DE GRUYTER OPEN
Foundations of Management, Vol. 10 (2018), ISSN 2080-7279
DOI: 10.2478/fman-2018-0014

SECURITY IN TOPOLOGICAL, FUNCTIONAL AND SEMIOTIC TERMS

Tadeusz KRUPA*, Teresa OSTROWSKA**
Warsaw University of Technology, Faculty of Management, Warsaw, POLAND
* e-mail: tadeusz.krupa@pw.edu.pl
**e-mail: teresa.ostrowska@pw.edu.pl

Abstract: The article is devoted to the modeling of object structures in sequences of event processes characteristic of critical infrastructure (CI) objects arising in emergency situations. The identification of risky sequences of events is a key issue carried out in topological, functional and semiotic terms. The topological approach includes flat, hierarchical and hypergraph – it is possible by means of transformations of equivalent models of the event network through its simplification to the form of a hypothesis or towards the desired functionality. The functionality approach covers theorizing and plural problems in the processes of the creation of a priori and aposteriorical errors of multiplication and synthesis on the basis of also incorrect graphical models of functioning. The semiotic approach captures combinatorically related functional and structural errors, which are impossible to identify and remove by means of arithmetic-logical tests. Currently, this is possible only on the basis of the paradigm of the characterization theory, which guarantees a semantic relationship between the correctness of the functioning and the structure of the analyzed versus the synthesized object of research.

Keywords: critical infrastructure, emergency situations, transformations of events networks, functionality network, graph models of functioning, semiotic approach, functional and structural errors, characterization theory.

JEL: C13, M19, O22.

1 Introduction[1]

Universally understood security and its defense can be prepared and implemented in an infinite number of ways. The approach presented in this publication does not give one specific answer because, according to the authors, a simple answer to such a question does not exist. In this case, the natural question becomes – can security and its effective defense be built in an integral way and on what theoretical grounds?

Our article is modeled on the work of the Faculty of Management at the Warsaw University of Technology, which is devoted to the broad and unfortunately still current problem of risk management and business continuity safety (Zawiła-Niedźwiecki, 2013, 2014). It reaches the mathematical and universal terminology in terms of topological (but not structural), functional (but not functional) issues and semiotic issues (in terms of syntactic, semantic and pragmatic categories). An additional pretext for the creation of this work is the growing issues of defense and security in the common understanding of the European Union's societies – their diverse scope provoked us to unusual thoughts and actions (Jajuga, 2007; Kieżun, 2018; Maj and Krupa, 2010).

The approach proposed in our article is a methodological experiment based on the previous achievements of the Warsaw University of Technology Management Department under project ID 193751 – devoted to the methodology for estimating the risk of a crisis situation, including the destruction or disruption of critical infrastructure (CI)[2] – adapted to

[1] The subjects of interest of the authors of this paper are selected aspects of the development project entitled: "A highly specialized platform supporting civilian and rescue planning in the public administration of the Republic of Poland and organizational units of the National Fire and Rescue System" (as part of competition 7/2015 NCBiR).

[2] CI – Critical Infrastructure in accordance with the Act of April 26, 2007 Journal of Laws of 2013 item 1166 on Crisis Management Art. 3 points CI, as amended, includes the following resources and systems: energy supply, energy raw materials and fuels; communications; ICT networks; financial; food supply; water supply; health protection; transport; rescue; ensuring the continuity of public administration; production, storage, storage and use of chemical and radioactive substances, including pipelines of hazardous substances; resources of culture and national heritage.

the requirements of the planning and program documents developed for the needs of the crisis management system of the Republic of Poland[3].

The essence of the conducted methodological experiment is the integral linking of the phenomenon of security in one of the following three groups of categories of concepts:

- in terms of topological flat, hierarchical and hypergraph models (Domański, Kotarba and Krupa, 2014; Ficoń, 2007; Koziej, 2009; Ostrowska, Krupa and Wiśniewski, 2015) – section 2,
- in terms of discrete functional events occurring in proper buffers (PB[4]) in the form of Cartesian products of graphs of functional events – section 3, and
- in terms of semiotic set theory and a number of memory models of PB functional events transformed into semantic forms of PB functional memory models, and as the complexity of the situations increases – transformed into structural forms of PB potential memory written on the paradigm of the characterization theory – in the form of Hasse diagrams[5] - section 4.

2 Security in topological terms

Security in topological categories is nothing but actions, the aim of which is the homeomorphic behavior of all the invaluable elements of the subject's security. The security has its price, just as there is the not always well-used concept of security at all costs, which the defending subject is willing to incur. Security also has its rich literature, as well as many other historically significant events and key concepts, which in addition to topology, include functionality and semiotics (Homenda, 2009; Kulińska, 2016; Pogorzelski, 1999).

We have included flat graph models, hierarchical models and hypergraph models to interpret the topological understanding of security (Krupa, 2009; Krupa and Ostrowska, 2007). The latter, by definition, aspires to the most general. For topology in the security sense, it is most appropriate to maintain the optimal integrity of functional-structural compounds – which, in the sense of the engineering of action, is tantamount to the basic principle of characterization, or in its developed form, to the character of the characterization theory.

It is worth noting here that models of flat and hierarchical decision problems originate from the morphological analysis of related decision areas proposed in 1948 by F. Zwicky[6].

2.1 Topological flat models

Fig. 1, Fig. 2 and Fig. 3 show topological flat graph models. Objects or their potential buffers functioning in the world of flat models take the form of the vertices (nodes) of a graph. It should be noted that the $B^{R \to S}$ buffer combines two different R and S objects in a manner that ensures the transfer of functional potentials from object R to object S (which is marked as R→S), while the $B^{R \to R}$ buffer internally connects the same object. Of course, an external connection of the same object is also possible.

Objects cannot connect directly to each other without the intermediation of buffers, and so:

- the universal rule "two objects and only one potential buffer" applies (Fig. 2); the object deciding about the transfer of functionality potential (TFP) is determined by the object having at least one potential buffer (PB) connected to the receiving

[3] Crisis management system – Skomra, W., ed. (2015), Methodology of risk assessment for the needs of the crisis management system of the Republic of Poland.

[4] PB – potential buffer – a virtual unit designed to support the transfer of functional potential (TFP) between objects (giving and receiving) that couples in pairs: an object giving a digitized functional potential p# with values of 0#, 1#, ..., 4# (in conversion to %); PB accumulates in its memory data the potential of the entire critical infrastructure system or selected objects of its infrastructure; each PB is assigned to only one distinguished class (feature) of the object; for example – an external or internal PB connected to an object is a carrier of a specific internal or external functionality – e.g. a 100-liter fuel tank filled with 100% of fuel can, as an object, realize a maximum functionality of 4#, if it does not contain other objects with distinguished and supported functionalities.

[5] Hasse diagram – a simple display using a partially ordered set of graphs.

[6] The creator of the basics of morphological analysis and the discoverer of neutron stars, the Swiss astrophysicist F. Zwicky (1898 - 1974), treated morphological research as "the perception of a reality image in which all the more important structural relations between objects, phenomena, ideas and activities would be taken into account ..."

object (in Fig. 2, the decisive object is the R and $B^{R \to S}$ object as PB),

- an example of the configuration of the links that associate internal objects (S and U) outside their external object R is shown in Fig. 3,
- object T in Fig. 3, although it has 3 PB, cannot initiate TFP, because there are no attached objects to PB – it can instead collect TFP, if such a situation occurs,
- the TFP sent to the site cannot be greater than the TFP allowed for the given facility.

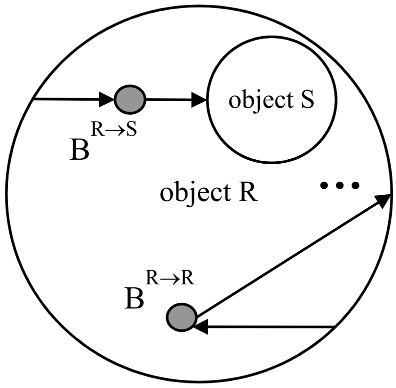

Figure 1. Objects - external R, internal S, their connecting channels and internal potential buffers $B^{R \to R}$ and $B^{R \to S}$ (*Source:* own elaboration)

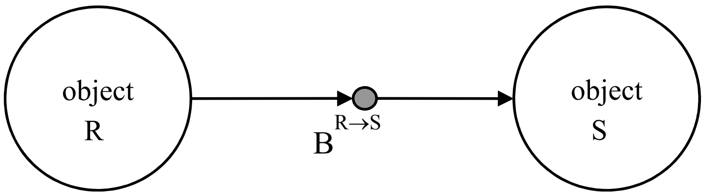

Figure 2. Principle: two feeding and receiving facilities and only one potential buffer $PB^{R \to S}$ (An exception to this rule is when the receiving object is also an issuing object) (*Source:* own elaboration)

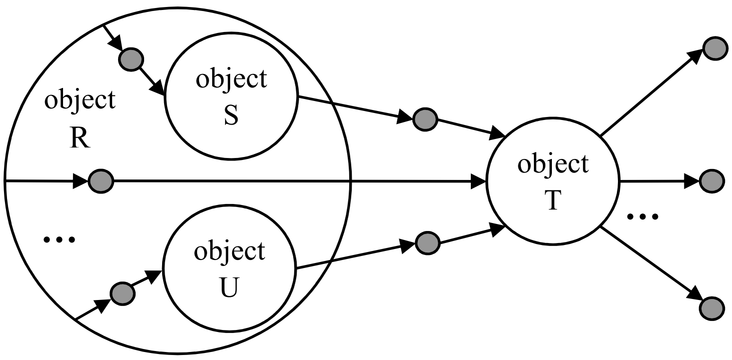

Figure 3. An example of the configuration of the connections that aggregate internal CI objects (*Source:* own elaboration)

Different constraints can be imposed on the channel connections of objects and buffers in the CI system, in particular:

- each object from the inside of it may correspond to one or more PBs that connect the internal channels as well as other internal objects; the analogous situation can also apply to any external object – one or more PBs connect external objects with channels – and so in Fig. 1, the $B^{R \to S}$ buffer attaches the S object located in the R object, and in Fig. 2, the $B^{R \to S}$ buffer connects an S object that is outside the R object,

- buffers cannot connect directly to each other without the intermediation of objects,
- objects cannot connect directly to each other without a buffer intervention.

The graphical language of symbolic objects and buffers with decision functionality assigned to objects and the operational (transmission) functionality assigned to buffers, with appropriate contextual constraints, enables the building of precise schemes with high homeomorphic transformation capabilities and a wide field of applications.

2.2 Topological hierarchical models

Containing objects can be treated as flat and as hierarchical (multilayered) if their boundary lines do not cross and do not meet.

Fig. 4 presents a situation where the O^X object is a functional coordinator of six potential buffers. Coordination can be done indirectly, either by means of three indirect $PB^{X \to O}$, or by means of two direct (currently inactive) PBs.

PBs and O^X, O^Y, O^Z objects presented in Fig. 4 have the following interpretation:

- buffers connecting internal objects:
  $B_1{}^X$, $B_2{}^X$, $B_m{}^X$ are PBs in the O^X object,
  $B_1{}^Y$, $B_n{}^Y$ are PBs in the O^Y object,
  $B_1{}^Z$ is PB in the O^Z object,
- buffers connecting external objects:
  $B_p{}^X$, $B_r{}^X$ are PBs in the O^X object.

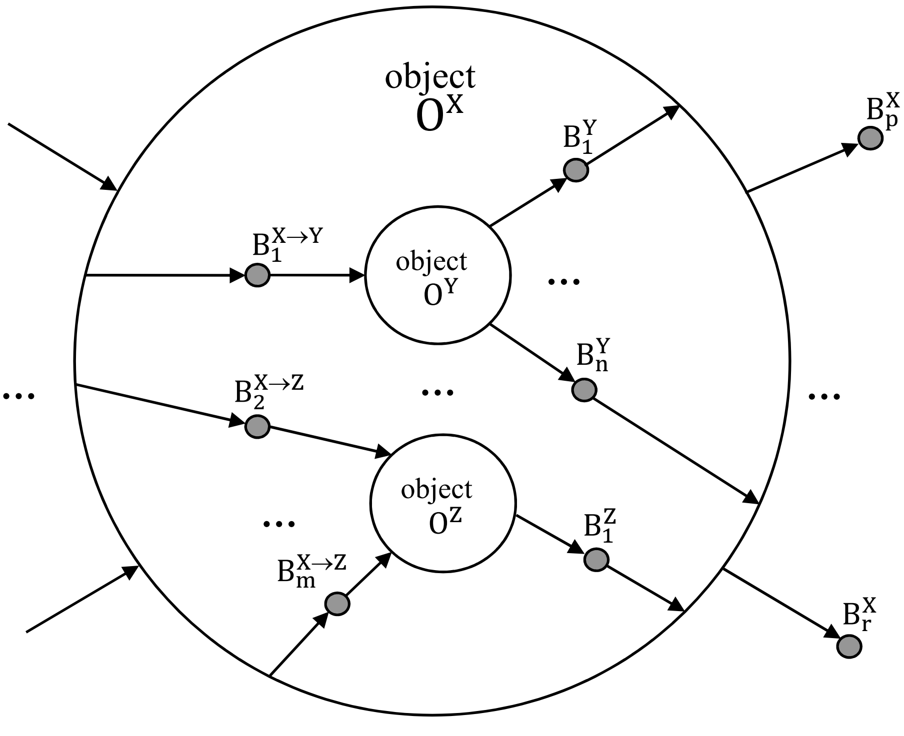

Figure 4. Example of a fragment of the permissible internal structure of connections between objects and buffers connecting with the central O^X object and its two internal O^Y and O^Z objects belonging to the CI model (*Source:* own elaboration)

In the case of the two-layered structure of CI objects (an example is presented in Fig. 5), the rules governing the functioning of objects become an important issue, in particular, the observation about the uniqueness of the functioning of both real resources and their computer models during simulation experiments due to the passage of time and the shrinkage of the space and effects that accompany these phenomena.

The impacts of the considered CI objects, presented in the layered interpretation, emphasize the autonomy of the behavior of the individual objects within both layers. Each of the layers aggregates the causal relationships between the input and output channels of the objects (the CI resources) contained therein.

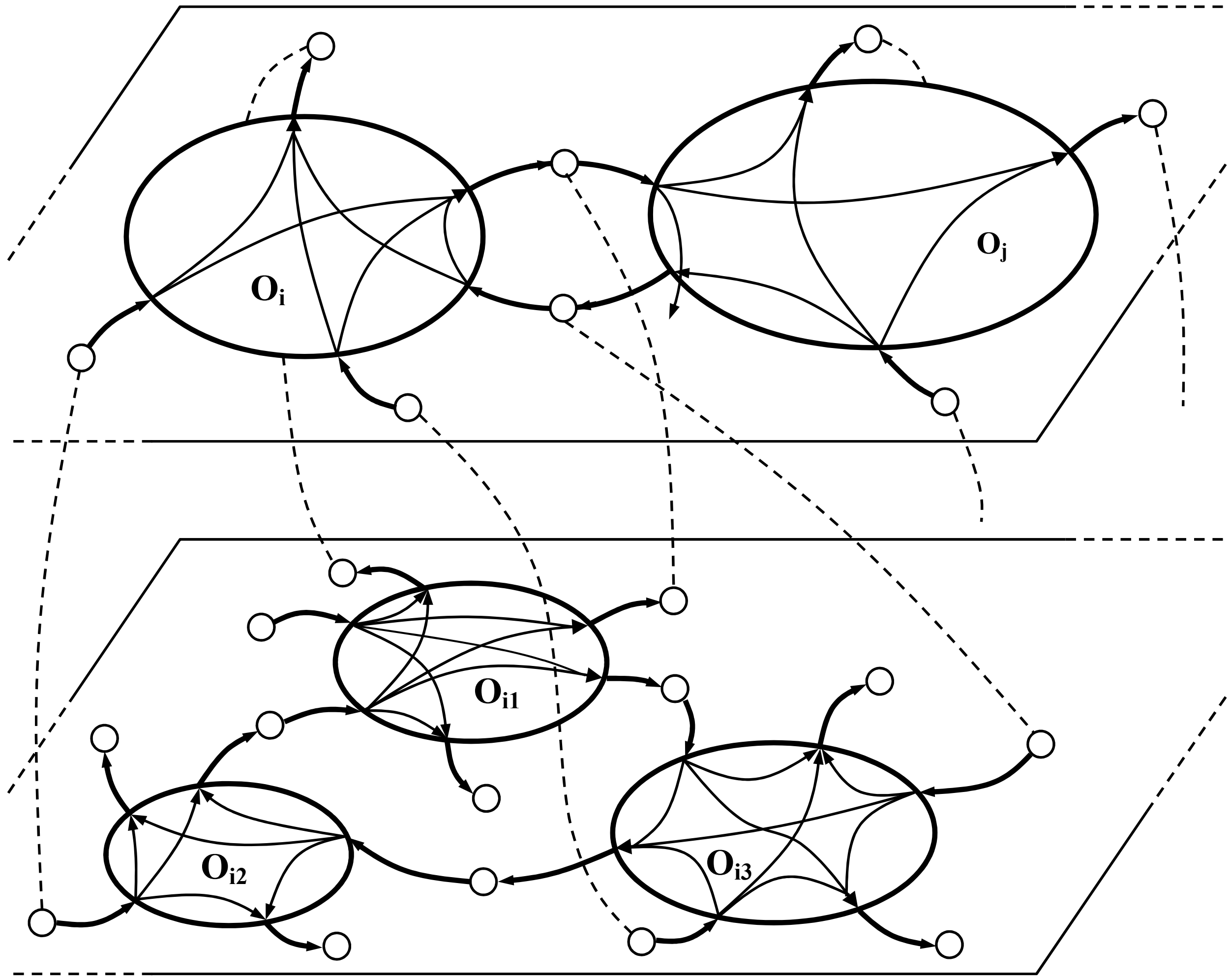

Figure 5. Layered interpretation of structural and functional behavior of objects Oi, Oj. Containing objects can be treated as flat and as hierarchical (multilayered) if their boundary lines do not cross and do not meet (*Source:* Krupa, 2006, p.77)

The layered interpretation of phenomena accompanying objects and their channels shown in Fig. 5 aggregates 23 compounds in the O_{i1}, O_{i2} and O_{i3} objects to 6 cause-and-effect relationships in the O_i object. It is worth noting that the aggregation of channels from the lower layer was achieved by means of two upper layer objects.

2.3 Topological hypergraph models

The hypergraph structure model is formally presented in the form of three graph symbols:

$$< V, G_v, \Gamma v >$$

where:

V, G_v – respectively, a set of nodes and a graph reference $<V, G_v>$,

Γv – a hypergraph signature specifying each node $V_i \subset V$ as $V_i \in V$.

When preparing the model of the hypergraph structure, an agreed representation of the hypergraph's nodes and arcs should be developed at the same time.

A hypergraph recording is particularly convenient if it is assumed that the relationship of belonging to certain subsets of nodes – treated as elements of a hypergraph, to other nodes thereof – treated as sets, will express affiliations (e.g. "elements of a certain object" – written in the form of a hypergraph, they will be expressed as a feature such as "to be part of the entire reactor").

Fig. 6a shows an example of a hypergraph describing the spatial and temporal relations occurring in certain communities of energy system objects. It is worth noting that the adopted convention of markings allows for the flexible displacement of objects (Fig. 6b) with respect to each other, provided that the invariant behavior of internal and external potential buffers (except the introduction of the $B^{U \to S}$ buffer) is in relation to its U and S transfer objects.

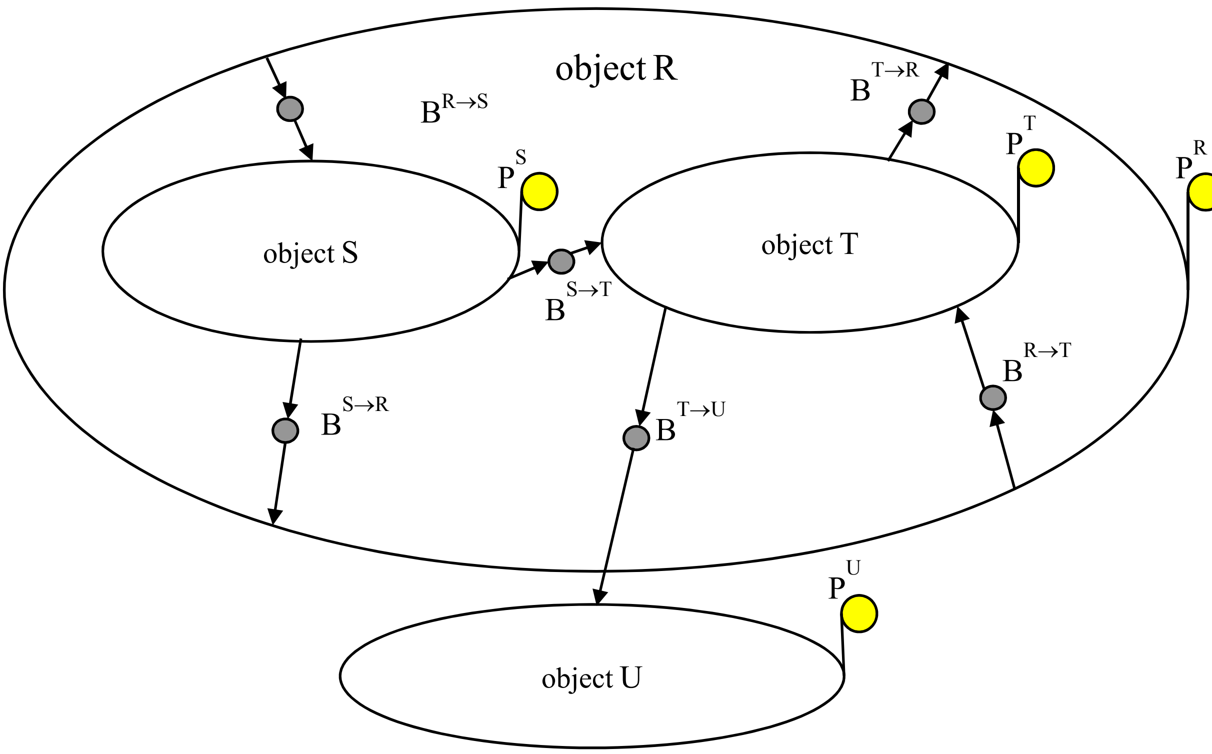

Figure 6a. An example of a hypergraph structure of CI objects – phase I
(*Source:* own elaboration)

It is worth noting that the adopted convention of markings allows for the flexible movement of objects relative to each other, provided that the invariable behavior of internal and external buffers is appropriate to their ownership objects. In Fig. 6b, object U has been additionally mutated with object S via its external $B^{U \to S}$ buffer.

Hypergraph links of objects and their buffers allow for the formal recording of the relationships between the functional potentials of CI objects and their links to object buffers. For the above purpose, sets can be formulated and analyzed logically (flow) for related functional potentials of objects and their potential buffers.

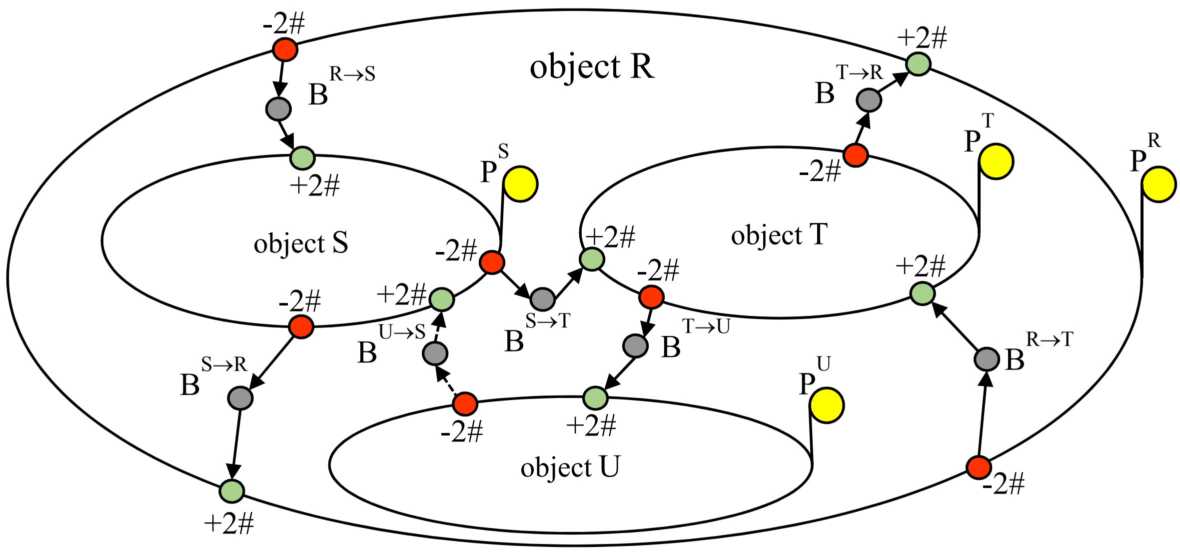

Figure 6b. An example of a hypergraph structure model of CI objects after the operation of making a U object with an S object using a $B^{U\to S}$ buffer – phase II (*Source:* own elaboration)

3 Security in functional terms

Security in functional terms is the most popular view of operational openness undertaken in situations of direct threat or as a deterrent against unrecognized potential attackers (e.g. defense against subversion or anti-terrorism). Its feature is the universality and effectiveness of the actions taken, provided that the identification of the threats takes place in advance and with sufficient and competent forces and means (Krupa and Wiśniewski, 2015; Nye, 2009; Ostrowska, 2013).

The concept of functionality in this study diametrically differs from the mathematical concept of function as an unambiguous right mapping. Functionality is rather a finite automaton endowed with memory that is more adapted to learning than to making decisions. Certainly, it cannot be closed in accordance with the ISO/IEC 9126-1:2001Software engineering - Product quality.

Security of functionality, as well as the topological issues of security, have been the subject matter of extensive literature, in which we have included:

- the potential of functionality (p#)[7],
- the coincidence of events on potential buffer (PB) objects involved in counteracting threats, and
- the simulation modeling of functional potential dynamics in potential buffers responsible for the coincidence processes of events observed using Cartesian products of the graphs of the functional states of the monitored objects.

3.1 The essence of the functional potential

CI objects and their total functional potential, as well as potential buffers, determine the space of the decisions (decision space).

For the sake of simplicity of presentation, the article adopts parallel sets of PBs and 5-element symbolism p0, p1, ..., P4 values of p#, which were included in Table 1.

[7] Potential of functionality (p#) – a conventional unit of measure corresponding to the possibility of executing 25% of the total value of the task assigned to the CI object buffer or corresponding to the possibility of executing 25% of the total task value assigned to the CI object as a whole.

Table 1. Symbolism of acceptable values of p# states in buffers of a protected object
(*Source:* own elaboration)

Symbol and value of the assessment in units #		Value in%
p0 – zero potential	0#	0 %
p1 – minimal potential	1#	25 %
p2 – half potential	2#	50 %
p3 – safe potential	3#	75 %
p4 – maximum potential	4#	100 %

3.2 Coincidence model of functional events of PBs

The diagram of the closed flow of the functional potential units p# shown in Fig. 7 (objects R, S, T, U and W, E and F and buffers $B^{R\to S}$, ..., $B^{T\to U}$ and $B^{U\to W}$) presents the situation of the cyclic flow p#. To simplify the considerations, we assume that the various accumulated potentials of P^R, P^S, ... and P^W will be determined simultaneously, and their flow p# through PB buffers will be equally intense and will run clockwise with a minimum unit of 1# per contractual unit of time τ, which means that the p# flow process will depend on the decision mechanisms that will be used in the p# transfer facilities on the network.

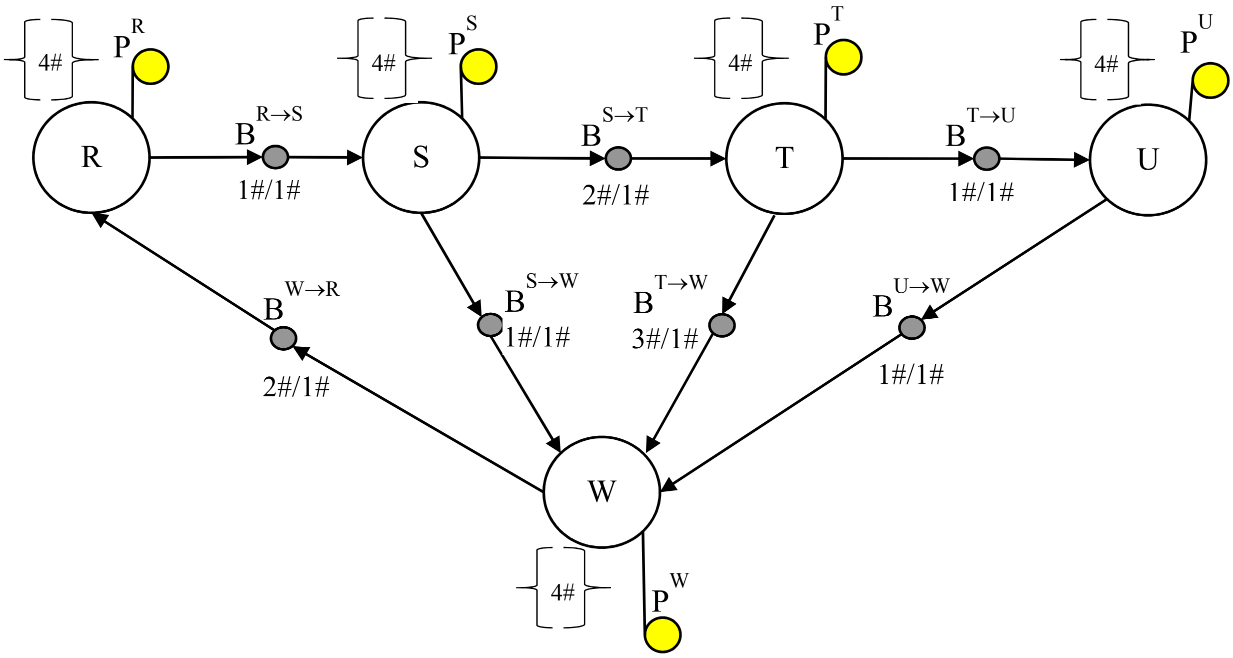

Figure 7. An example of the coincidence of functionality and events in a closed model of a single-layer structure of CI objects connected with each other by channels and buffers, with a distinguished coordinating object W to secure the continuity of the chain of R, S, T, U and W objects (*Source:* own elaboration)

The activity of a given object or a given buffer can take into account the occupancy of PB on the side of a pair of coincident objects and the potential of p# stored at a given facility, as well as on both sides of each PB of a given object. It is assumed that the number of PB of a given facility is limited only to the number of its active PBs, i.e. those to which pairs of objects providing and receiving p# are currently connected.

Signaling the state of p# objects and coordinating the protection of the balance of their desired level requires the use of natural mechanisms coordinating all the active (transferring) objects and their PBs.

3.3 The Cartesian product of functional graphs of PBs

The Cartesian product states' graphs, or more precisely, the graphical models of functionality can be effectively used to detect a priori errors in the initial phase or errors of a posteriori multiplication in graphical models of functionality.

To illustrate the possibilities of Cartesian products, we will use a simple example of the graph synthesis of states of the object, about which we know only which state graphs are characterized by PBs on two channels of the actual object being synthesized.

Many experiments indicate that carelessness with the Cartesian product may lead to the synthesis of a "one-armed bandit" automaton, rather than to the synthesis of an object with the correct functionality of a deterministic automaton with memory.

The task is to synthesize the $G_X = G_1 \times G_2$ graph generated as a result of the Cartesian product. In the first example, we will lead to the synthesis of an erroneously functioning graph of the states of the object with ambiguous mapping.

In the second example, our careless synthesis will lead to the oscillatory behavior of the object with three potential buffers and a tendency toward unexpected relaxation on three objects A, B and C connected to object X with similar functionality and unstable functioning. The scale of use of the Cartesian product of graphs is unlimited.

Example 1.

The Cartesian product of graphs saved in the form of a signature:

$V_1 = \{a, b, c\}$, $V_2 = \{p, q\}$

are sets of vertices of G1 and G2 graphs, and

$\Gamma_1 = \{\Gamma_a, \Gamma_b, \Gamma_c\}$, $\Gamma_2 = \{\Gamma_p, \Gamma_q\}$

are the signatures of the following graphs of the form:

$\Gamma_a = \{a, b\}$ $\quad$ $\Gamma_p = \{p, q\}$

$\Gamma_b = \{b, c\}$ $\quad$ $\Gamma_q = \{q\}$

$\Gamma_c = \{a, c\}$

The V_x file is the carrier of the G_x graph

$V_x = V_1 \times V_2$

$= \{(a,p), (b,p), (c,p), (a,q), (b,q), (c,q)\}$

The signature of the G_x graph is a set of

$\Gamma_x = \Gamma_1 \times \Gamma_2 = \{\Gamma_{a,p}, \Gamma_{b,p}, \Gamma_{c,p}, \Gamma_{a,q}, \Gamma_{b,q}, \Gamma_{c,q}\}$:

$\Gamma_{ap} = \{(a,p), (a,q), (b,p), (b,q)\}$

$\Gamma_{bp} = \{(b,p), (b,q), (c,p), (c,q)\}$

$\Gamma_{cp} = \{(a,p), (a,q), (c,p), (c,q)\}$

$\Gamma_{aq} = \{(a,q), (b,q)\}$

$\Gamma_{bq} = \{(b,q), (c,q)\}$

$\Gamma_{cq} = \{(a,q), (c,q)\}$.

Drawings of G_1, G_2 and G_x graphs are shown as Fig. 8 and Fig. 9, respectively.

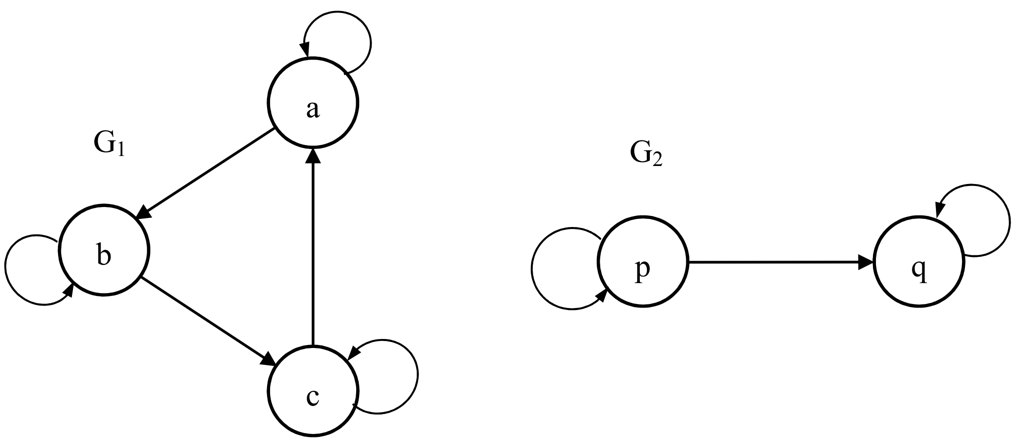

Figure 8. State graphs G_1 and G_2 (*Source:* based on Krupa, 2006, p.60)

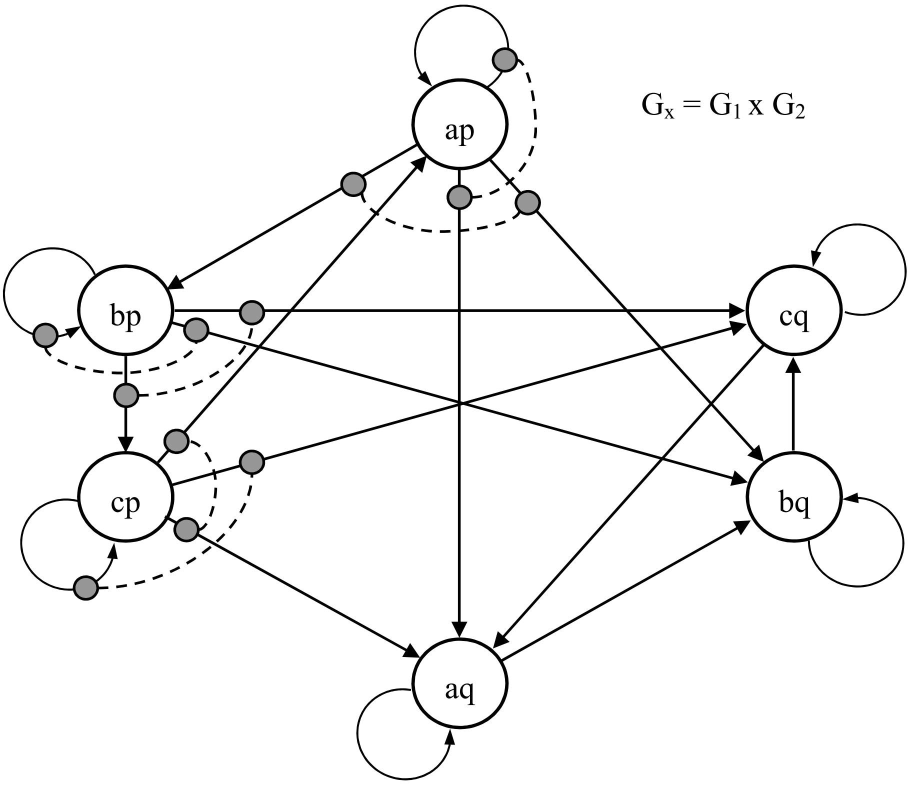

Figure 9. State graph $G_x = G_1 \times G_2$ (*Source:* based on Krupa, 2006)

Drawings of G_1, G_2 and G_x graphs are shown as Fig. 8 and Fig. 9, respectively.

The G_x graph created as a result of the Cartesian product of G_1 and G_2 graphs introduces an unexpected effect of the uncertainty of state changes on the G_x graph. In Fig. 9, we have three pairs of non-deterministic behaviors, which are presented in more detail in Table 2. The indeterminacy effect can occur in the case of three states of the G_x graph - these are states: ap, bp and cp.

Table 2. An example of the undefined change in the current state of the G_x graph for three cases of the current state of the G_x graph (*Source:* own elaboration)

	New state at the B^{G1} entry	Alternative G_x states	The current state of G_x	New state at the B^{G1} entry	Alternative G_x states
ap	a	ap	bp	c	cp
		aq			cq
ap	b	bp	cp	a	ap
		bq			aq
bp	b	bp	cp	c	cp
		bq			cq

Example 2.

The task is to synthesize the

$O^x = G_1 \times G_2 \times G_3$

graph created as a result of the Cartesian product of the graphs presented in Fig. 10a and saved in the form of the signature:

$G_1 = <V_1, \Gamma_1>$,

$G_2 = <V_2, \Gamma_2>$,

$G_3 = <V_3, \Gamma_3>$,

where:

$V_1 = \{a, b\}$, $V_2 = \{c, d\}$, $V_3 = \{e, f\}$,

they are sets of vertices of G1, G2 and G3 graphs and

Γ_1, Γ_2 i Γ_3

are the signatures of these graphs of the form:

$\Gamma_1 = \{ \Gamma_a, \Gamma_b \}$,

$\Gamma_2 = \{\Gamma_c, \Gamma_d \}$,

$\Gamma_3 = \{\Gamma_e, \Gamma_f \}$,

$\Gamma_a = (b)$, $\Gamma_d = (c)$,

$\Gamma_b = (a)$, $\Gamma_e = (f)$,

$\Gamma_c = (c,d)$, $\Gamma_f = (e)$.

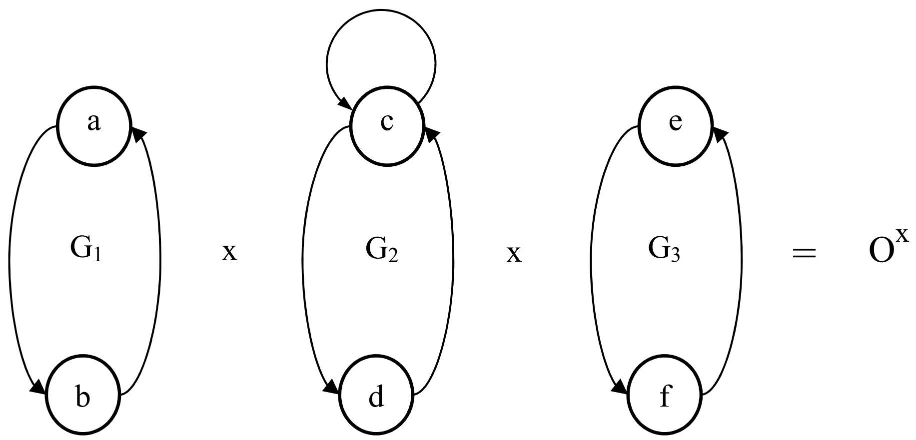

Figure 10a. Graph created as a result of the Cartesian product
(*Source:* own elaboration)

G_X carrier is shown in Fig. 10b set of nodes:

$V_x = V_1 \times V_2 \times V_3 = \{a, b\} \times \{c, d\} \times \{e, f\}$

$= (a,d,e),\ (a,c,e),\ (b,d,e),\ (b,c,e),$

$(a,d,f),\ (a,c,f),\ (b,d,f),\ (b,c,f).$

The signature of the Gx graph is as follows:

$\Gamma ade = (b,c,f)$

$\Gamma ace = (b,d,e) / (b,c,f)$

$\Gamma bde = (a,c,f)$

$\Gamma bce = (a,d,f) / (a,c,f)$

$\Gamma adf = (b,c,e)$

$\Gamma acf = (b,d,e) / (b,c,e)$

$\Gamma bdf = (a,c,e)$

$\Gamma bcf = (a,d,e) / (a,c,e)$

In the G_x graph, it is not difficult to identify two intersecting graphical figures in Figure 10b, the so-called "Wolf pits":

Wolf pit nr 1: bde & acf & bce & adf

Wolf pit nr 2: ade & bcf & ace & bdf

which, regardless of the state of the input buffers, causes the test object to be introduced into one of two trajectories of no-output states.

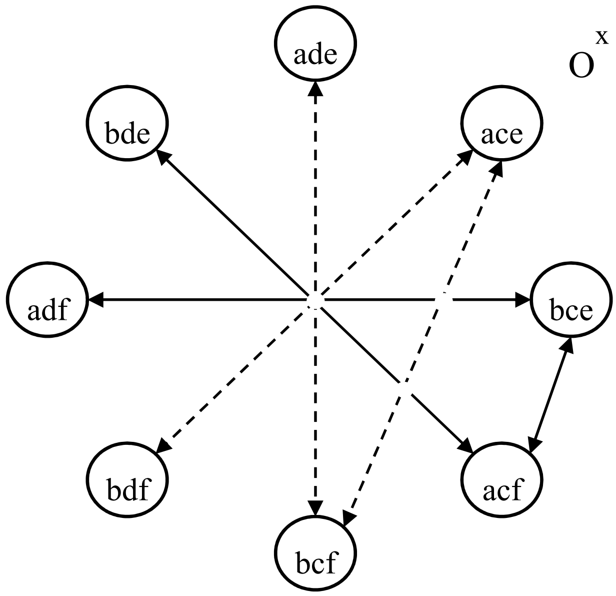

Figure 10b. Two trajectories of no-output graphical figures
(*Source:* own elaboration)

4 Security in semiotic categories

The semiotic analysis of the network of events of the functional potentials is carried out in three stages:

- a collection of sentence variables is created, which is called the carrier of the semiotic model, in which all the objects of the protected critical infrastructure are mapped,
- infrastructure objects are grouped into clusters of similar objects with the same characteristics and the same repertoires of features values,
- using the paradigm of the Gorbatov characterization principle related to the semantic correctness of the functioning of CI objects (Ficoń, 2007; Krupa, 2010).

The semantic analysis is carried out in three stages:

- a collection of sentence sequences of a CI object (section 4.1);
- a semantic model of the memory function of the CI object (section 4.2),
- transforming the model of the potential memory function into structural Hasse diagrams (section 4.3).

The management of the status of the functional potentials, even in only three objects and 15 buffers connecting objects, requires a specific decision-making policy in terms of the function potential buffers of each object, in which a given number of buffers B shall perform a specified target function on the directions $B^X \rightarrow B^Y$ objects X and Y.

The analysis of actions taken in relation to the objects makes us realize that the functional transfer mechanisms should be covered by a uniform policy of conduct if their action is to implement an effective, uniform and long-term strategy in relation to all objects considered as an CI system or subsystems.

In reference to the above, the detection of the CI objects responsible for the risk[8] and the increasing intensity of the events in the buffers is an important issue to counteract the growing crisis situations. In the considerations regarding the loss or excessive growth of p#, it is necessary to control buffers connecting objects for the indicated CI fragments – used to secure the current level of p# of the entire CI system to the point where it would be possible to lower the p# level to the risk discontinuity point called working on the gambling threshold[9].

---

[8] Risk – the value expressed in the formula P x U x Z, where: P – the probability of a hazard occurring within open limits (0..1); U – vulnerability within closed limits [0..1], where: 0 – means a complete lack of compliance, 1 – full vulnerability; Z – threat understood as the expected loss of functional potential in open limits [0..100]% of the analyzed object as a result of the impact of other objects.

[9] Gambling threshold – such a situation on a given object or combination thereof in the form of CI, which reached the risk discontinuity point expressed by P x U x Z ≥ 50% (H = 50%

The above-mentioned phenomena of CI continuity[10] protection points to the need for the formalization, monitoring and semantic analysis of events in CI decision spaces[11] to prevent incidents, crises and disasters.

The essence of risk calculus in decision spaces focuses on an integrated network of events with a multi-layer or hypergraph structure of objects connected through buffers.

The essence of the risk account in the decision spaces focuses on the integration of the event network with a multi-layer or hypergraph structure of objects connected through buffers. The mentioned elements of this integration are connected with each other by means of:

- event forcing initiated on the external and internal buffers of potential p# objects in single- and multi-layer structures, as well as in hypergraph structures,
- semantic analysis carried out using the paradigm of the characterization principle related to the semantic correctness[12] of p# CI objects.

CI's continuity:

- the organization's ability to respond to disruptions of normal operation conditions, and where possible, to quickly restore normal operating conditions, and where it is not possible, to go to the planned manner of substitute activities decision space,
- a set of alternative sequences of sentence variables, forming a semantic model, of which the decision about the most favorable (optimal) p# value is indicated as the paradigm of the characterization principle,
- the principle of characterization as a pattern of scientific research on the essence of risk in decision spaces and semantic correctness of the network,
- a set of relationships that occur between network events guaranteeing the completion of all correctly initiated processes.

4.1 Preparation of the collection of sentence sequences of an CI object

In relation to the above, an important problem of counteracting the growing crisis situation becomes the detection in the buffers of CIs responsible for the risk of the growing intensity of events threatening their relationship to the decreasing activity of the security events.

In the consideration of the account of the risk of loss or excessive growth p#, it is necessary to control buffers linking the objects of all or specified fragments of CI – used to secure the current level of p# of the entire CI system to the point where it would be possible to lower the p# level to the risk discontinuity point known as the gambling threshold, which occurs as a result of coincidences on the loss of p# event buffers and maintenance events p# of the considered CI.

The above-mentioned phenomena of CI continuity protection points to the need for the formalization, monitoring and semantic analysis of events in CI decision spaces in order to prevent the performance of the risk account[13] results in the form of incidents, crises and disasters.

The essence of calculating the risk of losing p# in decision spaces focuses on the integration of the event network with a multi-layer or hypergraph structure of objects connected through buffers.

The mentioned elements of this integration are connected with each other by means of:

- event forcing initiated on the external and internal buffers of potential p# objects in single- and multi-layer structures, as well as in hypergraph structures,

value is set a priori assuming that: P = 0.8 , U = 0.8 and Z = 80%; the next level of P = 0.9, U = 0.9 and Z = 90% would cause a nearly 50% increase in H = 73.9%).

[10] CI's continuity – the organization's ability to respond to disruptions of normal operational conditions, where possible, to quickly restore normal operating conditions, and where it is not possible, to go to the planned manner of substitute activities.

[11] Decision space – a set of alternative sequences of sentence variables, forming a semantic model, of which the decision about the most favorable (optimal) p# value is indicated.

[12] Semantic correctness of the network – a set of relationships that occur between network events guaranteeing the completion of all correctly initiated processes.

[13] Risk account – a systematic CI risk assessment carried out with a frequency proportional to the contractual risk discontinuity point referred to in this gambling application.

Table 3. Closed network of functional transfers with feedback (Fig. 7)
(*Source:* own elaboration)

Objects Phase I	P^X	P^Xtran	P^Xused	P^Xrest	P^Xcor	P^Xsum	P^Xrev	
	X_1	X_2	X_3	X_4	X_5	X_6	X_7	
W	4#	2#	1#	1#	3#	4#	2	rep. 1
R	4#	1#	1#	2#	1#	3#	2	rep. 2
S	4#	3#	1#	0#	0#	0#	1	inc. 1
T	4#	4#	2#	-2#	1#	-1#	0	inc. 2
U	4#	1#	1#	2#	0#	2#	2	
Objects Phase II	P^X	P^Xtran	P^Xused	P^Xrest	P^Xcor	P^Xsum	P^Xrev	
	X_1	X_2	X_3	X_4	X_5	X_6	X_7	
W	4#	2#	1#	1#	3#	4#	2	rep. 1
R	3#	1#	1#	1#	1#	2#	2	rep. 2
S	0#	3#	1#	-4#	0#	-4#	0	inc. 1
T	-1#	4#	2#	-7#	1#	-6#	0	inc. 2
U*	2#	1#	1#	-1#	0#	-1#	0	

Legend (description details):

P^X – the initial potential of the facility's functionality in a given phase,
P^Xtran – the potential reported for transfer from the facility in a given phase,
P^Xused – the potential used in object buffers,
P^Xrest – the potential remaining in the facility,
P^Xcor – the potential for correction created for the object,
P^Xsum – the total potential after correction in the object,
P^Xrev – the potential revision in the facility,
rep. – full repetition of the sequence of sentence variables,
inc. – full containment sequence of propositional variables.

- semantic analysis carried out using the paradigm of the characterization principle related to the semantic correctness of p# CI objects.

The subject of the semantic analysis will be an example of a network of objects and transfer buffers with the highlighted object W shown in Fig. 7. The network and phenomena of p# transfer were coded in subsequent moments of its functioning in Table 3 with accompanying comments[14].

The key in the pre-semantic analysis is the separation from the Table 3 sentence variables and the creation of a sequence set from them, which will be used to build a semantic model of buffer potentials and CI objects from them, which will be used to build a semantic graph model at the level guaranteeing the proprietary functionality of the CI objects. The details of this procedure are presented in section. 4.2.

[14] The paradigm of the characterization principle – the principle of characterization as a pattern of scientific research on the essence of risk in decision spaces.

4.2 Semantic functional model of memory of the potentials of CI and PB objects

The semantic model of the potential memory of CI objects is saved using the symbolic formula:

$[X_{11} \ \& \ X_{21} \ \& \ ... \ \& \ X_{m1}]_1$ □ $[X_{12} \ \& \ X_{22} \ \& \ ... \ \& \ X_{m2}]_2$ □ ... □ $[X_{1n} \ \& \ X_{2n} \ \& \ ... \ \& \ X_{mn}]_n$

where:

- X_{ij} represents no more than a single occurrence of the propositional variable Xi (object) inside the above sequence but with the possibility of repetition in concurrent sequences of the sentence variables (SSV),
- concurrency SSV is marked with the symbol „□" and allows their conjunction or parallelism,
- the value of variable X_i can be homogeneous objects of the modeled problem (e.g. events, logical variables, buffer identifiers; in the example in question, they are identifiers of specific objects).

In the discussed issue of the memory of the potentials of the CI objects, presented in Table 3, the value of the sentence variables X_{ij} is 2 x 5 the sequence of the potentials of all available objects W, R, S, T and U, for which the total sum of the potentials selected for the analysis of the semantic parameters in the first phase varies within -2# .. 4#; in the second phase, it ranges between -7# .. 2#. The limits have been selected so that for the initial (I) and final (II) phases, one can estimate why the crisis of transfer of the functional potentials occurred so quickly. The final result of the sequence of the phase I and II sentence variables is shown below.

Sequences of phase I propositional variables:

$[X2\&X3\&X4]_1$ □ $[X2\&X3\&X5]_2$ □ $[X3\&X4''\&X5]_3$ □ $[X4''\&X5\&X6']_4$ □ $[X2\&X3\&X6]_5$

Sequences of phase II propositional variables:

$[X2\&X3\&X4]_1$ □ $[X2\&X3\&X5]_2$ □ $[X3\&X4''\&X5_{\&}X6']_3$ □ $[X4''\&X5\&X6']_4$ □ $[X2'\&X4'\&X6]_5{*}$

A single sequence of $[X2' \ \& \ X4' \ \& \ X6]_5{*}$ phase II has been limited to phase I.

The remaining phase II sequences were incorporated into the phase I sequence. All the qualified sequences were introduced into the semantic model of the functional memory of the analyses presented in Fig. 11.

Fig. 11 is a kind of semantic memory record (states of semantic memory graph) of the event network presented in Fig. 7 in a closed model of a single-layer structure of CI objects connected with each other by buffers with a distinguished coordinating object W to protect the continuity of the buffer chains R, S, T, U and in the object CI.

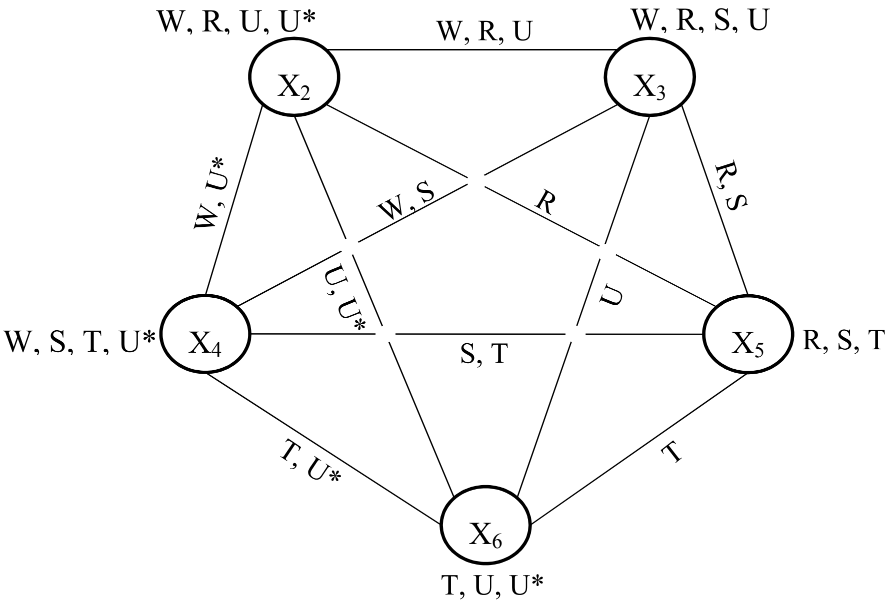

Figure 11. Semantic model of the graph of functional transfers on the web (*Source:* own elaboration)

4.3 Transforming the model of potential memory function into structural Hasse diagrams

The search for erroneous sequences of events is carried out in hypergraph-structure object structures. The results of the research are the mechanisms of the transformation of the event network.

The final stage in the analysis of security phenomena in semiotic categories is the transformation of the semantic model of potential memory into the structural network of Hasse branches presented in Fig. 12.

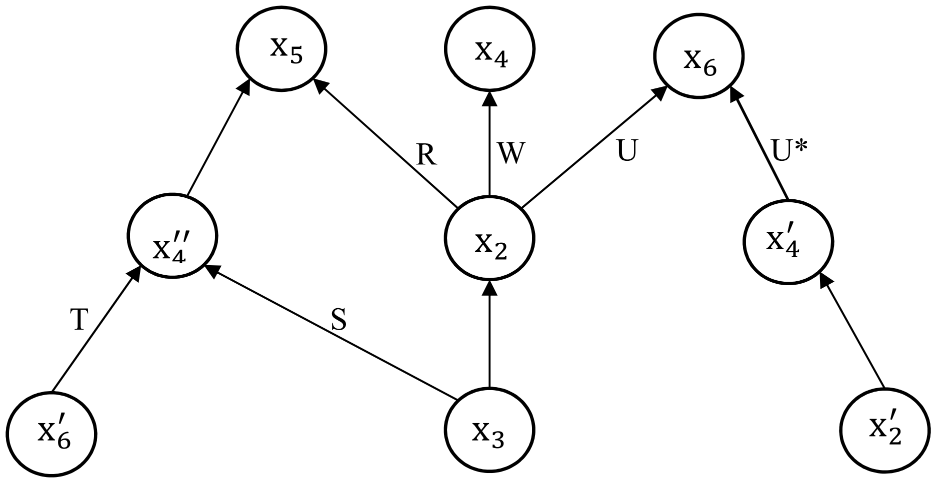

Figure 12. Hasse diagram illustrating the chaotic phenomenon of functional transfers as a result of the lack of proper coordination of transferring parameters (*Source:* own elaboration)

The possibility of giving the features of a partially ordered structure is proof of its correctness, provided that the paradigm of the characterization principle is preserved. The degree of complexity (the minimum number) of searching for solutions is the power of the set |{p#}|!, all functional potential events that occur on all CI network object buffers.

The semantic memory medium is the CI network buffers contained in Table 3, together with p#. The analysis of the semantic memory model will then be used in p. 3.3 to examine the complexity of the structure of 5 p# events. As a result, it will turn out that their number will have to be significantly increased (up to 9 p#) in order to be able to use the diagram (Hasse branches, Fig. 12).

In the example under consideration, we have:

- the initial number of P^X sentence variables in the sequence (1) Table 3 is: 6 (6! = 720), and after a reduction of buffer redundancy, is 5 (the number of solutions 5! = 120)
- the minimum number of P^X propositional variables after split sentence variables by an additional four replicas enlarged to P^X = 9 (the number of solutions 9!= 362 880).

In the assessment of the above-mentioned proceedings, it should be realized that the assessment of complexity – and especially the assessment of the increase in the complexity of searching for solutions as a result of variable splitting, as well as the diversity of the sequence of sentence variables, can be very different.

5 Conclusion

This work does not sufficiently solve all the threads of broadly understood security; in particular, it cannot answer any doubts regarding the problems of functional theory in security applications. However, the authors of the article tried to introduce the elements of functional theory to the circulation of research and formulate a simple paradigm of functionality as a way to solve issues that have seemingly been solved or are subject to new research interests arising from technological progress, climate change, the political and economic situation, population migration, the change of state borders, terrorism and many other more or less dangerous phenomena in the natural environment of individuals, groups, societies, nations and states.

The title of the work was defined in highly abstract categories, and at the same time, functionality was interpreted in the application of the topological and semiotic context. Hence, the need to extend the mechanisms for controlling the correctness of the potential for the functioning of particularly complex objects and their spaces requires, in our opinion:

- advanced semiotic analysis based on semantic control of the correctness of simulatively generated products of the events network, enriched with a topological analysis of digital objects,
- the creation of laboratories and research centers educating professionally trained specialists to function in the infinite space of the virtual world of advanced system technologies.

6 References

[1] Domański, J., Kotarba, W., Krupa, T., 2014. The Prisms of Management. *Foundations of Management*. Vol. 6, No. 2, pp.43-50, DOI: 10.1515/fman-2015-0010.

[2] Ficoń, K., 2007. *Inżynieria zarządzania kryzysowego. Podejście systemowe* (*Crisis Management Engineering. System Approach*). Warszawa: BEL Studio.

[3] Gorbatov, V.A., 1979. *Semanticeskaja teorija projektirovanija avtomatov (Semantic Theory of Designing Automata*). Moskva: Izd. Energia.

[4] Homenda, W., 2009. *Algorytmy, złożoność obliczeniowa, granice obliczalności* (*Algorithms, Computational Complexity, Limits of Computability*). Warszawa: Wyd. Centrum Studiów Zaawansowanych Politechniki Warszawskiej.

[5] Jajuga, K., ed., 2007. *Zarządzanie ryzykiem* (*Risk Management*). Warszawa: PWN.

[6] Kieżun, W., 2018. Four Riders of the Apocalypse of the Polish Bureaucracy. *Foundations of Management*. Vol. 1, pp.7-12, DOI: 10.2478/fman-2018-0001.

[7] Koziej, S., 2009. *Między piekłem a rajem. Szare bezpieczeństwo na progu XXI wieku* (*Between Hell and Paradise. Gray Security on the Threshold of the 21st Century*). Toruń: Wydawnictwo Adam Marszałek, pp.27.

[8] Krupa, T., 2005. O pewnej specyfikacji procesu decyzyjnego (About a Certain Specification of the Decision-Making Process). *Problemy Zarządzania* (*Management Problems*). Warszawa: Wydawnictwo Naukowe WZ UW, No. 1, pp.79-88.

[9] Krupa, T., 2006. *Elementy organizacji, zasoby i zadania* (*Elements of Organization, Resources and Tasks*). Warszawa: WNT.

[10] Krupa, T., 2009. Events and Events Processes. *Foundations of Management*. Vol. 1, No. 2, pp.143-158, DOI: 10.2478/v10238-012-0016-9.

[11] Krupa, T., 2010. Hierarchiczny model procesów podejmowania decyzji z wielopoziomowymi ograniczeniami i sprzecznościami - rozważania I propozycje (Hierarchical Model of Decision-Making Processes with Multi-Level Constraints and Contradictions - Considerations and Proposals). In: M., Hopej, M., Moszkowicz, J., Skalik, eds. *Wiedza w gospodarce i gospodarka oparta na wiedzy. Zarządzanie w gospodarce opartej na wiedzy* (*Knowledge in the Economy and Knowledge-Based Economy: Management in a Knowledge-Based Economy*). Wrocław: Uniwersytet Ekonomiczny we Wrocławiu, pp.149-158.

[12] Krupa, T., 2013. V.A. Gorbatov Theory of Characterization – Principles and Examples. *Foundations of Management*, Vol. 5, No. 3, pp.89-102, DOI: 10.2478/fman-2014-0022.

[13] Krupa, T., 2016. Zasada charakteryzacji jako systemowy paradygmat w naukach o zarządzaniu – eksperymenty i zastosowania (The Principle of Characterization as a Systemic Paradigm in Management Sciences - Experiments and Applications). In: A., Zakrzewska-Bielawska, ed. *Stan i perspektywy rozwoju nauk o zarządzaniu – Wybrane problemy* (*Status and Prospects of Development of Management Sciences - Selected Problems*). Toruń: Wyd. TNOiK, pp.180-217.

[14] Krupa, T., Ostrowska, T., 2007. Multilayer Decision Support Model for Value and Cost Analysis of IT Solutions – Hierarchical Approach. In: *Managing Worldwide Operations and Communications with Information Technology*. IGI Pub-

lishing, IRMA Int. Conf., Vancouver Canada, pp.86-90.

[15] Krupa, T., Ostrowska, T., 2017. Prakseologiczne aspekty teorii zdarzeń – symetria zagrożeń i podatności (Praxeological Aspects of the Theory of Events - Symmetry of Threats and Vulnerabilities). In: W., Kieżun, J., Wołejszo (red.). *Prakseologia w zarządzaniu i dowodzeniu. Ekonomiczność w zarządzaniu* (*Praxeology in Management and Command. Economics in Management*). Kalisz: Państwowa Wyższa Szkoła im. Prezydenta Stanisława Wojciechowskiego w Kaliszu, pp.59-73, ISBN 978-83-65872-09-8.

[16] Krupa, T., Prokopowicz, T., 2018. Paradygmat teorii charakteryzacji w procesach podejmowania decyzji (The Paradigm of the Characterization Theory in Decision-Making Processes). In: M., Budzanowska-Drzewiecka, K., Czernek, eds. *Kierunki ewolucji nauk o zarządzaniu* (*Directions of Evolution of Management Sciences*). Kraków: Wydawnictwo Uniwersytetu Jagiellońskiego, pp.51-72.

[17] Krupa, T., Wiśniewski, M., 2015. Situational Management of Critical Infrastructure Resources under Threat. *Foundations of Manafgement*, Vol. 07, pp.93-104, DOI: 10.1515/fman-2015-0028.

[18] Kulińska, E., 2016. Model of Axiological Dimension Risk Management. *Foundations of Management.* Vol. 5, No. 3, pp.211-226, DOI: 10.1515/fman-2016-0017.

[19] Maj, K., Krupa, T., 2010. The Management Method Preventing a Crisis Situation in an Electrical Energy Utility. *Foundations of Management,* Vol. 2, No. 2, pp.37-50, DOI: 10.2478/v10238-012-0027-6.

[20] Nye, J.S., 2009. *Konflikty międzynarodowe. Wprowadzenie do teorii i historii* (*International Conflicts. Introduction to Theory and History*). Warszawa: Wydawnictwa Akademickie i Profesjonalne, pp.287.

[21] Ostrowska, T. (2013). The Resource Hazards Model for the Critical Infrastructure of the State Emergency Management Process. *Foundations of Management*, Vol. 5, No. 3, pp.49-60, DOI: 10.2478/fman-2014-0019.

[22] Ostrowska, T., Krupa, T., Wiśniewski, M., 2015. Dynamic Hazards in Critical Infrastructure of State. *Foundation of Management*, Vol. 7, pp.143-158, DOI: 10.1515/fman-2015-0032.

[23] Pogorzelski, W., 1999. *Inżynieria badań systemowych*. *Prolegomena* (*Systems Research Engineering. Prolegomena*). Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej.

[24] Saaty, T.L., 1980. *The Analytic Hierarchy Process*. New York: Mc-Graw Hill.

[25] Skomra, W., ed., 2015. *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP* (*Risk Assessment Methodology for the Needs of the Crisis Management System of the Republic of Poland*). Warszawa: Szkoła Główna Służby Pożarniczej.

[26] Wiśniewski, M., 2016. Concept of Situational Management of Safety Critical Infrastructure of State. *Foundation of Management*, Vol. 8, pp.297-310, DOI: 10.1515/fman-2016-0023.

[27] Zawiła-Niedźwiecki, J., 2013. *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania* organizacji (*Operational Risk Management in Ensuring the Continuity of the Organization's Operations*). Kraków: Wyd. edu-Libri, ISBN: 978-83-63804-12-1.

[28] Zawiła-Niedźwiecki, J., 2014. *Operational Risk as a Problematic Triad: Risk – Resource Security – Business Continuity*. Kraków: edu-Libri, ISBN: 978-83-63804-42-8.

[29] Zwicky, F., 1969. *Discovery, Invention, Research – Through the Morphological Approach.* Toronto: The Macmillian Company.