Scenarios of Societal Security and Business Continuity Cycles

Jiří F. Urbánek, Jiří Barta

***Abstract*—**Societal security, continuity scenarios and methodological cycling approach explained in this article. Namely societal security organizational challenges ask implementation of international standards BS 25999-2 & global ISO 22300 which is a family of standards for business continuity management system. Efficient global organization system is distinguished of high entity´s complexity, connectivity & interoperability, having not only cooperative relations in a fact. Competing business have numerous participating ´enemies´, which are in apparent or hidden opponent and antagonistic roles with prosperous organization system, resulting to a crisis scene or even to a battle theatre. Organization business continuity scenarios are necessary for such ´a play´ preparedness, planning, management & overmastering in real environments.

***Keywords*—**Business Continuity, Societal Security Crisis Scenarios Cycles.

I. Introduction

THE societal security understanding and continuity scenarios methodology takes into account also the sight toward problem clarification and implementation of processes cycling approach. The term Societal Security was first used by B. Buzan [2] in the book *People, states and Fear: National Security problem in International relations*, (1991). In Czech language, according Czech explanatory dictionary, the term ´societal´ is enforce translated as a word "societární". However, "r" letter instead ´l´ isn't right in international language context. Now, the Societal Security is comprehended [8], [9] as integrated range of interconnected disciplines including: asset protection (human, physical, environmental, financial, tangible and intangible), security, risk management, preparedness, crisis management, emergency management, business continuity management, recovery management and disaster management. Nevertheless societal security standardization addresses the challenges for the organizations, groups of organizations and society, facing up to disturbances closely before, during and after disruptive events.

The systems and processes of prosperous organizations at the beginning of 21th century embody the characters, property and behavior, resulting from their cooperative or competitive globalization. The globalization takes place on too many levels; however standardization and security levels are especially treated here. Efficient global organizational systems are distinguished of high connectivity, complexity and radical demand on their interoperability. It is resulting from their mutual interactions, avocatory pertinent relationships among participating players' entities of these systems. These entities are not only in cooperative relations in real environments! But always there have been numerous participating ´enemies´, which are in apparent or hidden opponent roles with prosperous organization system. They can overgrow till in antagonistic dramatically irreconcilable relations, resulting to a crisis scene [12] or even to a battle theatre.

The scenarios of such ´the plays´ then always are enacted on net integrated structure on many process´ chains and environments. They operate on a scene of more or less competitive, however always complex influencing special interests: on commodity, informative, financial, production, organizational, and personal and others for these play important relations [10]. Together with complexity growth [13] of global organization systems is developing & growing system´s hazard of antagonistic relations, which doesn't greater organizational profit, but contrariwise, it eliminates its effects. However, it is necessary to notify old knowledge that namely the process structure of any organization system isn't static, but it changes dynamically, innovates [3] and forms in real-time. System´s dynamics is characterized by global interdependence, mutual interactions, information feedbacks and circular causalities [9]. System and its process dynamics is possible to describe then as mutual dependence and incidence of system entities. In every system, the cyclic feedback loops run to an incidence of mutual bindings and response. Where the feedback is, there a loop or even cycle can be found. Their existence is conditioned by information diffusion, relevant definite activities if, within pertinent system after certain time, they return back to starting point, influencing next system activities. The feedback underlies the systems structure and at the same time is determinant of its behavior. The interconnection and influence of entity´s and system´s component bindings and feedbacks in the cycle, it is possible titled as a relation (-ship) [11]. The relation then, in real time and owing to an environment, can change entity´s intensity and systemic importance.

Feedback existence is natural in every system. Nevertheless, during system crisis development, the feedbacks can operate in mode and impact that are not common in ´peace time´. Such the feedback is possible titled as negative, regarding its necessity of changes enforcing of system behavior. For example [1] said for bank's sector: *Negative feedback of banks debts balance and subsequently pertinent*

J. F. Urbánek is professor at the Department of Civil Protection, University of Defence, Kounicova 65, 662 10 Brno, Czech Republic (phone: +420603326355; e-mail: jiri.urbanek@ unob.cz).

J. Barta works as a lecturer at The Department of Civil Protection of University of Defence and he is studying a doctorate at the University of Defence. Kounicova 65,662 10 Brno, Czech Republic (e-mail: jiri.barta@unob.cz).

decreasing of its rating causes financing costs increasing, which reduce its future ceteris paribus and this bank is more vulnerable, because its resulting rating decreasing would be able to bring ′a waste of the possibilities of other financial resources obtaining′ on inter banking market. However, negative feedbacks have system′s self-regulation character and they operate so like specific automatic stabilizer, contributing to an elimination of system′s crisis. That is why, so the changes [6] are compensated by feedbacks here, inducing for example: *values growth of system′s entity A lead to lower value of B entity, than it would was without the changes.* However, positive feedback (a growth in A lead to higher B, than it would was without the changes), needn't operate just in ′positive words sense′, but they can evoke negative feedbacks even [5], for example: *prices fall in a realty market evokes declining in consumer's expense, that have more and more weaken realty market and spread further to the others economy sector* [7].

II. Cycling of Business Continuity Scenarios

The cycles are native for a course almost of all natural or man-made processes. E.g.: for the state and influence of financial organizational system on the real economy is excellent detector *a ′procyclicality′ mechanism*, amplified natural amplitude of economic *cycle*. For example *excessive ′procyclicality′embodies of such a fluctuation that has induced excessive expense reinforcement of real economies and it is resulting to a health damage of financial sector* [4].

General question asserts to the foreground of system′s vulnerability and security during not only economic, but any processes ′life cycles′: *How is the resilience and resistance of any ′processes life cycle′ against relevant threats and hazards, relating to particular entities, or even to whole complex organizational system?* Not only for economic, but also for all other sectors of human society, the answer can be obtained from the analyzing, planning, testing and auditing procedures, according of international BS 25999-2 and global ISO family 22300 standards [14]-[16] - for a Business Continuity Management System - BCMS. Next figures are the ′blazons′, modeled by DYVELOP (Dynamic Vector Logistics of Processes) method [10]-[13].

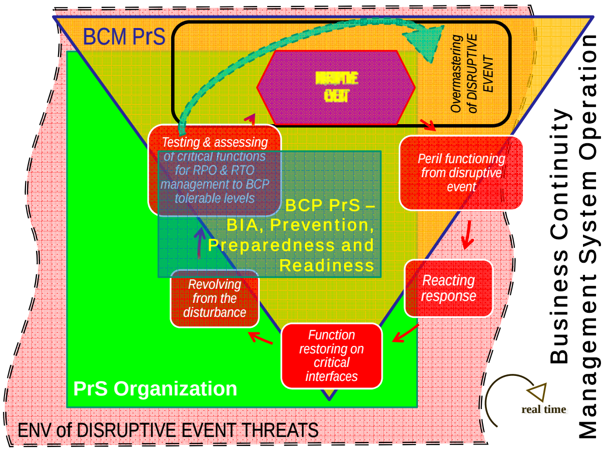
BCM PrS
DISRUPTIVE EVENT
Overmastering of DISRUPTIVE EVENT
Testing & assessing of critical functions for RPO & RTO management to BCP tolerable levels
Peril functioning from disruptive event
BCP PrS – BIA, Prevention, Preparedness and Readiness
Revolving from the disturbance
Reacting response
Function restoring on critical interfaces
PrS Organization
ENV of DISRUPTIVE EVENT THREATS
real time
Business Continuity Management System Operation

Fig. 1 Blazoning scenario of BCP with life cycle operating for a use case ⟨⟨Overmastering of extraordinary event⟩⟩

The BCMS acts as a part of organizational total management system. It sets and innovate a continuity cyclic process approach of total integrated management system activities and processes in whole Organization′s ′life′ cycles. As the business continuity management Process System (i.e. ′PrS′, having sharp corners tetragonal symbol DYVELOP blazonry) = ⟨⟨BCM PrS⟩⟩ for Business Impact Analysis= BIA [13] and for prevention, preparedness and readiness processes is used Business Continuity Planning PrS i.e. ⟨⟨BCP PrS - BIA, Prevention, Preparedness and Readiness⟩⟩ at above Fig. 1. Here in DYVELOP blazoning scenario, this ⟨⟨BCP PrS-BIA, Prevention, Preparedness and Readiness⟩⟩ works permanent and systematically for production Organization = a ⟨⟨PrS Organization⟩⟩ at its environment [11] = ⟨⟨ENV of DISRUPTIVE EVENT THREATS⟩⟩, producing threats prediction, prevention, preparedness and readiness, as well as analysis, solution design, implementation, testing of organizational acceptance and maintenance services for the ⟨⟨PrS Organization⟩⟩. These services are used only, if DYVELOP blazonry (hexagonal shaped) a ⟨⟨DISRUPTIVE EVENT⟩⟩ occurs in necessary crisis/ emergency operation of business continuity management ⟨⟨ BCMPrS⟩⟩ (DYVELOP triangle symbol). It is clear that the ⟨⟨ BCM PrS⟩⟩ response procedure is initiating only *after* ad hoc ⟨⟨DISRUPTIVE EVENT⟩⟩ occurrence, which activates *′critical functions′*! Then it repeat acts and operates in a cycle of Use Cases (having rounded corners tetragonal symbol DYVELOP blazonry): *⟨⟨Peril functioning from disruptive event → Reacting response → Function restoring on critical interfaces → Revolving from the disturbance → Testing & assessing of critical functions for RPO & RTO management to BCP tolerable levels⟩⟩.*

The function may be considered critical if the implications of damage are regarded as unacceptable for Organization′s stakeholders. The perceptions of the acceptability of disruption may be modified by the cost of establishing and maintaining appropriate business or technical recovery solutions. A function may also be considered critical if it is dictated by a law. For each critical function, two values must be then identified: Recovery Point Objective (RPO) – it identifies maximum tolerable data loss for each activity, which cannot be exceeded; And Recovery Time Objective (RTO) – it identifies acceptable amount of time to restore the functions, till the Maximum Tolerable Period of Disruption (MTPD) [16]. This use cases cycle is multiple repeating to the RPO & RTO successful obtaining. It brings ⟨⟨DISRUPTIVE EVENT⟩⟩ elimination and consequently it's *⟨⟨Overmastering of DISRUPTIVE EVENT⟩⟩*. It guarantees satisfy organization continuity, improving the ⟨⟨BCP PrS – BIA, Prevention, Preparedness and Readiness⟩⟩ process system.

III. Business Continuity Management System Life Cycles, Operation and Implementation

A life cycle of critical (urgent or crisis) organizational functions/ activities is displayed at Fig. 2. Here the Business Continuity Management System – a ⟨⟨BCMS⟩⟩ (PrS intriangle shape) brings next providing process system (PrS) phases, operating into a *⟨⟨*Business Threats ENV⟩⟩, looping at organization use case *⟨⟨organizing Business Continuity⟩⟩*,in an agreement with global standard draft ISO/DIS 22313: ⟨⟨Analysis → Solution design →Implementation → Testing and organizational acceptance → Maintenance⟩⟩.

A. Analysis Phase

Analysis phase (see PrS⟨⟨ANALYSIS⟩⟩ on Fig. 2) is very important for BCP manuals (handbooks, documents) development and it is fully in process system of business continuity management ⟨⟨PrS BCMS⟩⟩ arrangement, where with be enacting inside of its ´triangle´. This phase consists from an *impact analysis, threat analysis* and *impact scenarios. Impact analysis (Business Impact Analysis, BIA)* results in the differentiation between critical (urgent or crisis) and non-critical (non-urgent) organization functions/ activities. A criterion if the function is critical is explicitly defined by Organization´s business stakeholders and relative laws. Implicitly - by the cost of establishing and maintaining appropriate business or technical recovery solutions and by RPO, RTO& MTPD identification. Impact analysis results in the recovery requirements for each critical function, consisting from business and/or technical information.

Threat analysis comes after defining recovery requirements, documenting potential threats and it is recommended to detail a specific disaster's unique recovery steps. Some common threats include the following: Disease; Earthquake; Fire; Flood; Cyber attack; Sabotage (insider or external threat); Hurricane or other major storm; Utility outage; Terrorism; Theft (insider/ external theft, vital information or material); Random failure of mission-critical systems and Economic crisis.

Impact scenarios definition comes after of potentially operating peril, documenting the business recovery plan recommendation in impacts. The most wide-reaching disaster or disturbance is preferable to plan for a smaller scale problem, because almost all smaller scale problems are partial elements of larger disasters. A business continuity plan may also document additional impact scenarios.

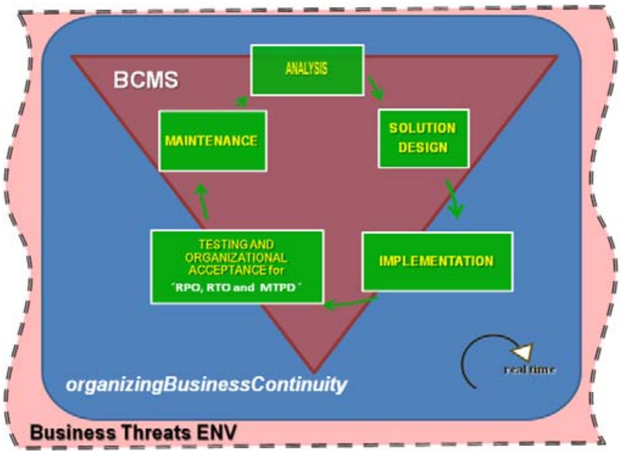
BCMS
ANALYSIS
SOLUTION DESIGN
MAINTENANCE
TESTING AND ORGANIZATIONAL ACCEPTANCE for ´RPO, RTO and MTPD´
IMPLEMENTATION
real time
organizingBusinessContinuity
Business Threats ENV

Fig. 2 Blazoning Scenario of Business Continuity Management System Life Cycle Operation

B. Solution Design Phase

PrS ⟨⟨SOLUTION DESIGN⟩⟩ on Fig. 2 has an aim to identify the most cost effective disaster recovery solution. This BCP phase overlaps with disaster recovery planning methodology. The solution phase determines: the crisis management command structure; the location of a secondary work site; telecommunication architecture between primary and secondary work sites; data replication methodology between primary and secondary work sites; the application and software required at the secondary work site, and the type of physical data requirements at the secondary work site.

C. Implementation Phase

PrS ⟨⟨IMPLEMENTATION⟩⟩ on Fig. 2 is the execution of the design elements, identified in the solution design phase. Work package testing may take place during the implementation of the solution. However; work package testing does not take the place of following organizational testing. This phase according scenario of BCMS operates partially on real ⟨⟨PrS Organization⟩⟩.

IV. Testing and Organizational Acceptance System Development

PrS ⟨⟨TESTING ORGANIZATIONAL ACCEPTANCE⟩⟩ purpose is to achieve organizational acceptance that the business continuity solution satisfies the organization's recovery requirements. Manuals, scenarios, projects and plans may fail to meet expectations due to insufficient or inaccurate recovery requirements, solution design flaws, or solution implementation errors. Testing may include: Crisis command team call-out testing; Technical swing test from primary to secondary work locations and contrariwise; Application test and Business process test. Problems, identified in the initial testing phase may be rolled up into next maintenance phase and retested during the next test cycle. This phase according scenario of ⟨⟨BCM PrS⟩⟩ operates partially on real ⟨⟨PrS Organization⟩⟩ also.

V.Maintenance Phase

PrS ⟨⟨MAINTENANCE⟩⟩ phase of a BCP manual is broken down into three periodic activities. The first activity is information confirmation in the manual, rolling out to all staff for awareness and specific training for individuals whose roles are identified as critical in response and recovery. The second activity is the testing and verification of technical solutions, established for recovery operations. The third activity is the testing and verification of documented organization recovery procedures.

VI. Conclusion

Future societal security needs continuity scenarios and methodological cycling approach understanding. Its brief rules and outline, using international BS 25999-2& global ISO 22300 family standards implementation, brings this paper. These standards are served for business continuity management system purpose in organizational environments of competing business, resulting to cycling scenarios of crisis scene, events or even battle theatre. Organization business continuity scenarios are necessary for crisis/ emergency preparedness, planning, management & overmastering. They are modeled here by DYVELOP blazons, displaying necessary organizational and management functions & activities in real business threats and disruptive events environments.

References

[1] Aikman, D. et al. 2009. *Funding liquidity risk in a quantitative model of systemic stability*, Bank of England working paper No. 372.

[2] Buzan, T. *The Ultimate Book of Mind Maps*. Glasgow: Harper Thorsons, 2006.

[3] Drucker, P. *Innovation and entrepreneurial spiri*t, Management press, Prague, 1991.

[4] Gerlach, S. Grunewald, P. *Procyclicality of Financial Systems in Asia*, Hong Kong Institute of Monetary research. 2006

[5] Elliot, D. Swartz, E. Herbane, B. *Just waiting for the next big bang: business continuity planning in the UK finance sector*. Journal of Applied Management Studies, 1999, Vol. 8, No, pp. 43–60.

[6] Hammer, M. Champy, J. *Reengineering*, Management press. 1993.

[7] Kubicová, I. et al. *Analýzamikrofinančníchrizik a jejichpřenosů v kontextuzranitelnostičeskéekonomiky*, Hlávkovonadání, Praha, 2012, ISBN978-80-86729-76-3.

[8] Ludík, T., Ráček, J. Process Methodology for Emergency Management. IFIP Advances in Information and Communication Technology, Heidelberg: Springer 2011, 359, p. 302-309. ISSN 1868-4238.

[9] Richardson, G. P. *System dynamics*, In Encyclopaedia of Operations Research and Information Science, Saul Gass and Carl Harris, eds., Kluwer Academic Publishers, 2011.

[10] Urbánek, J. F. *New Instrument of Integrated Waste Management – DYVELOP*. In The Journal of Solid Waste Technology and Management, 1999, 15th International Conference on Solid Waste Technology and Management, Philadelphia, PA U.S.A. 9A 1-6 pages. ISSN: 1091-8043.

[11] Urbánek, J. F. *Teorieprocesů – management environmentů*, CERM Brno, 2003, ISBN 80-7204-232-7.

[12] Urbánek, J. F. a kol. *Scénářeadaptivníkamufláže*. Brno: Tribun EU s.r.o., 2012, ISBN 978-80-263-0211-7.

[13] Urbánek, J. F. et al. *Crisis Scenarios.* Brno: Univerzity of Defence, 2013. 240 pp. ISBN: 978-80-7231-934-3.

[14] BS 25999-2.

[15] ISO 22301.

[16] ISO/DIS 22313.

Professor Jiri F. Urbanek, Ph.D.was born 29th March, 1949 in Pelhrimov, Czech Republic. He was graduated 1972 at Brno University of Technology, Faculty of Mechanical Engineering. 14 years he operated in Czech industrial and mining enterprises, including technical help for mining rescue services. Parallel he was graduated Ph.D. with thesis Mathematical Methods in Industrial Processes. Then he gave the lectures on technological, managerial and military universities in the branches Automation, Cybernetics, Management, Logistics and Non-conventional Technologies. OnBrno University of Technologyhe habilitated in branch Mechanical Technology and later in branch Management and Battle Employment of Ground Forces in Vyskov Military University.

Now, he gives professor's lectures atUniversity of Defence, Faculty of Economics and Management in Brno, Czech Republic. His research branches are Safety, Civil Protection, Interoperability, Security Management, Crisis Scenarios and Civil Emergency Planning. He is European Commission expert for Security Research and for the Development of Small and Middle Enterprises. He solves many national and international research and development projects. Now is in the solution of EC 7FP Security Research project CAST. He is not WASET member to this date.

Jiri Barta was born 16th June 1977 in Vyskov, Czech Republic. He was graduated 2001 at Military University of Ground Forces in Vyskov, Faculty of Economic and Management. From 2003 to 2004 he worked as a lecturer at the Civil Protection Department of Military University of Ground Forces in Vyskov.He gave the lectures on Crisis Scenarios, Civil Emergency Planning and Information Systems for Crisis Management. Parallel he 11 years operated in the private sector in the field of insurance and family finances.

Since 2004he gives lectures at University of Defence, Faculty of Economics and Management in Brno, Czech Republic. His research branches are Safety, Civil Protection, Interoperability, Security Management, Crisis Scenarios and Civil Emergency Planning. He solves many national research and development projects. He is the author of more than 50 scientific articles, 2 patents and co-author of two monographs collective expertise.