these attacks. A vivid example of a large-scale cyber-attack that hit a lot of companies around the world from May 12 to May 15, 2017 is the attack of a network worm—the coder WannaCry [1]. Among the victims of this well-coordinated attack were companies engaged in various types of production, oil refineries, urban infrastructure facilities, and distribution power grids.

In May 2018, VPNFilter malware, which infected at least 500,000 routers and data storage devices in 54 countries around the world, was detected. The purpose of this software is to steal credentials, detect industrial SCADA equipment, and carry out various attacks using infected devices in the botnets. June 2018 was marked by a large-scale cyber-attack on telecommunications companies, communication satellite operators, and defense contractors in the United States and Southeast Asia. During the attack, the attackers infected computers used for managing the communication satellites and collecting geoposition data. According to experts' opinions, the purpose of the cyber-attack was espionage and data interception from civilian and military communication channels. In total, according to Kaspersky Lab, the share of attacked IACS computers in the world in 2018 increased by 3.2% compared with 2017 and amounted to 47.2% [2].

Considering the seriousness of the current situation and the need to take urgent measures, the international community and information security experts are concerned about finding effective ways to solve the problem of ensuring the security of industrial automated systems. For instance, the European Commission has developed the European Program for Critical Infrastructure Protection. Several international standards for ensuring the cybersecurity of automated process control systems have been proposed and effectively used in world practice, such as NERC Critical Infrastructure Protection, NIST SP 800-82 Guide to Industrial Control Systems Security, ISA/IEC 62443 Industrial Automation and Control Systems Security [3, 4].

The basis of the requirements presented by the ISA/IEC 62443 standards series for ensuring the IACS security is a risk-oriented approach. In accordance with this approach, designing of a management system for a protected IACS involves the following stages:

- high-level (preliminary) risk assessment of cyber-attacks effects;
- building a reference model of IACS as the protection object, describing the classification of main activities types, technological process, automatic control systems, and other assets;
- building an asset model, describing the hierarchy of main objects and assets of IACS, their interaction with networks, key divisions, etc.;
- building a reference architecture model, reflecting all basic elements of IACS, telecommunication equipment, communication lines, etc.;
- building a zone and conduct model, dividing the protected object into separate security zones;
- detailed risk analysis for each selected zone; and
- determination of the current security level for each zone and requirements to ensure the target security level of the zone, implemented by the choice of appropriate protection measures.

At the same time, the “bottleneck” of the above normative documents regulating the issues of ensuring IACS cybersecurity is the absence of formalized methods for detailed risk assessment. As the volume of statistical data, development of mathematical models of risk, threats, and security incidents increase, it becomes topical to develop methods and algorithms for quantitative risk assessment, ensuring the possibility of a reasonable choice of IACS devices and the necessary countermeasures both within individual security zones and ensuring the required cybersecurity level of IACS as a whole.

A promising way to solve this problem is the use of technology of cognitive modeling, based on construction and analysis of fuzzy grey cognitive maps (FGCM), which has been widely used in recent years [5–10]. Fuzzy grey (interval) cognitive maps are considered to be a good extension of fuzzy cognitive maps (FCM) family, since they are better suited to experts representations, have a greater interpretability and provide more degrees of freedom to the decision making person on the basis of modeling results.

Brief information concerning the “grey” system, the “grey” number, and the “grey” variable is presented below, and the mathematical apparatus of FGCM is considered. Then, on the example of solving the problem of ensuring the integrity of telemetric information in IACS, the technique of assessing the cybersecurity risks with use of FGCM is discussed. In the end of the chapter, the conclusions are drawn and the list of references is given.

Let us note one important circumstance. When considering below a specific example of AIS risk assessment using FGCM (Section 2), an approach based on decomposition of the original (integrated) FGCM by disclosing (detailing) the content of its concepts is used, resulting in the set of interconnected local FGCM that characterize certain aspects of AIS risks assessment procedure associated with the features of its subsystems. In ideological plan, this approach is based on the FCM decomposition theory and the algebra of FCM causal transformations proposed in [11, 12]. However, the main difference between the approach described in [12] and our approach is that in [12] the detailed FCM system of a large size comes out as the original FCM, which reduces to a simpler (quotient) FCM by using the operations proposed by the authors. Each concept of this quotient FCM accumulates information on the state of several similar concepts of the original FCM, thus aggregating the corresponding concepts. In our case, on the contrary, the original FGCM has a small dimension, the number of forming its basic concepts corresponds to the number of basic subsystems of the system under study, and the decomposition of FGCM implies a representation of each concept of the original FGCM in the form of independent (local) FGCM, describing the behavior of this concept.

2. Theoretical foundations of building FGCM

The basis of building FGCM is the Grey Systems Theory, proposed in 1989 by Deng [10]. Within the framework of this theory, objects and systems with high uncertainty, represented by small samples of incomplete and inaccurate data, are studied. Depending on the character of the available information, the studied systems are divided into three types:

- "white" systems (the internal structure and the properties of the system are completely known);
- "grey" systems (partial information about the system is known); and
- "black" systems (the internal structure and the properties of the system are completely unknown).

In accordance with the terminology of the grey systems theory, a fuzzy grey cognitive map is a cognitive model of a system in the form of a directed graph defined with use of the following set:

$$\mathrm{FGCM} = \langle C, F, W \rangle, \tag{1}$$

where $C = \{C_i\}$ is the set of concepts (vertices of the graph), $(i = 1, 2, \ldots, n)$; $F = \{F_{ij}\}$ is the set of connections between concepts (arcs of the graph); and $W = \{W_{ij}\}$ is the set of the relationships between the concepts determining the weights of these connections, $(i,j) \in \Omega$. Here, $\Omega = \{(i_1, j_1), (i_2, j_2), \ldots, (i_L, j_L)\}$ is the set of the pairs of adjacent (interconnected) vertices indices, $L \leq n(n-1)$.

In contrast to the traditional FCM representation, the weights of FGCM connections are set with the use of "grey" (interval) numbers $\otimes W_{ij}$, defined as

$$\otimes W_{ij} \in \left[\underline{W_{ij}}, \overline{W_{ij}}\right], \text{where } \underline{W_{ij}} < \overline{W_{ij}}, \left[\underline{W_{ij}}, \overline{W_{ij}}\right] \in [-1, 1], \tag{2}$$

where $\underline{W_{ij}}$ and $\overline{W_{ij}}$ are, respectively, the lower and the upper boundaries of the grey number. So, the weight of connection between i-th and j-th concepts $(C_i \to C_j)$ can take any value within the given range of change $\left[\underline{W_{ij}}, \overline{W_{ij}}\right] \in [-1, 1]$. In the particular case, when $\underline{W_{ij}} = \overline{W_{ij}}$, we get $\otimes W_{ij} \in \left[\underline{W_{ij}}, \underline{W_{ij}}\right]$—a "white" (crisp, usual) number.

It is assumed that the change of the concepts state in time is described by equations

$$\otimes X_i(k+1) = f\left(\otimes X_i(k) + \sum_{\substack{j=1 \\ (j \neq i)}}^{n} \otimes W_{ji} \otimes X_j(k)\right), (i = 1, 2, \ldots, n), \tag{3}$$

where $\otimes X_i(k)$ is the "grey" (interval) variable of the i-th concept C_i state, the values of which at each time instant $k = 0, 1, 2, \ldots$ belong to some interval $\left[\underline{X_i}(k), \overline{X_i}(k)\right]$; f is the activation function of the i-th concept, mapping the argument values into the interval $[-1, 1]$. The activation function $f(\bullet)$, as a rule, is accepted in the following form:

a. linear function with saturation:

$$f(x) = \begin{cases} x, \text{if} |x| \leq 1; \\ \text{sgn } x, \text{if} |x| > 1, \end{cases} \tag{4}$$

b. bipolar sigmoid (hyperbolic tangent):

$$f(x) = \frac{(1 - e^{-x})}{(1 + e^{-x})} = \text{th}\left(\frac{x}{2}\right); \tag{5}$$

c. unipolar sigmoid:

$$f(x) = 1/(1 + e^{-x}). \tag{6}$$

To solve the system of equations (Eq. (3)), it is required to set the initial conditions $\otimes X_i(0)$, which also should be considered as the grey numbers $\otimes X_i(0) \in \left[\underline{X_i}(0), \overline{X_i}(0)\right]$. Most interesting is usually to obtain the equilibrium (steady state) solution, which is a grey vector $\lim_{k \to \infty} [\otimes X_i(k)] = \otimes X^* \in \left[\underline{X^*}, \overline{X^*}\right]$ or a limit cycle (strange attractor).

To determine the stability of the steady-state solution $\otimes X^*$, one can use the theorem [12], according to which the only equilibrium (steady state) solution of equation (3) ("the fixed point") exists if and only if

$$\left(\sum_{i,j=1}^{n} \overline{W}_{ij}^2\right)^{\frac{1}{2}} < H, \tag{7}$$

where the value of the positive constant H depends on the choice of activation function of the concepts: $H = 1$ for function (Eq. (4)); $H = 2$ for function (Eq. (5)); and $H = 4$ for function (Eq. (6)). In the case of negative connection, i.e., for $\underline{W}_{ij} < \overline{W}_{ij} < 0$, we also put in (Eq. (7)) the upper boundary $\overline{W}_{ij}$ of the grey number $\otimes W_{ij}$.

More detailed information on FGCM construction and their learning algorithms can be found in [5, 6, 9].

3. Risk assessment of IACS cybersecurity

Let us consider the task of assessment of IACS risk on the example of the automated system for collecting, storing, and processing the telemetric information (TMI) of the aviation equipment manufacturer. The current information on the state parameters of on-board aviation systems is continuously collected during the entire period of their operation by the ground services of technical maintenance. The detailed analysis of this information allows the subsequent making the right management decisions on the further operation and modification of on-board aviation systems. Therefore, the task of ensuring the integrity of the mentioned telemetric information under the conditions of possible impact of external and internal threats undoubtedly takes on particular significance.

The generalized structure of the studied territorially distributed automated information system (AIS), providing the collection, storage, and processing of TMI, is presented in **Figure 1**.

As the parts of AIS, the following subsystems (zones), combined according to the principle of the unity of functions performed and security requirements for their implementation, are identified:

1. The subsystem for collecting and storing the primary data at the service stations (Zone 1), which includes:

   Element 1—the client part of the SCADA system Web-base;

   Element 2—the server part of the SCADA system Web-base;

   Element 3—OPC UA client;

   Element 4—the temporary storage for accommodating the operative telemetry data accumulated at the object;

   Element 5—the server part of the accumulated data transmission to the storage of the aviation equipment manufacturer;

2. The core of the corporate information network (CIN) of the enterprise-manufacturer (Zone 2), where:

   Element 6—the client part for providing access to the server of the service station transferring the accumulated operational data of TMI to the enterprise-manufacturer's storage;

   Element 8—the workstations of administrator and service personnel of the CIN core of the enterprise-manufacturer;

3. TMI storage subsystem with fault tolerance functions (Zone 3), where:

   Element 7—the node of access to TMI data storage at the enterprise-manufacturer;

4. TMI data processing subsystem with the use of a hierarchy of mathematical models of aviation equipment (Zone 4);

5. Subsystem of support and implementation of business processes of the enterprise-manufacturer (Zone 5).

The corresponding subsystems (security zones) are interconnected (see **Figure 1**) with the aid of telecommunication channels (conducts).

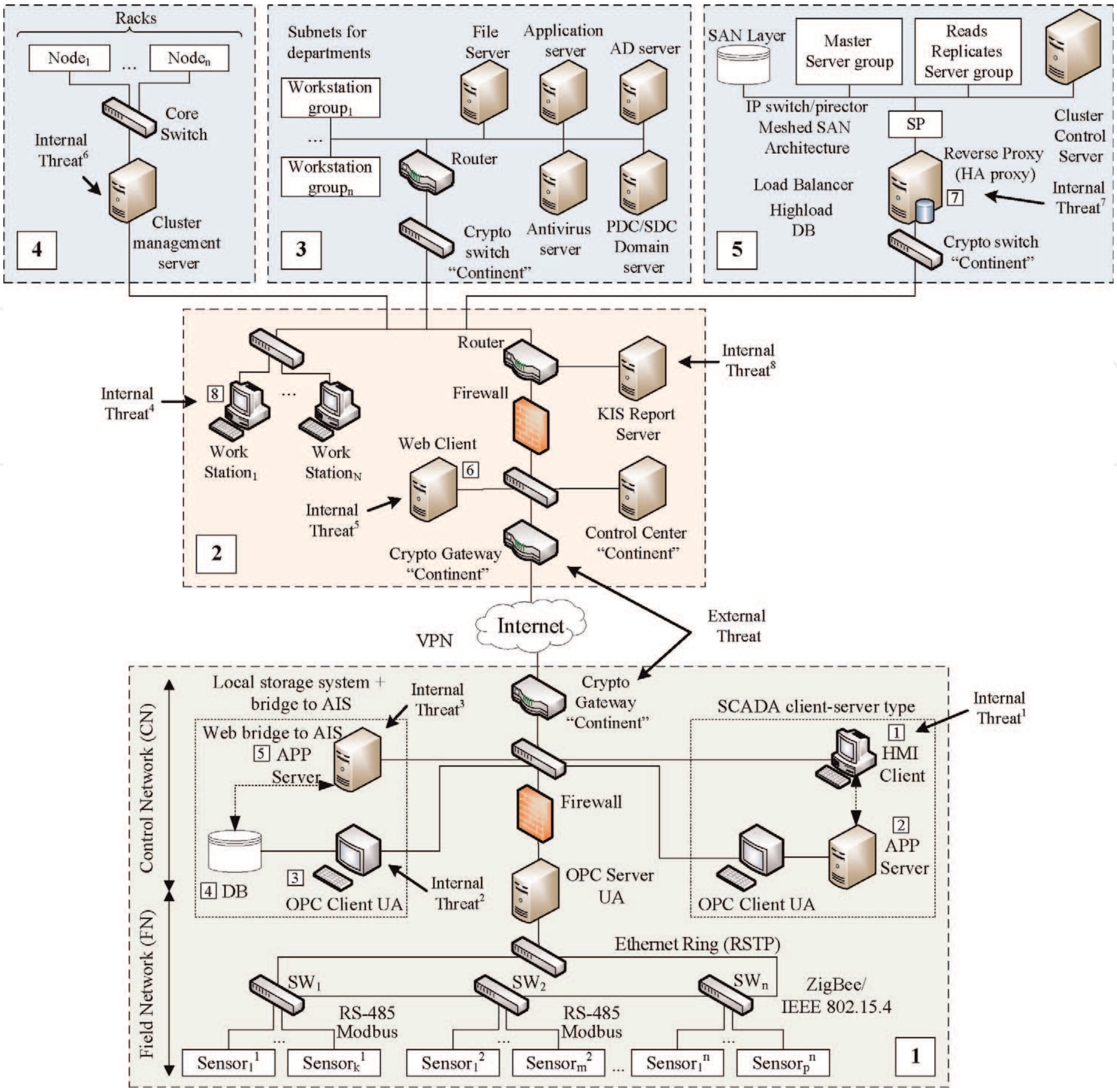


Figure 1.
The generalized structure of territorially distributed automated information system for the collection, storage, and processing of TMI. The corresponding subsystems (security zones) are interconnected with the aid of telecommunication channels (conducts).

Using FGCM as a tool for cognitive modeling, let us turn to the task of analyzing the risks associated with ensuring the TMI integrity in AIS considered above, taking into account the impact of possible external and internal threats to the system. The original (integrated) FGCM for assessing the risks of AIS, serving in this case as the AIS cognitive model of initial approximation (zero decomposition level), is presented in **Figure 2**.

The following descriptions are used in **Figure 2**: superscript ("*") denotes the affiliation of the concept C_p^* to integrated FGCM and subscript (p) denotes the number of the concept (**Table 1**).

The presence of the grey connection weights $\otimes \tilde{W}_{ij}$ indicates an uncertainty in the assessment of the mutual influence of main risk factors. The state variables of concepts $\otimes X_{T_1}^*$, $\otimes X_{T_2}^*$, $\otimes X_i$, $(i = 1, 2, \ldots, 5)$, $\otimes X_R^*$ represent the probabilities of occurrence of the enumerated events corresponding to the concepts $C_{T_1}^*$, $C_{T_2}^*$, C_1^*, …, C_5^*, C_R^*. Let us note that in this case we mean so-called subjective probabilities, reflecting the expert's point of view on the possibility of an event occurrence [13]. Taking into account that each of these events is a complex event consisting of a chain of consecutive elementary events, it is reasonable to decompose FGCM of AIS

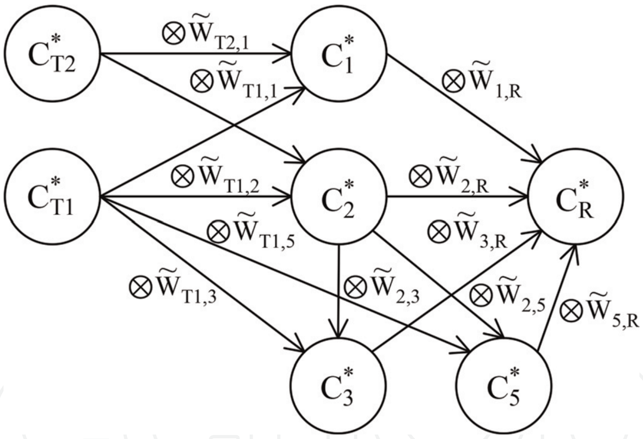


Figure 2.
Integrated FGCM for AIS risk assessment. $\otimes \tilde{W}_{ij}$—the grey connection weights indicate an uncertainty in the assessment of the mutual influence of main risk factors and C^*—concepts.

Concept	Concept name
$C^*_{T_1}$	Internal threat to TMI integrity (e.g., due to failures or erroneous actions of staff)
$C^*_{T_2}$	External threat to TMI integrity (e.g., due to attempts of unauthorized access from outside to information)
C^*_1	Modification of TMI data in Zone 1
C^*_2	Modification of TMI data in Zone 2
C^*_3	Modification of TMI data in Zone 3
C^*_5	Modification of TMI data in Zone 5
C^*_R	Potential damage caused by violation of TMI integrity in AIS

Table 1.
List of the concepts of the integrated FGCM.

shown in **Figure 2** as the set of FGCMs for separate concepts (AIS security zones containing targets objects for attack to TMI).

The first decomposition level of the original (integrated) FGCM is presented in **Figure 3**.

The following designations of the concepts are used in **Figure 3**: the superscript (q) of C_p^q indicates the belongings to the concept C_q of the integrated FGCM; and the subscript (p) is the number of the concepts in the FGCM of the first level of decomposition (**Table 2**).

Figure 4 shows the further decomposition level (the second level) for the concept C_1^*, allowing to make clearer the impact of the threats on the considered target concept.

On the scheme, the following designations of the concepts of FGCM second-level decomposition are used: the superscript (q) of the $C_r^{q,p}$ concept is the number of the concept (the parent concept of the zero decomposition level) of the original FGCM whose decomposition includes this element, the superscript index p is the number of the parent concept of the first level of decomposition, the subscript (r) is the number of the concept of the current level (**Table 3**).

The further decomposition of the third level allows us to go to the detailed FGCM, which allows us to take into account the influence of individual vulnerabilities on the potential violation of TMI integrity in the intermediate information processing elements.

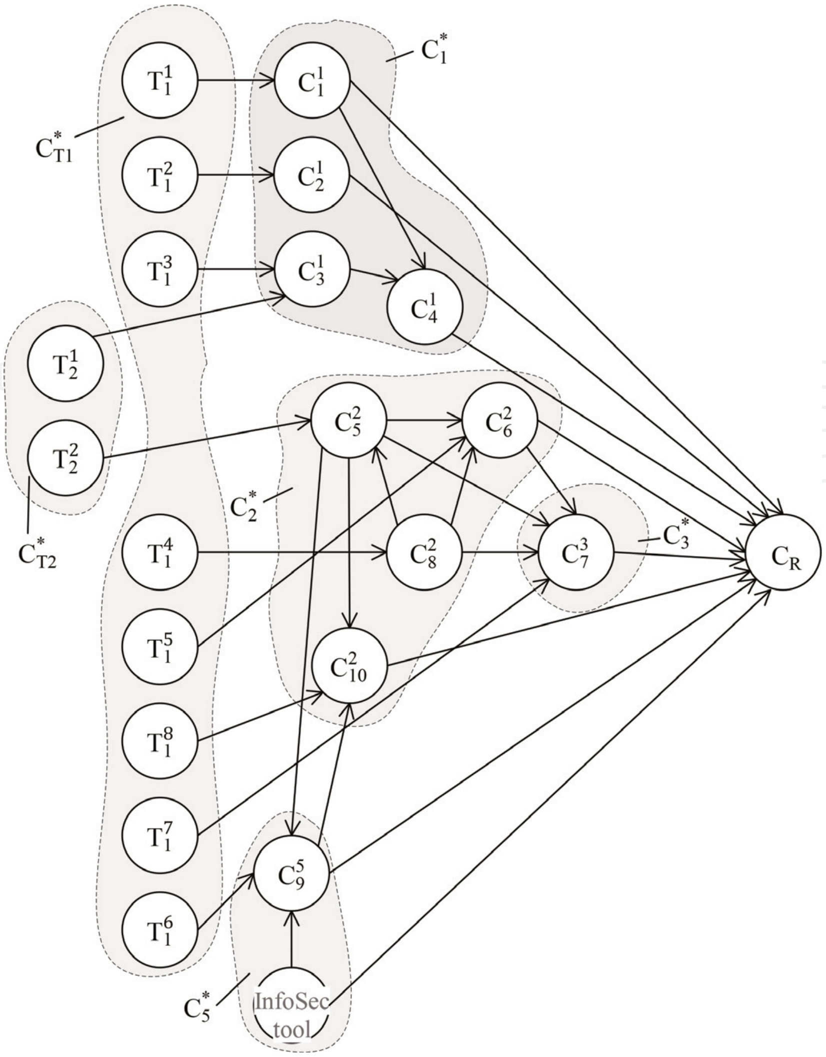


Figure 3.
The first level of FGCM decomposition to assess the AIS risks.

As for the concept $C_1^{1,1}$, characterizing the possibility to run in the browser of the client part of SCADA system on the base on Web technology (Zone 1), the corresponding decomposition can be represented as FGCM in **Figure 5**.

Here, the numbers 1–5 denote the following concepts:

1. the exploitation of the vulnerability of OS authorization system;

2. the exploitation of the vulnerability of SCADA Web client;

3. the exploitation of the vulnerability of OS browser for launching the client part of SCADA;

4. the exploitation of the vulnerability of access to OS memory;

5. the exploitation of the vulnerability of OPC UA client authorization system.

Similarly, it is possible to decompose the other concepts of original FGCM for the second decomposition level of Zone 1 presented in **Figure 4** (**Figures 6**–**9**, **Tables 4**–**6**). The corresponding FGCM, revealing the content of the concept $C_2^{1,1}$ (Zone 2), is shown in **Figure 6**.

Concept	Concept name	Parent concept
$T_1^1 - T_1^8$	Internal threats to the integrity of TMI (concept T_1^* decomposition on the block diagram of AIS, **Figure 1**, i.e., the points of potential realization of the threat to TMI integrity by the internal subject of the system)	T_1^*
T_2^1, T_2^2	External threats to TMI integrity (concept T_2^* decomposition)	T_2^*
C_1^1	Access to TMI in the client-server SCADA Web-base before adding to the database of TMI operational storage	C_1^* (Zone 1)
C_2^1	Access to the database of operative TMI data storage	
C_3^1	Access to the network equipment	
C_4^1	Access to the module of Web server sending TMI data in the long-term storage of the enterprise-manufacturer	
C_5^2	Access to the network infrastructure	C_2^* (Zone 2)
C_6^2	Access to the Web client module that implements receiving TMI at the enterprise-manufacturer from remote service stations	
C_8^2	Unauthorized access to workstation (node 8 in **Figure 1**) of the core of CIN of the enterprise-manufacturer	
C_{10}^2	Access to the server of equipment status reports generated for users of Zone 4	
C_7^3	Access to TMI in the long-term storage	C_3^* (Zone 3)
C_9^5	Access to computing cluster management server of Zone 5	C_5^* (Zone 5)
IST^5	TMI integrity control model	

Table 2.
List of the first level decomposition concepts of the FGCM.

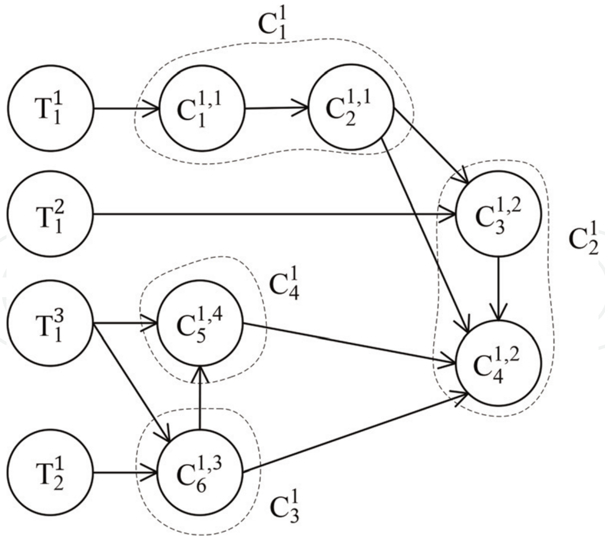


Figure 4.
The second level of FGCM decomposition for assessing AIS risk in Zone 1.

Consider the numerical example of risk assessment for the concept $C_1^{1,\,1}$ (**Figure 5**).

Let us assume that while choosing the grey values of FGCM weights, it is necessary to focus on a certain fuzzy scale, which determines the strength of the connections between different concepts (see, e.g., **Table 7**).

Let us further assume that the expert estimated the values of FGCM connections weights in **Figure 5** as follows (**Table 8**).

Concept	Concept name	Parent concept
$C_1^{1,1}$	Access to HMI client SCADA	C_1^1
$C_2^{1,1}$	Access to operative TMI data on the client-server part of the SCADA before entering in the operative storage	
$C_3^{1,2}$	Access to the client to interact with the OPC UA server	C_2^1
$C_4^{1,2}$	Access to the database of operative TMI storage data	

Table 3.
List of second-level decomposition concepts for Zone 1.

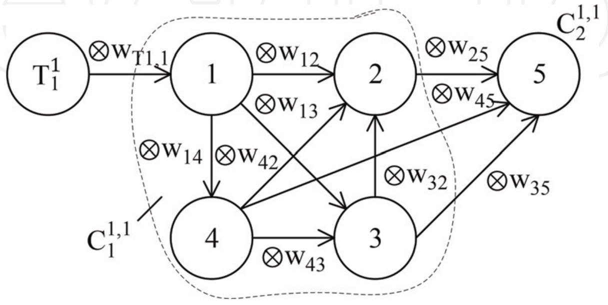


Figure 5.
The third level of FGCM decomposition—the concept $C_1^{1,1}$.

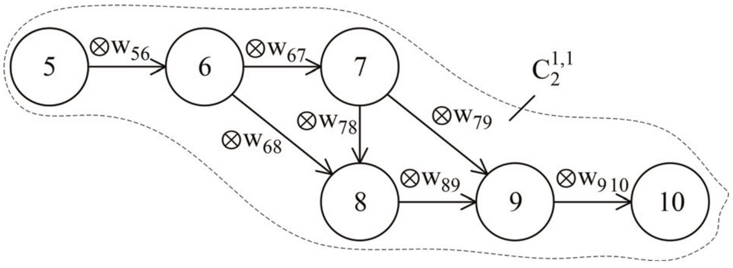


Figure 6.
Decomposition of the concept $C_2^{1,1}$ of FGCM for AIS risk assessment (Zone 1)

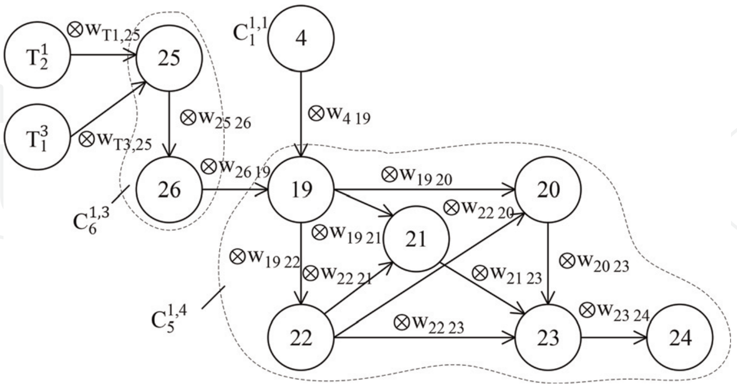


Figure 7.
Decomposition of the concepts $C_6^{1,3}$ and $C_5^{1,4}$ of the second level of FGCM decomposition

Let us take a bipolar sigmoid (5) here as an activation function $f(\bullet)$ for the concepts 1–5. Checking condition (7) for the data presented in **Table 2** shows that

$$\left(\sum_{i,j=1}^{5}\overline{W}_{ij}^{2}\right)^{\frac{1}{2}} = \sqrt{2,76} = 1.66 < 2, \tag{8}$$

i.e., the steady-states of FGCM will be stable.

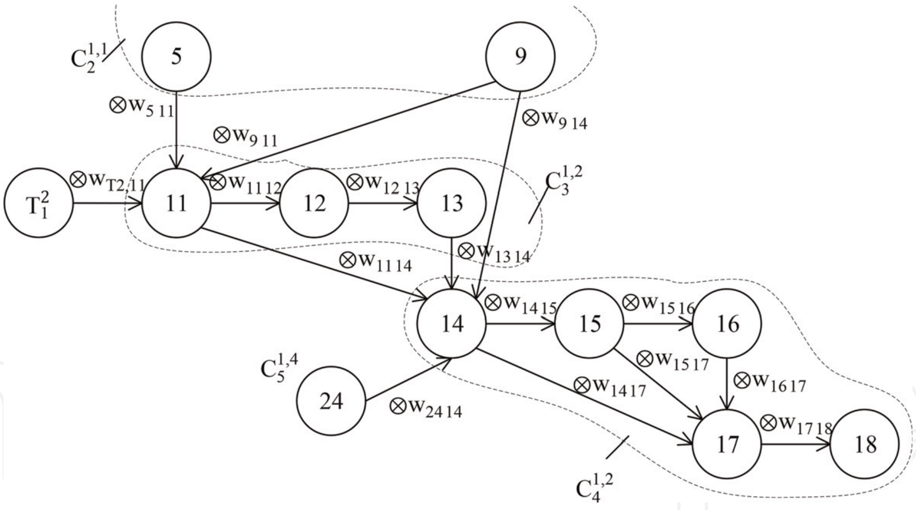
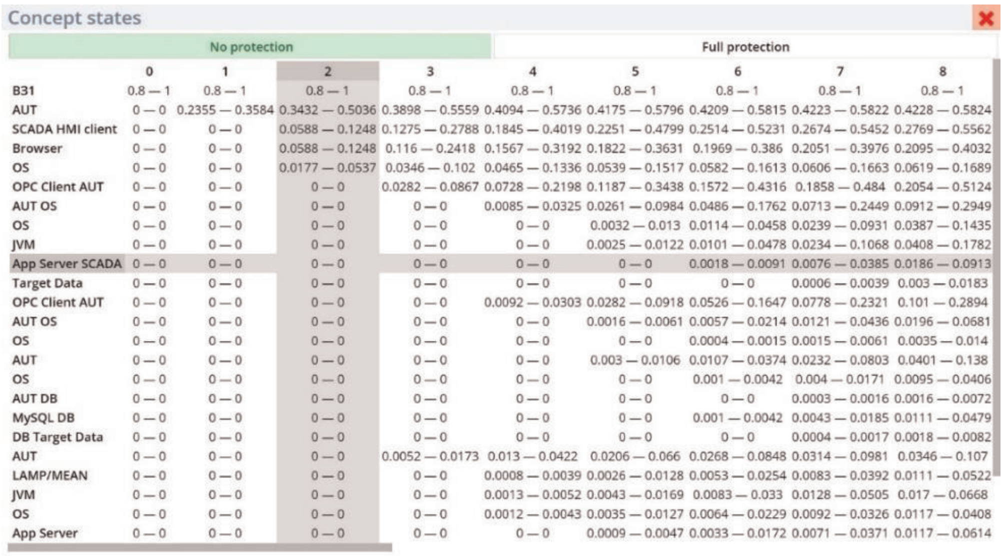


Figure 8.
Decomposition of the concepts $C_3^{1,2}$ and $C_4^{1,2}$ of FGCM for AIS risk assessment


Concept states

	No protection				Full protection				
	0	1	2	3	4	5	6	7	8
B31	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1	0.8 — 1
AUT	0 — 0	0.2355 — 0.3584	0.3432 — 0.5036	0.3898 — 0.5559	0.4094 — 0.5736	0.4175 — 0.5796	0.4209 — 0.5815	0.4223 — 0.5822	0.4228 — 0.5824
SCADA HMI client	0 — 0	0 — 0	0.0588 — 0.1248	0.1275 — 0.2788	0.1845 — 0.4019	0.2251 — 0.4799	0.2514 — 0.5231	0.2674 — 0.5452	0.2769 — 0.5562
Browser	0 — 0	0 — 0	0.0588 — 0.1248	0.116 — 0.2418	0.1567 — 0.3192	0.1822 — 0.3631	0.1969 — 0.386	0.2051 — 0.3976	0.2095 — 0.4032
OS	0 — 0	0 — 0	0.0177 — 0.0537	0.0346 — 0.102	0.0465 — 0.1336	0.0539 — 0.1517	0.0582 — 0.1613	0.0606 — 0.1663	0.0619 — 0.1689
OPC Client AUT	0 — 0	0 — 0	0 — 0	0.0282 — 0.0867	0.0728 — 0.2198	0.1187 — 0.3438	0.1572 — 0.4316	0.1858 — 0.484	0.2054 — 0.5124
AUT OS	0 — 0	0 — 0	0 — 0	0 — 0	0.0085 — 0.0325	0.0261 — 0.0984	0.0486 — 0.1762	0.0713 — 0.2449	0.0912 — 0.2949
OS	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.0032 — 0.013	0.0114 — 0.0458	0.0239 — 0.0931	0.0387 — 0.1435
JVM	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.0025 — 0.0122	0.0101 — 0.0478	0.0234 — 0.1068	0.0408 — 0.1782
App Server SCADA	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.0018 — 0.0091	0.0076 — 0.0385	0.0186 — 0.0913
Target Data	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.0006 — 0.0039	0.003 — 0.0183
OPC Client AUT	0 — 0	0 — 0	0 — 0	0 — 0	0.0092 — 0.0303	0.0282 — 0.0918	0.0526 — 0.1647	0.0778 — 0.2321	0.101 — 0.2894
AUT OS	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.0016 — 0.0061	0.0057 — 0.0214	0.0121 — 0.0436	0.0196 — 0.0681
OS	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.0004 — 0.0015	0.0015 — 0.0061	0.0035 — 0.014
AUT	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.003 — 0.0106	0.0107 — 0.0374	0.0232 — 0.0803	0.0401 — 0.138
OS	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.001 — 0.0042	0.004 — 0.0171	0.0095 — 0.0406
AUT DB	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.0003 — 0.0016	0.0016 — 0.0072
MySQL DB	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.001 — 0.0042	0.0043 — 0.0185	0.0111 — 0.0479
DB Target Data	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.0004 — 0.0017	0.0018 — 0.0082
AUT	0 — 0	0 — 0	0 — 0	0.0052 — 0.0173	0.013 — 0.0422	0.0206 — 0.066	0.0268 — 0.0848	0.0314 — 0.0981	0.0346 — 0.107
LAMP/MEAN	0 — 0	0 — 0	0 — 0	0 — 0	0.0008 — 0.0039	0.0026 — 0.0128	0.0053 — 0.0254	0.0083 — 0.0392	0.0111 — 0.0522
JVM	0 — 0	0 — 0	0 — 0	0 — 0	0.0013 — 0.0052	0.0043 — 0.0169	0.0083 — 0.033	0.0128 — 0.0505	0.017 — 0.0668
OS	0 — 0	0 — 0	0 — 0	0 — 0	0.0012 — 0.0043	0.0035 — 0.0127	0.0064 — 0.0229	0.0092 — 0.0326	0.0117 — 0.0408
App Server	0 — 0	0 — 0	0 — 0	0 — 0	0 — 0	0.0009 — 0.0047	0.0033 — 0.0172	0.0071 — 0.0371	0.0117 — 0.0614

Figure 9.
FGCM concepts states for risk assessment of Zone 1 (the change in the state of concepts over time and the final states of the target concepts of the FGCM, software window form).

Concept	Concept name	Parent concept
6	Exploitation of the vulnerability of authorization system of the primary OS user	$C_2^{1,1}$
7	Exploitation of the vulnerability of access to operating system memory	
8	Exploitation of the vulnerability of Java virtual machine	
9	Exploitation of the vulnerability of system software of application server for running the SCADA server Web application	
10	The target concept of access to operative TMI data, which can be modified before adding to the database on the nodes of SCADA client-server type	

Table 4.
List of the concepts of the third decomposition level for AIS risks assessment of Zone 1.

Using for calculation the "Cognitive Map Constructor" tool, which is described more detailed in the next section of this chapter, we will estimate the change in the upper and lower boundaries of the state variable X_5 over time $k = 1, 2, 3, \ldots$

Concept	Concept name	Parent concept
19	Exploitation of the vulnerability of authorization system of the main OS user	$C_5^{1,4}$
20	Exploitation of the vulnerability of system software implementing work of Apache Web application server, MySQL DBMS, PHP runtime frameworks to support interactive Web pages	
21	Exploitation of the vulnerability of OS memory access	
22	Exploitation of the vulnerability of Java Virtual Machine Memory Access	
23	Exploitation of the vulnerability of Application Server Software	
24	The target concept of unauthorized launching of the module for access to the database of operative storage of TMI at service stations	
25	Exploitation of the vulnerability of authorization system of the main OS user	$C_6^{1,3}$
26	Exploitation of the vulnerability of access to operating system memory	

Table 5.
List of the concepts of the third decomposition level of Zone 1.

Concept	Concept name	Parent concept
14	Exploitation of the vulnerability of authorization system of the main OS user	$C_4^{1,2}$
15	Exploitation of the vulnerability of OS memory access	
16	Exploitation of the vulnerability of authorization system of the main DBMS user	
17	Exploitation of the vulnerability of DBMS memory access	
18	The target concept of unauthorized modification of TMI operative data TMI stored in the database	
11	Exploitation of the vulnerability of authorization system of the client part of OPC Client UA software	$C_3^{1,2}$
12	Exploitation of the vulnerability of authorization system of the main OS user	
13	Exploitation of the vulnerability of OS memory access	

Table 6.
List of the concepts of the third level of FGCM decomposition of Zone 1.

Linguistic meaning of connection strength	Numeric range
Does not affect	0
Very weak	(0; 0.15]
Weak	(0.15; 0.35]
Average	(0.35; 0.6]
Strong	(0.6; 0.85]
Very strong	(0.85; 1]

Table 7.
Evaluation of the strength of communication between concepts.

(**Tables 9** and **10**). The state of the input concept C_{T_1} is defined here as $\otimes X_{T_1}(k) = [0.8;1]$ for all $= 0, 1, 2, \ldots$; the initial conditions for other state variables $\otimes X_1(0) \div \otimes X_5(0)$ are assumed to be zero, i.e., equal to [0;0].

As a result, the steady-state value of the grey state vector $\otimes X$ for FGCM presented in **Figure 6**, i.e., for the concept $C_1^{1,1}$ decomposition is found as

$$\otimes X = \{[0,8;1],[0,43;0,58],[0,28;0,55],[0,20;0,40],[0,06;0,16],[0,24;0,53]\},$$

and the final value for the target concept state is determined by the grey number $\otimes X_5 \in [0,24;0,53]$.

Consider the state of the target concept C_R (**Figure 2**)—the damage caused by the potential violation of TMI integrity in the AIS—after clarifying all weights by the level of decomposition of the original FGCM. Let us assume that the active

Connection weight	The value of the connection weight	Greyness (scatter of assessment)
W_{T_11}	[0.6; 0.75]	0.075
W_{12}	[0.5; 0.7]	0.1
W_{13}	[0.5; 0.7]	0.1
W_{14}	[0.15; 0.3]	0.075
W_{25}	[0.55; 0.65]	0.05
W_{32}	[0.35; 0.55]	0.1
W_{35}	[0.55; 0.65]	0.05
W_{42}	[0.3; 0.5]	0.1
W_{43}	[0.15; 0.3]	0.075
W_{45}	[0.2; 0.45]	0.125

Table 8.
The values of communications FGCM weights.

k	1	2	3	4	5	6	7	8
$\overline{X}_i$								
$\overline{X}_1$	0.36	0.50	0.55	0.57	0.58	0.58	0.58	0.58
$\overline{X}_2$	0	0.125	0.28	0.40	0.48	0.52	0.54	0.55
$\overline{X}_3$	0	0.125	0.24	0.32	0.36	0.38	0.39	0.40
$\overline{X}_4$	0	0.054	0.10	0.13	0.15	0.16	0.16	0.16
$\overline{X}_5$	0	0	0.093	0.23	0.36	0.45	0.50	0.53

Table 9.
Upper boundaries of concept state estimates

k	1	2	3	4	5	6	7	8
$\underline{X}_i$								
$\underline{X}_1$	0.24	0.34	0.39	0.41	0.43	0.43	0.43	0.43
$\underline{X}_2$	0	0.059	0.13	0.18	0.22	0.25	0.27	0.28
$\underline{X}_3$	0	0.059	0.115	0.16	0.18	0.19	0.20	0.20
$\underline{X}_4$	0	0.018	0.034	0.046	0.052	0.058	0.06	0.06
$\underline{X}_5$	0	0	0.034	0.087	0.14	0.18	0.21	0.24

Table 10.
Lower boundaries of concept state estimates.

threat is the internal threat of violation of the integrity of TMI, the value of which is determined by a grey number $\otimes X^*_{T_1} \in [0, 6;0, 95]$.

Risk assessment because of violation of the integrity of TMI information is defined as $\otimes X^*_R \big|_A \in [0.19;0.28]$.

To reduce the potential damage from the violation of TMI integrity, a monitoring system, deployed as a protected container in Zone 5, is used. In **Figure 3**, this information protection tool is designated as a TMI integrity monitoring model—concept IST^5. The protected container ensures the continuous operation of the TMI integrity monitoring system, which implements online and offline analysis of operational data and data collected in the repository (Zone 3).

The concept of TMI integrity monitoring system as a whole has some peculiarities:

- Simulated parameters of the aviation engine operation and TMI can be presented in the form of multidimensional technological time series;

- Monitoring the TMI integrity is based on the analysis of the consistency of the behavior of parameters obtained by using the model of complex technical object, and taken from the on-board aircraft systems;

- The output of the monitoring system is the evaluation of conditional probability of the events of data integrity violation events.

Risk value estimate due to violation of TMI information integrity after applying the tool based on the integrity monitoring model is $\otimes X^*_R \big|_A \in [0.07;0.15]$.

Due to the significant amount of computation when working with FGCM containing a large number of concepts, it was necessary to develop a software tool to automate cognitive modeling with use of FGCM. The change in the state of concepts over time and the final states of the target concepts of the FGCM, calculated in the developed software tool, are presented in **Figure 9**.

4. Automation of risk analysis and management on the base of cognitive modeling technology

To improve an efficiency of risk analysis and management with use of FGCM, the special software tool “Cognitive Map Constructor” was developed. This software allows us to build and edit FGCM, use them to carry out the security risk analysis, and justify the choice of the necessary countermeasures from the given user-specified set. As a result, a diagram of risk assessment is built under various scenarios of countermeasures’ implementation and threats’ realization.

Besides supporting the FGCM with the installation of connections weights in the form of the upper and lower boundaries, the software allows us the use of linguistic terms of fuzzy logic, as well as setting the weights in the form of “white” crisp numbers. The software has the interface implemented in HTML using CSS, which allows displaying the FGCM and all the necessary accompanying information by the concepts and connections, and also is able to work on any graphical operating system that has a current Web browser.

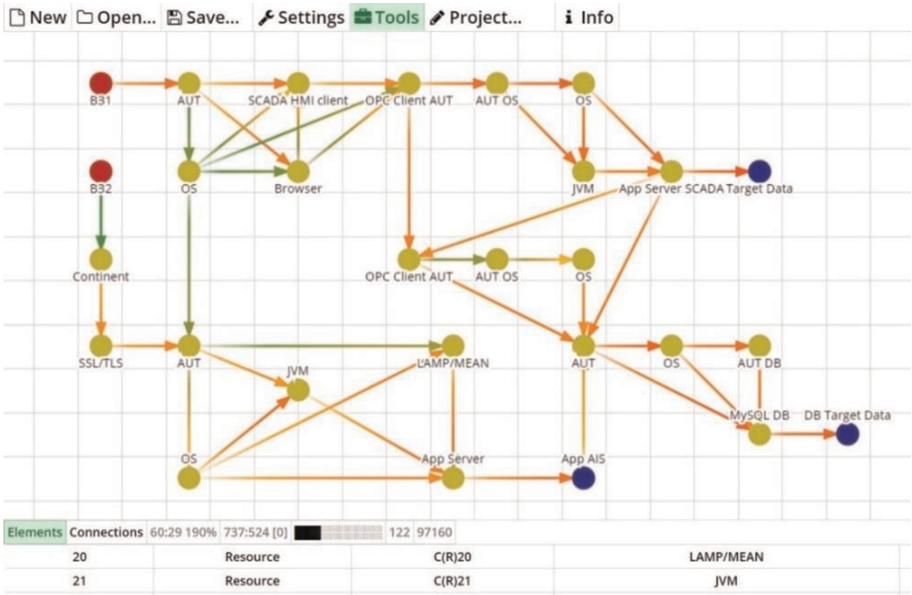
There are five kinds of concepts which are used in FGCM: threats, information assets, intermediate concepts, targets, and countermeasures, which can be marked by different colors for convenience and clarity.

The set of the options depends on the type of the concept, but in most cases its name is specified with description, as well as its current state. In the case when the weights of all connections, pointing to the concept, are assumed to be equal, one can mark the option "Imposed weight" and set the desired value. For countermeasures, it is permissible to indicate which of existing countermeasure it is, that allows realizing situations when one countermeasure acts on several connections at once.

To establish the relationships between the concepts, it is necessary to click on the button "Placement" of the action group "Connections" in the tool window. After that, the connections are located by pressing consecutively on the initial and final element. The located countermeasures and initial states of the concepts can be adjusted and combined, creating the different scenarios that allow us to compare the effectiveness of countermeasures.

Figures 10 and **11** show the FGCM risk estimates built in the "Cognitive Map Constructor."

Thus, the developed software "Cognitive Map Constructor" allows evaluating the effectiveness of the use of the TMI integrity monitoring system in the protection of telemetric information from the effects of external and internal threats.



20	Resource	C(R)20	LAMP/MEAN
21	Resource	C(R)21	JVM

Figure 10.
FGCM for risk assessment of data collection and storage subsystem at the service stations (Zone 1) (software window form).

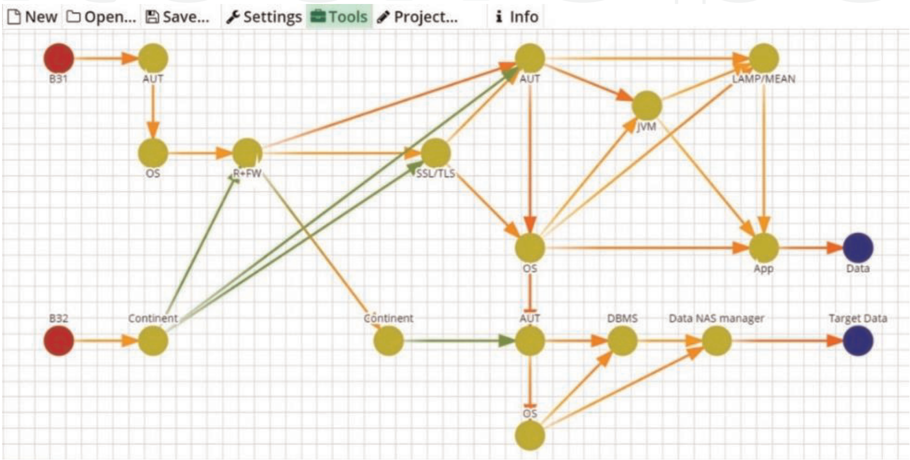


Figure 11.
FGCM for risk assessment in the core of the CIN (Zone 2) and TMI (software window form).

5. Conclusions

A promising way to solve the problem of assessing the cybersecurity risks of industrial automated systems is to model the threats realization scenarios using the tools of topological analysis of the system security and cognitive modeling with the aid of Fuzzy Grey Cognitive Maps.

At the basis of this approach, the construction of original FGCM is proposed to assess the risk of automated control system with the following decomposition of FGCM into the number of cognitive maps of the next level of detail (the same as it is done in IDEF0 Functional Modeling technology). The features of construction of this procedure are discussed in this chapter in relation to the task of ensuring the telemetry information integrity in the industrial automated system for collecting, storing, and processing information on the conditions of on-board aviation systems. It is shown that the use of FGCM allows us to obtain more reliable estimates of security risk factors with account of the possible variations of the available actual data and expert opinions.

To automate the proposed risk assessment procedure in the considered system for collecting, storing, and processing telemetry information with use of FGCM, the software tool “Cognitive Map Constructor” was developed, which can be used for identifying the most dangerous vulnerabilities in the system and evaluating the effectiveness of various measures (countermeasures) realization for telemetric information protection from the impact of external and internal threats.

Acknowledgements

The reported study was funded by RFBR according to the research Project No. 18-00-00238 “Decision support methods and models for innovative project management based on knowledge engineering.”

Author details

Vladimir I. Vasilyev*, Alexey M. Vulfin and Liliya R. Chernyakhovskaya
Ufa State Aviation Technical University, Ufa, Russian Federation

*Address all correspondence to: vasilyev@ugatu.ac.ru

References

[1] WannaCry. Threat Landscape for Industrial Automation Systems in H2 2017 [Internet]. Available from: https://ics-cert.kaspersky.com/tag/wannacry/ [Accessed: May 10, 2019]

[2] Threat Landscape for Industrial Automation Systems. H2 2018 [Internet]. Available from: https://ics-cert.kaspersky.com/reports/2019/03/27 [Accessed: May 10, 2019]

[3] Cyber Security Standards [Internet]. Available from: https://en.wikipedia.org/wiki/Cyber_security_standards [Accessed: May 10, 2019]

[4] Byres E. Using ISA/IEC 62443 Standards to Improve Control System Security. Tofino Security White Paper. Version 1.2. Deutschland GmbH: Tofino Security, a Belden Brand, Belden Inc.; 2014

[5] Salmeron JL. Modelling grey uncertainty with fuzzy grey cognitive maps. Expert Systems with Applications. 2010;**37**(12):7581-7588

[6] Salmeron JL, Papageorgiou EI. Chapter 14: Using Fuzzy Grey Cognitive maps for industrial processes control. In: Fuzzy Cognitive Maps for Applied Sciences and Engineering: From Foundations to Extensions and Learning Algorithms. Intelligent Systems Reference Library. Vol. 54. Berlin/Heidelberg: Springer; 2014

[7] Salmeron JL. Fuzzy grey cognitive maps-based intelligent security system. In: 2015 IEEE International Conference on Grey Systems and Intelligent Services (GSIS); August 12–20, 2015; Leicester, UK; 2015. pp. 29-32

[8] Shishkin VM, Savkov SV. The method of interval estimation of risk-analysis system. In: Proceedings of the Second International Conference on Security of Information and Networks (SIN'09); October 6–10, 2009; Famagusta, North Cyprus; 2009. pp. 3-7

[9] Hajek P, Prochazka O. Interval-valued fuzzy cognitive maps with genetic learning for predicting corporate financial distress. Univerzitet u Nišu. 2018;**32**(5):1657-1662

[10] Vasilyev VI, Vulfin AM, Guzairov MB, Kirillova AD. Interval evaluation of information risk with the aid of fuzzy grey cognitive maps. Information Technology. 2018;**24**(10): 657-664

[11] Harmati IA, Koczy LT. On the Convergence of Fuzzy Grey Cognitive Maps. Information Technology, Systems Research, and Computational Physics. Springer Verlag; 2018. pp. 74-84

[12] Zhang JY, Liu ZQ, Zhou S. Quotient FCMs—A decomposition theory for fuzzy cognitive maps. IEEE Transactions on Fuzzy Systems. 2003; **11**(5):593-604

[13] D'Agostini C. Role and meaning of subjective probability: Some comments on common misconceptions. AIP Conference Proceedings. 2001;**568**(1): 23-30. Available from: https://aip.scitation.org/doi/pdf [Accessed: May 10, 2019]