

MODELING OF SOCIO-COGNITIVE VULNERABILITY OF HUMAN ORGANIZATIONS: TOGA META-THEORY APPROACH

Adam Maria Gadomski
ENEA¹

Keywords: vulnerability, human organization, management, decision-making, social, cognitive, human-caused threats, methodology.

Abstract

The paper dealing with the identification of the sources of vulnerability in human organizations. It is focused on the preliminary demonstration how a systemic unified computational methodological approach can be useful for the modeling of the vulnerability on individual, inter- and intra-organizational decisional levels in case of human-caused threats and organizational crisis. The modeling paradigms and framework of the TOGA (Top-down Object-based Goal-oriented approach) has been applied as a meta-modeling framework.

"human self, threats to the self"

Introduction

Human organizations efficiency plays an essential role in the mitigation of disasters, calamities, energy blackouts and other large scale emergencies. The vulnerability of the emergency management organizations, such as, civil protections, local administrations, owners of large energy and telecommunication networks, is a critical but usually not well visible factor under the normal not extreme everyday conditions. In the analysis of risks concerning large human-technology systems, the probability of human errors becomes dominating parameter in the assessments of their reliability.

Human organization socio-cognitive vulnerability can be seen as a state of the organization when possible dangerous events are able to cause either its wrong decisions or may lead to its internal crisis. Organization decisions are two types, individual and collective. They both involve many social constrains and depend on complex cognitive and psychological factors. The aim of this work is focused on the preliminary demonstration how a systemic unified computational methodological approach can be useful for the modeling of the vulnerability on inter- and intra-organizational decisional levels in case of human-caused threats and organizational crisis.

Problem

This work is dealing with the identification of socio-cognitive vulnerability of human organizations.

Searching on the full Worldwide Web we may see only (Google, Feb. 17, 2006): 2 docs for *"vulnerability of human organizations"*, 9 docs for *"critical infrastructures"*, *"organization vulnerability"*. 14 docs for: *"organization vulnerability"*, *"human errors"*, and 64 for *"vulnerability of technological"*, but we have 132.000 docs for *vulnerability*, *"critical infrastructures"*, and 49.500.000 documents for: *vulnerability, research*. Such results indicates that the problem of human organization is only mentioned, in general, in rich

¹ National Agency for New Technology, Energy and Environment
Via Anguillarese 301, Rome. Adam.gadomski@casaccia.enea.it

contexts of very specific technological and psychological vulnerabilities, and not yet an object of regular research. The critical infrastructures direction and the problem of the organization responsibility for these structures is only indicated as always more and more important for our technological society. Such preliminary conclusion leads us to the necessity of the identification of the influence of human organization states and dynamics, on the development and exploitation properties of critical infrastructures (such as energetic and communication grids), especially under various large-scale emergency conditions.

On the base of the analysis of the management of, generally known, last natural and technological disasters (hurricanes, blackouts) we may claim that organizational managerial errors may lead to the essential increasing of human and economical losses. This type of human-caused threats has its source in the complex functioning of large organizations, and in socio-cognitive decisional models adapted by their managers, more or less consciously.

In this paper, we are focused on the vulnerability of human organization caused by the vulnerability of individual and group decision-making processes.

For the reason of the lack of standards and commonly accepted ontologies (terminology), in order to be comprehensible, there is necessary to explain systematically how we understand the basic terms we intend to use.

Short preliminary definitions

Vulnerability

Most general, vulnerability is a lack of immunity or insufficient resistance on unexpected but possible events. We distinguish two basic types of vulnerability:

A. Vulnerability on external events: dangerous situations, attacks, intrusions - human-based threats, natural threats, technological, market threats.

B. Vulnerability on internal events: internal crisis, pathologies, and improper reorganization.

The similar definition of vulnerability was recently proposed by A. Gheorghe, D. V. Vamanu, 2005 [1]

*“The **system vulnerability** can be defined as the chance that a specified change in the system environment leads to disruptions in the nominal functionality of the system. A technological system can be said to be resilient in the face of a particular threat if it is capable of maintaining its functionality (original ‘purpose’) when the environmental challenge occurs.”*

Any of them may lead to the heavy losses for vulnerable objects.

According to FEMA (see Web), for the emergency management organizations: *“The key to the use of the Vulnerability Analysis is the recognition of the many types of emergencies, which could affect you, and the resources that are available to respond to the emergency.”*

From the perspective of internal events, the key factors responsible for the vulnerability are properties of organization itself and its employers.

In order to comprehend better this concept we need to define *crisis*.

Crisis:

It is a complex situation/phenomenon where a routine management is not more efficient.

Crisis creates a system with unknown functionality [2] and behavior.

Crisis can appear on various organizational levels. In extreme crisis situation routine control/management is not more possible or efficient. Using a model-base interpretation:

Crisis is when the model applied for the management is not more adequate to the real organization structures and processes.

A crisis may lead to an emergency or an externally caused emergency may cause an organization crisis.

Emergency

Emergency is characterized by well visible unacceptable levels of risk and losses generation caused by abnormal events and it requires not routine immediate interventions, called emergency management. They are or have to be performed during whole emergency state.

The emergency state can be caused by internal events (crisis – as organization inefficacy) or external events as natural and technological disasters. In organization, usually a crisis states is mitigated by re-organizations, in contrary, it activates, sooner or later, an emergency state [3]. In such context, **vulnerability is a readiness to a crisis state**.

Human organization

For our purposes we define human organization as a system/network with explicitly established reciprocal dependencies between people, which, according to their competences, collaborate for achieving common objectives or realize predefined missions.

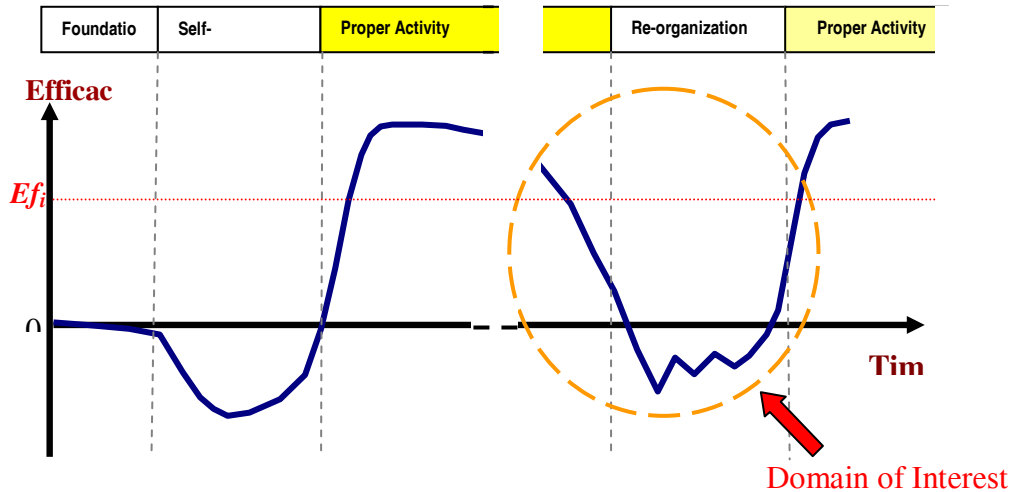


Fig.1 En example of the qualitative representation of the organization efficacy curve during its life-cycle. Ef_i denotes a critical value of efficacy for a crisis and possibility of emergency.

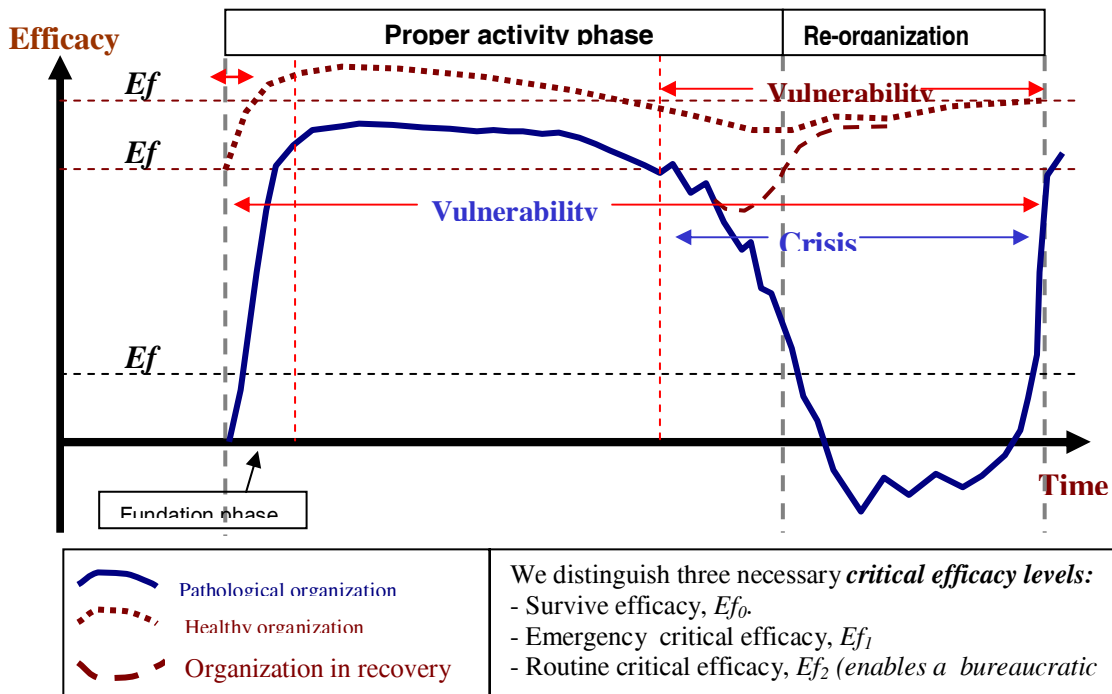


Fig. 2. A qualitative representation of the relations between different levels of efficacy and crisis and vulnerability during last two phases of the generic organization life-cycle.

For the above reason, the top indicator of an organization utility is *efficacy*. On the other hand, from the time perspective, we may distinguish five phases in the organization life cycle: foundation phase, self-organization, proper activity and re-organization, Fig.1. The concepts: *vulnerability*, *crisis* and *emergency* are well visible in this generic life-cycle picture where they can be, in different manner, allocated to the organization phases. This allocation is qualitatively illustrated on the next figure, Fig. 2.

In the preliminary life-cycle model, if organization efficacy $ef < Ef_1$ then the organization is vulnerable. Unfortunately, an assessment of socio-cognitive organization efficacy is a relatively new and complex problem. It requires sufficient problem-oriented definitions of: metrics, measurement and estimation/assessment of: $ef(t)$, Ef_2 , Ef_0 , for $t \in T$ in frame of one integrated model.

Remark. In our study, we are only focused on “nude” human organizations, it means without technical supports and technological infrastructures. Of course, their presence and states influence strongly human decisions but they are taken under consideration indirectly, i.e. they exist in the organization knowledge, information available, and preferences, which are effectively used. These aspects are discussed later, in the progress of the article.

Socio-cognitive vulnerability.

Organization vulnerability includes a socio-cognitive vulnerability. It means a vulnerability caused by human components, their cognitive properties and involvement in social processes inside and outside of the organization Socio-cognitive engineering and management [4], [5] takes under consideration the interests and points of view of: citizens, employers, managers, owners & politicians. They assume a subjective perspective of an intelligent entity. Complexity in socio-cognitive approaches is not only a physical complexity but it includes complexity of mental processes under social constrains. Therefore it includes such new for engineers attributes as : vagueness, uncertainty conflicts, incomplete knowledge, variable access to information, emotions, irrationality, ethical preferences and organizational & socio-cultural factors.

Human components are highly autonomous systems, which usually participate, in parallel, in many social roles; they have hardly identified and controlled attributes, such as personal interests, individual competences and emotional irrationalities. Their participation in the organization actions is based on motivations and more or less shared values systems.

The main problem of socio-cognitive management of organization is to synchronies individual motivations and capabilities with objectives of the organization and its decisional style. Socio-cognitive vulnerability appears when the organization members are not able together to produce decisions that satisfy their organization objectives.

Method: the TOGA framework

We start from the request of a proper methodology of the modeling/identification of human organizations.

We distinguish three main types of modeling approaches in the state of the art:

1. Soft modeling, which is descriptive, partial and intuitive – human-user oriented, for example, [6],
2. Hard mathematico-physical modeling, it is usually focused on partial continuous processes, with difficulties of the measurements of employed variables. They are idealistic, and rather for illustrative simulations interpreted later by “soft specialists”. Hard modeling is computer oriented and includes numerical and logical calculations (for example it is frequently visible in Operational Research) [7].
3. Flexible socio-cognitive modeling: It is computational modeling under real-world conditions, It has to be the systemic based on AI technologies employing external and internal observers, and designed for simulation and decision-support. Its important paradigm is a top-down perspective which enables always complete vision of the problem on different levels of

generality. It is interdisciplinary by definition and human-computer oriented. This approach is in early stage of development [see Web].

For the reason of numerous attributes and complexity of human organizations, in order to not omit its properties essential for vulnerability, the proper methodology of identification has to be top-down investigated. As a consequence of the mentioned requirements the adapted identification approach is based on the TOGA (Top-down Object-based Goal-oriented Approach) meta-theory [8], [9], being applied to the formulation of elements of the socio-cognitive human organization theory .

More precisely it should provide a meta-ontology and conceptual tools for the modeling and indications of vulnerable components, processes and properties of h-organization in specific, domain-dependent situations.

TOGA is a formal goal-oriented knowledge ordering meta-theory, it has three basic components:

- Theory of Abstract Objects (TAO), which is a first level and a basic domain independent conceptualization system and consensus building platform;
- Knowledge Conceptualization System (KNOCS), It includes TOGA's ontology, i.e. axiomatic assumptions and basic conceptualization frameworks for the definition and decompositions of the real-world into an intelligent agent (IA), and domains of IA goal-oriented activities;
- Methodological Rules System (MRUS) for the specification (if not existed yet) or identification (if existing) of complex systems and problems; in our perspective, it indicates how TAO and KNOCS have to be used during the conceptual identification, specification and solution of real word problems.

The model-based analysis employed are based on the KNOCS meta-frameworks being represented by four ideal conceptualization paradigms/laws which describe behaviour of an abstract intelligent agent, they are:

1. **Universal Reasoning Frame Paradigm (URP)**, which is based on the IPK (Information, Preferences, Knowledge) architecture.
2. **Universal Management Paradigm (UMP)**, which represent a functional definition and the context of the managerial role.
3. **SPG Universal Domain Paradigm (UDP)**, it is a framework of the conceptualization of the relation between an organization and its foundation-goal in terms of: systems, processes, functions and intervention-goals.
4. **WAG Universal Activity Paradigm (UAP)**, it is a framework for the conceptualization of the relation between a problem world and a goal of intervention of intelligent agent (World- Action-Tasks-Goal interrelation).

The above paradigms we consider essential for the identification of vulnerabilities. Their applications are governed by top-down goal-oriented MRUS (Methodological Rules System).

Universal Reasoning Frame Paradigm (URP)

URP is based on the application of the data processing scheme to the human goal-oriented reasoning. It assumes three basic types of "data bases" which distinguish such subjective concepts as information, preferences, knowledge as reciprocally independent mental entities employed in every decisional process.

Information is a concept from the ontology of a modeler, problem solver, or decision-maker. In this view, information is data describing a property of an object or entity of interest.

According to the TOGA meta-theory, it is "*data which represent a specific property of the domain of human or artificial agent's activity (such as addresses, telephone numbers, encyclopedic data, various lists of names and measurements)*". In this view:

- every piece of information has a source,
- every piece of information has a subjective true or false value for its receiver/owner,

- information is a relative concept; that is, what is a piece of information for one person might only be a signal for another.

Knowledge is one of the essential for humans but always ill defined concept with numerous local notions in natural languages and professional, domain-dependent terminological systems. From the most diffused intuitive functional perspective it is a mental property which enables humans to act in a goal-oriented/directed manner. From a most universal point of view, we may separate information from knowledge, and knowledge from our preferences or values.

Here we assume, **knowledge** is every abstract property of a human or artificial agent which has ability to process/transform a (quantitatively/qualitatively) information into other information

Every knowledge has to have a reference domain where it is applicable. It has to include the source domain of the processed information. [9].

We distinguish descriptive (dependencies, models) and operational knowledge (such as: instructions, emergency procedures, manuals, scientific materials, models, theories). **Meta-knowledge** enables operations on knowledge and produces another knowledge.

As a knowledge is a relative term, an entity which is knowledge for one agent can only be information for another.

Preferences. Preference is an ordered relation among two properties of a real or abstract domain of activity of a cognitive agent. It indicates a property with higher utility or subjective importance. The preferences systems mirror a domain expert wisdom, as well as, individual ethical, cultural and emotional values. Preference relations serve to establish an *intervention goal* of an agent. Human preferences rules are hard but possible to extract. This can be done by various interviews, analyzing spontaneous declarations and opinions, and by observation of human actions.

Organization preferences are practically divided on officially declared and real. The primary are embedded in organization documents and expressed in contacts with external partners and authorities. The second are usually observable in concrete previously announced actions.

Information, preferences and knowledge are essential components of every decision process.

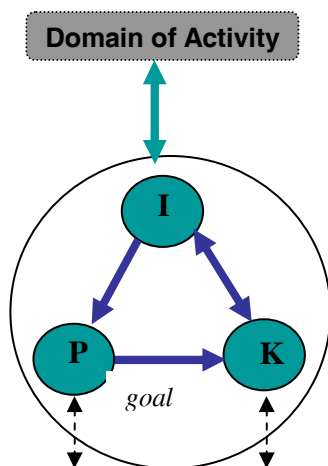


Fig. 3 IPK cell it is an elementary component of the TOGA computational mind model.

It works as follow:

- Signals arrives from a Domain-of Activity. They are transformed to new *information* using a *conceptualization* system and *descriptive knowledge*.
- Information is confronted with *preferences* what produces an *intervention goal*.
- Goal enable to choice *operational knowledge*
- Operational knowledge processes information: $I' = K_j(I)$, $j=1, \dots, N$, where choice of j depends from the goal.

Obtained information indicates how to modify Domain of Activity. If one of

the above operations is impossible then the cell is inactive or sends this meta-information to a higher level IPK cell, what is indicated by thin arrows. In these cases, P or K systems are considered as new domain of activity on the meta-reasoning level.

Conceptualisation system is a system of concepts which provides components for the construction of models and methods for their changing. It can be represented in frame of TAO as a set of meta-objects (or object-frames), their possible meta-interrelations (relation-frames) and

permissible meta-changes (changes-frames). In the « production » perspective, they are cognitive materials, tools and possible operations.

Conceptualization systems (C) are developed through the acquisition of human individual experience and by conscious learning. They are characterized by the following main properties:

- is possible to have a few C-systems; usually they refer do different classes of the domains of activity, and are developed from different points of view.
- they are not well separated; the same concepts and terms are used in different C-systems.
- they are only partially conscious for their owners; C-systems are usually hardly available consciously and not-consciously (automatically) used during everyday reasoning processes. Some their part “works” on subsymbolic neural network level.
- they are dynamic and modifiable; C-systems can evolve not consciously as a consequence of acquired experience and can be modified by self or group learning during special courses and trainings.

The proper use of a C conceptualization may leads to a problem solution but if it is impossible a modification of C became necessary.

Generic Decision-making

Main element of intelligent agents’ mental activity that causes goal-directed human behavior is a decision-making process.

The IPK conceptualization enables to define a generic decision-making process. Abstract IPK systems are basic necessary carriers of decisional process (D-M), and D-M can be represented as follows:

$I'' = \text{Complex_Choice_Operator } [I,P,K] I'$, where I' is an information which activates D-M, and I'' is an information which includes decision.

On the other hand, $\text{Complex_Choice_Operator } (Cr, Al)$, Where Cr denotes criteria and Al denotes alternatives.

Decision-making: it is an individual or group reasoning activity/process implied by the request/necessity of a choice caused by received information or task, or by delivered conclusion about possibility of risks/benefits. It is started when either choice criteria are unknown or intervention alternatives are unknown, and is finished when choice is performed. Therefore, we may write: $Cr ([I,P,K], \text{ and } Al[I,P,K]$

We distinguish:

Action-oriented decision-making: it is a decisional process when alternatives represent possible actions in pre-chosen physical domain.

Mental decision-making: when the final choice refers not to actions but to conceptual objects related to a preselected abstract domain of activity of intelligent agent.

Group decision-making: when responsibility for decision is allocated to a group of intelligent agents and is based on a shared decision-making process.

Fig.4 illustrates IPK employed in D-M.

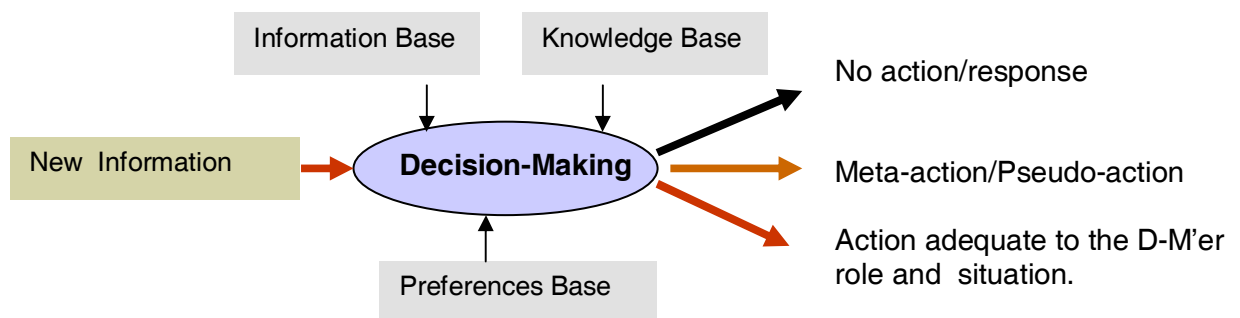


Fig. 4. An interrelation between IPK bases and Decision Making process.

Universal Management Paradigm (UMP)

UMP extends the URP paradigm over the relative functional structure of interactions of a manager.

This structure is also a functional definition of the manager concept in TOGA.

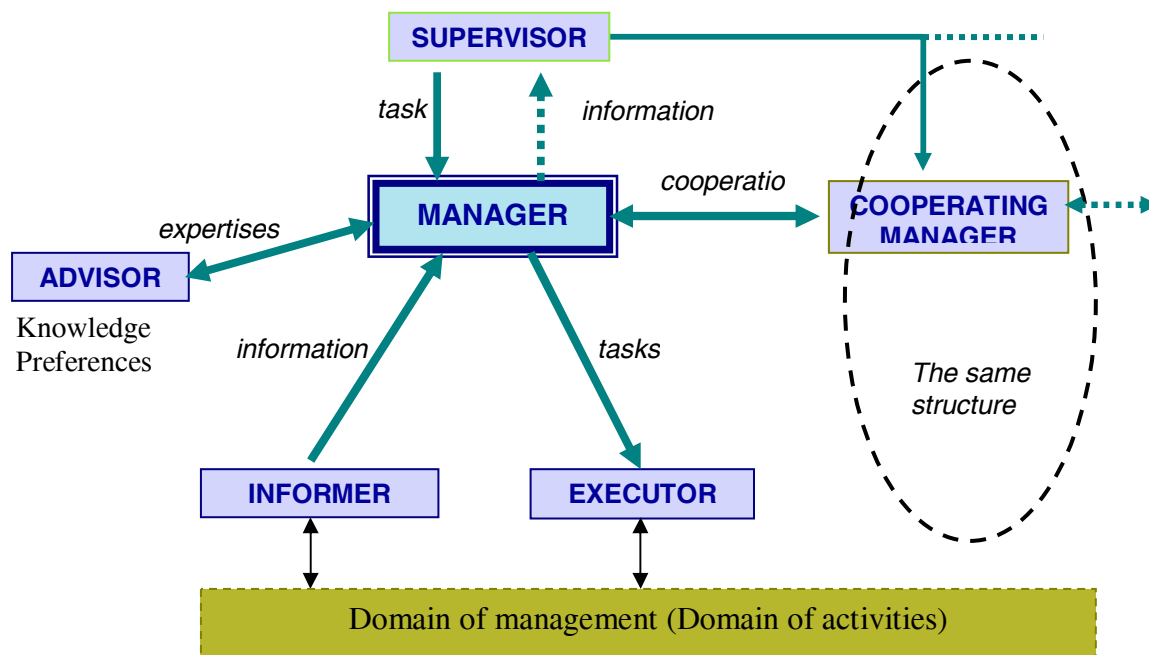


Fig. 5. Necessary components of the management process and their main interrelations according to the Universal Management Paradigm (UMP) [10].

UMP defines relative **roles** (Fig. 5) and their main interrelations in frame of an organization, where a role is defined by (competences, responsibility, privileges).

Competences: they define what intelligent agent is able to do and its possessed models of the domain (knowledge)

Responsibilities: they includes tasks, duties and requested or just own preferences

Privileges: It defines access to the information which produces conceptual images of the domain, and the range of executive power, i.e. possibility to activate execution resources (information).

As we see, every role is specified by its own IPK sets. Every element of the UMP structure is subjective, incremental and recursive.

In this context, human organization can be defined by reciprocally dependent roles, its structure, decisional mechanisms and resources of interacting/communicating intelligent subjects that should act in order to achieve a common goal (usually defined in the organization statute).

SPG Universal Domain Paradigm (UDP)

UDP serves for the specification of *Domain of Activity* of an abstract intelligent agent. From the external modeler perspective, it is a framework of the conceptualization of the relation between an organization and its foundation-goal in terms of independently defined : systems, processes, functions and intervention-goals. It is also called the SPG approach. Shortly speaking, UDP integrates subjective and objective points of view on the organization.

The relations between these concepts are graphically presented on the Fig. 6.

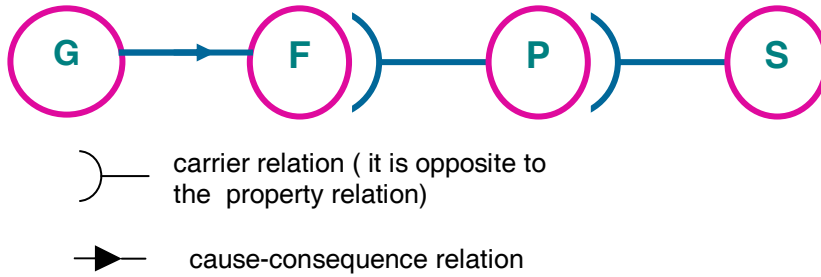


Fig. 6. Representation of a system in terms of the relation (System, its Goal). It is formally decomposed into four network layers: G- design/foundation goal, F – functions, P – processes, S – systems.

Here, the essential difference between function and process is stressed. Function is a goal-oriented property of an artificial system; Process is an identifiable or designed carrier of a function. We should remark that in this conceptualization, physical natural systems are described only by system object-based representation, and by processes dependent on variables and parameters. SPG framework can be considered as a descriptive meta-knowledge. It means, it enables a structuring of a specific domain-knowledge.

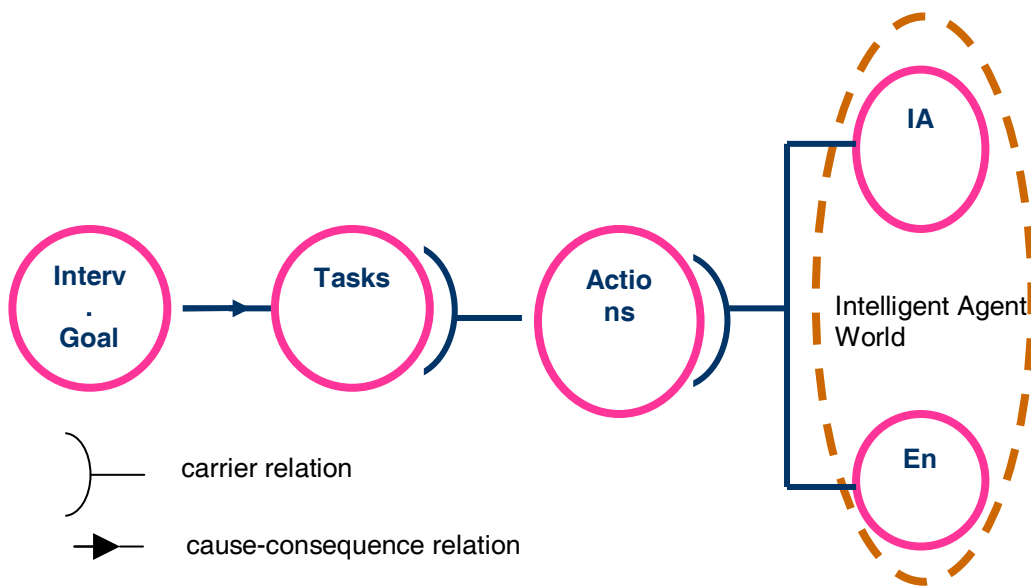


Fig. 7. WAG is a formal decomposition of the relation between Intelligent Agent World and agent's Intervention-Goal. IA – intelligent agent, En – its environment.

WAG Universal Activity Paradigm (UAP)

UAP is a last meta-knowledge framework for the conceptualization of the relation between the problem world and an intervention goal of intelligent agent (World-Action-Tasks-Goal interrelation).

UAP is illustrated on Fig.7.

The key concepts of this layered interrelations are *task* and *action*. Task is the specification of what has to be done, and action is a specification how it is or can be executed. In this sense, one task can be executed in different manners by different actions.

All the above introduced concepts are, in parallel, representable in frame of the TAO subtheory.

Vulnerability modeling

Here we demonstrate how before presented conceptual and methodological frameworks can be useful for the coping with the identification of the organizational vulnerability. In particular cases, we illustrate it on organizations which manage Large Complex Critical Infrastructures (LCCI).

Vulnerabilities recognition (taxonomy)

It is difficult to recognize organizational vulnerability in general and in particular circumstances. Vulnerabilities of organization are hidden states. The real visible symptoms of vulnerability are just associated with an organization crisis when the routine bureaucratic functioning is inefficient. Therefore an identification of the routine critical efficacy, Ef_2 should be here an important indicator, see fig.2.

A diagnostic approach requires a backward reasoning from uncertain symptoms to the causes. In this preliminary paper we are rather focused on the rough identification of the possible causes of vulnerability applying the TOGA top-down models and paradigms.

Using these frameworks we should be able to propose a working taxonomy of the key causes of organizational socio-cognitive vulnerability.

We distinguish sc-vulnerability caused directly by humans, and vulnerability caused by organization properties. For example, a competent manager is not able to complete in time a decisional process for the reason of too complicated and long hierarchical control procedures. We may state that organization structures influence strongly organizational decisions.

Identification of the causes of vulnerability

In a centralized organization, any symptom of inefficiency is caused by not adequate to its mission, available information, preferences and knowledge, as well as, their applications in organizational decisional processes

This IPK is distributed among managers and other employees. For the reason of their high autonomy, every employee has his/her own IPK which is only partially observable and only its part includes the IPK required by his formal role in the organization. Especially that individual IPKs are protected by personal privacy laws. These hidden IPKs may influence critically the organizational decisions.

The essential psychological feature, which is the product of invisible preferences systems, is individual motivation of employees. The motivation is not stable property of the human mind and depends on numerous individual and organizational factors.

Every dynamic system tends to homeostasis, in case of humans it is focused on the congruence between the image of the world and their preferences system. A lack of such congruence generate positive or negative for organization motivations.

If decision-making autonomy increases then the efficacy of the organizational control decreases, and importance of ethics and personal motivation increase. This plausible rule indicates the importance of motivation management. The theories of motivation and the motivation management are widely analyzed using soft-modeling approach in the subject matter literature [see Web].

In such context, psychological vulnerability is an insufficient resistance on stress situations and leads to irrational decisions and behaviors.

From the top-down perspective, socio-cognitive analysis takes under consideration the interests and points of view of owners, operators and customers of LCCIs :

- + LCCIs customers need the reliability and continuous providing of the services as long as possible and at low cost as possible.
- + LCCIs operators wish to be well informed about the infrastructure state and require its efficient management to satisfy customers expectations
- + LCCIs owners are focused on the politico-economic aspects of LCCIs.

These three objectives refer to different but not separable domain of activities, are based on different preferences systems, and their conflicts may lead to the conflict of interests and to the vulnerability of organization top-management .

Individual IPK and organizational decision-making

Main taxonomy criteria of sc-vulnerability are based on the analysis of: individual IPK, roles and interdependency networks/structures, individual capacities and emotional and motivation status.

The first is IPK based, it includes a separation of individual professional IPKs, IPK_p from the IPK of the organization, IPK_o .

Human individual errors can be caused by:

- Not proper or not sufficient information
- Lack or not proper Importance Scale (preferences, risk assessment)
- Not proper or not sufficient instructions, procedures (knowledge)
- Wrong cognitive and organizational factors related to emotional motivations.

The second aspect refers to the relation between roles expected and requested by organization and these really existing.

Every employee is in three roles together:

1. organizational role – requested and defined by the structure (fixed)
2. informal role – applied, structure independent (variable), which determines informal influence of one employee on others.
3. personal/real role – really realized professional role in frame of responsibilities structures (it is variable).

These types and dynamics of the roles may create different lacks of congruence between them leading to conflict of interests. Such situations during group decision making cause: necessity of negotiations, compromise acceptance, and finally, may cause inefficient risky decisions.

More precisely, conflict of motivations and interests is based on the risk-benefits assessment, which can be essentially different from the individual and organizational perspectives. On the rational level it refers to three preferences systems representing: social interest, organization interest and personal interest.

All of them influence organizational decision-making and improper or insufficient information and knowledge also lead to pathological decisions, such as, meta-decisions and pseudo-decisions.

Meta-decisions include, for example, decision of not decision-making, decision delaying, refuting of the problem. The official motivations of such decisions can be numerous and usually refer to the expected not specialist IPK of the decision evaluators, such as, society, mass media, manager's authority.

Pseudo-decisions are decisions that provide an answer/solution on similar problems and are represented in another conceptualization system. In these cases, lack of proper decision is hard to observe but their consequences may lead to the important losses for the organization.

The individual pathological decisions, especially in centralized organizations, are reinforced by rigid organization dependency structures, where subordinated manager roles do not enable critical feedbacks and wrong decisions are propagated to the executive level.

Cognitive reasoning factors, which cause ineffective or improper decisions, can be explained using the UDP and UAP paradigms. They rely on insufficient or not real situation assessment and its conceptual components should be analyzed in details.

It is evident that, the above pathologies increase strongly organizational vulnerability.

The next important tool for the vulnerability analysis is the Universal Management Paradigm. It enables to identify its numerous potential sources.

Every element of the management ensemble presented on the Fig 5 has proper IPK system and can be object of vulnerability. The second its source, which is not less important, is a communication network. All these aspects can also be simulated in frame of complex analysis of different combinations of parallel multi-source sc-vulnerabilities, and their propagation in short time intervals, as well as, in full organization life cycle (see Fig.1) For example, vulnerability of collaboration can be simulated as a vulnerability inside of organization, and, as well as a vulnerability of intradependences of the network of the cooperating organizations.

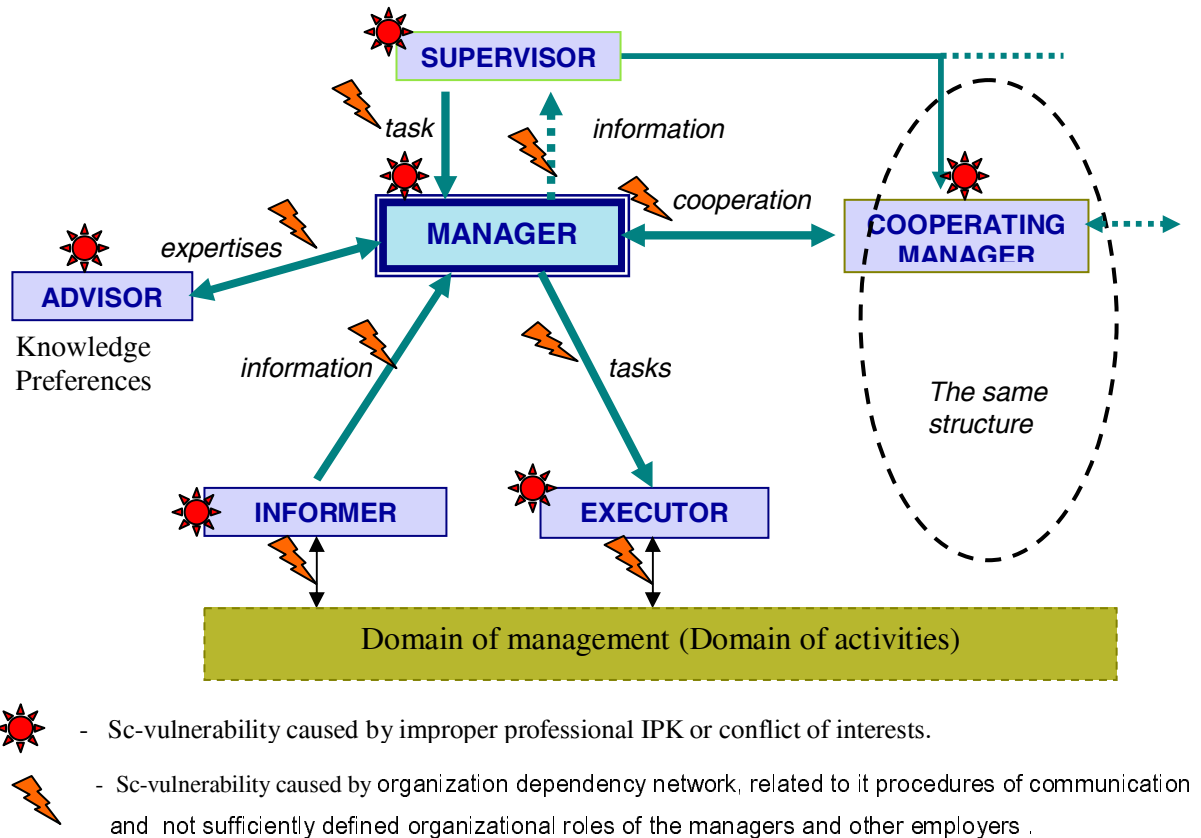


Fig. 8. Possible sc-vulnerabilities projected on the Universal Management Paradigm schema.

Conclusions

The article preliminarily investigated the relations between theoretical frameworks of the Top-down Object-based Goal-oriented meta-theory being developed in ENEA, since 1989, and the complexity of human based vulnerability of organizations.

For the reason of this complexity, we argue that possible dangerous organization pathologies ought to be recognizing by a specially nominated "vulnerability officer". This role should be established, especially in large LCCS organizations and in local and national emergency management institutions. On the other hand,, the obtained results are promising and encouraging to the continuation this research towards computer simulation of possible socio-cognitive vulnerabilities, as well as, for the exercitation of various strategies of the vulnerability elimination.

The work has been performed in the frame of the following ENEA's national and EU projects: CRESCO (Centro Computazionale di Ricerca sui Sistemi Complessi), IRRIS - Integrated Risk Reduction of Information-based Infrastructure Systems, FP6-2005-IST-4, CI2RCO (Critical Information Infrastructure Research Co-ordination).

References

1. Adrian Gheorghe, Dan V. Vamanu. Quantitative Vulnerability Assessment (QVA) for Critical Infrastructures. ETH Zürich , 2005.
<http://www.lsa.ethz.ch/research/projects/closed/aidram/qva>
2. Addis T. R., (1990) 'Knowledge for Design', Knowledge Acquisition, Vol. 2, pp. 95-105,
3. Gadomski Adam M., Nanni V., Intelligent Computer Aid for Operators: TOGA Based Conceptual Framework. Proceedings of "Second International Conference On Automation, Robotics, and Computer Vision", Singapore, Sept.1992. Also the document of ENEA/INN Informal series "Research notes on Abstract Intelligent Agent" N.6.
4. Gadomski Adam M., (2003), Socio-Cognitive Engineering Foundations and Applications: From Humans to Nations, Preprints of SCEF2003 (First International Workshop on Socio-Cognitive Engineering Foundations and Third Abstract Intelligent Agent International Round-Tables Initiative), Rome, 30 Sep. 2003 (in publishing).
5. Gadomski Adam M. ,Socio-Cognitive Scenarios for Business Intelligence Reinforcement: TOGA Approach, The paper preliminary accepted for publication in "Cognitive Science" ,Springer V.
6. Hannan, Michael T., and John Freeman, (1984): "Structural Inertia and Organizational Change." American Sociological Review, 49 149-164.
7. Cox, D.R. and D. Oakes. (1984). Analysis of survival data. Chapman and Hall, New York.
8. Gadomski Adam M. (1994), TOGA: A Methodological and Conceptual Pattern for modeling of Abstract Intelligent Agent. In Proceedings of the "First International Round-Table on Abstract Intelligent Agent". A.M. Gadomski (editor), 25-27 Gen., Rome, 1993, Publisher ENEA, Feb.1994. <http://erg4146.casaccia.enea.it/wwwerg26701/Gad-toga.htm>
9. Gadomski Adam M., S. Bologna, G.Di Costanzo, A.Perini, M. Schaerf. (2001), Towards Intelligent Decision Support Systems for Emergency Managers: The IDA Approach. International Journal of Risk Assessment and Management.
10. Gadomski Adam M. Personoids Organizations: An Approach to Highly Autonomous Software Architectures, "11th International Conference on Mathematical and Computer Modeling and Scientific Computing,: Concurrent Engineering Based on Agent-Oriented and Knowledge- Oriented Approaches", March 31 - April 3, 1997, Georgetown University Conference Center, Washington.
11. Amburgey, Terry L., Dawn Kelly, and William P. Barnett, "Resetting the Clock: The Dynamics of Organizational Change and Failure." Administrative Science Quarterly, 38 (1993): 51-73.
12. Simon, H. (1976), *Administrative Behavior* (3rd edition). New York: The Free Press.
13. Allison, G., Foresman Scott (1997), *The Essence of Decision*. Glenview, IL:
14. Robert, B., and Lajtha, C. (2002). A New Approach to Crisis Management. Journal of Contingencies and Crisis Management, 10(4), 181-191

Author Biography

Adam Maria Gadomski: with ENEA since 1984, MSc in nuclear physics at the Warsaw University, doctor degree recognised by the Physics Faculty of the Rome University "La Sapienza"; member of international scientific boards and referee for sc. journals related to intelligent agents technologies, systemic cognitive sciences and risk management. In Poland: Assistant Professor, head of Identification and Diagnostic Lab. in Nuclear Safety Department at the Institute of Atomic Energy; co-ordinator of the Computer-System Project for the Polish National Centre of Oncology. Gadomski is the author of more than 130 scientific papers where he contributed in particular to complex system modelling and the development of intelligence-based decision-support tools for high-risk management. He is the author of the knowledge ordering meta-theory TOGA (Top-down Object-based Goal-oriented Approach). He has promoted (general chair) several international workshops on abstract intelligent agents, socio-cognitive engineerings, m-learning and emergency management, <http://erg4146.casaccia.enea.it/>.