Modeling and Analyzing Disaster Recovery Plans as Business Processes

Andrzej Zalewski, Piotr Sztandera, Marcin Ludzia, and Marek Zalewski

Warsaw University of Technology, Institute of Automatic Control and Computational Engineering, Warsaw, Poland
a.zalewski@ia.pw.edu.pl

Abstract. The importance of business continuity and disaster recovery (BC/DR) plans has grown considerably in the recent years, becoming a well-established practice to achieve organization's resiliency. There are several applicable standards, like BS 25999-1:2006, sets of guidelines and best practices in this field. BC/DR plans are typically text documents and exercising is still the main measure used to verify them. On the contrary, to the common practice we suggest to model BC/DR plans as business processes using ARIS methodology and models, which have proven successful in the Enterprise Resource Planning systems projects. This provides uniform representation of BC/DR plans that can be applied across the whole distributed organization, strengthens the efficiency of traditional manual analysis techniques like walk-throughs, helps to achieve completeness, consistency and makes possible computer simulation of BC/DR processes. Timing and dynamic behavior, resource utilization and completeness properties have been also defined. It is possible to analyze them with computer support based on proposed ARIS model of BC/DR plan.

1 Introduction

The catastrophes of last decade, like hurricane Katrina or terrorist's attack on World Trade Center in New York, have shown the importance of organization's resilience against severe disruptions. This caused a rapid development in the genre of Business Continuity, which resulted in:

- the development of a number of standards and recommendation sets – e.g. Business Continuity Management (BCM) standard BS 25999-1:2006 [1], Standard on Disaster/Emergency Management and Business Continuity Programs NFPA 1600 [4], recommendations for contingency planning by NIST, U.S. Department of Commerce [5];
- the inclusion of business continuity practices in IT services management standard ISO 20000 [2] and IT auditing standard COBIT [3];
- numerous books published on the topic of BCM – e.g. [6], [7], [8].

Business Continuity Managements system is implemented within an organization to enable structured, well-organized and timely recovery from severe disruptions. Business Continuity (BC) Plans (including Disaster Recovery Plans)

M.D. Harrison and M.-A. Sujan (Eds.): SAFECOMP 2008, LNCS 5219, pp. 113–125, 2008.

are a key element of this system. As these plans are of vital interest to the organization they should not only be diligently elaborated but also validated and verified (either during the development or during the audits and maintenance).

As it has been shown in section 2 most of BC/DR plans are currently textual documents of different levels of detail and formality. As such they are prone to incompleteness, inconsistency and other imperfections, being at the same time difficult to analyse and verify. To compensate for these disadvantages we advocate an idea of integrating Business Continuity Management with business process modeling to increase the level of formality of BC/DR plans.

BC/DR plans in our approach are treated as a specific kind of business processes activated only in case of severe disruptions. As such, they can be modeled with notations used for business process modeling. In this paper, we use Sheer's Architecture of Integrated Information Systems (ARIS) methodology and notation, which has proved successful in commercial applications, especially Enterprise Resource Planning systems projects. Formalizing one of the disaster recovery plans available from the Internet we show the superiority of formalized diagrammatic representation to traditional textual form of BC/DR plans. Definitions of the important properties of BC/DR plans modeled with ARIS and techniques of their analysis have been provided.

The rest of the paper is organized as follows: the missing parts of BC management are discussed in detail in Section 2, the core concept of the paper i.e. modeling of BC plans with ARIS methodology and models are presented in Section 3, analysis of ARIS models are discussed in Section 4, the results of the paper are discussed in Section 5, future research areas have been suggested in Section 6.

2 The Missing Parts of Business Continuity Management

BS 25999-1:2006 defines how to implement Business Continuity Management within an organization. It defines Business Continuity Management life cycle. The cycle starts from identifying critical services and products, business impact analysis and risk analysis. It is aimed generally at identifying recovery requirements and threats. These in turn lead to the identification of BC Management options and elaboration of appropriate response in the form of incident management, business continuity and disaster recovery plans. These plans play a key role in the resiliency assurance. All these arrangements are subject to exercises, maintenances, audits and self-assessment in the last phase of the BCM life cycle. Similar approaches have been presented in numerous papers (e.g. [13], [11]).

BCM practices seem to be present in the majority of large organizations in the developed economies (see survey for US [9]). The Internet research on the form of BC/DR plans – presented in table 1 reveals that most of the BC/DR plans are just textual documents. The list of analysis/verification techniques for BC/DR plans is rather short – it includes mainly manual methods like desk-checks, walk-troughs, simulations (manual) as well as executions of a part or even entire plan (see BS25999:1 [1]). Only simulations are subject to computer

Table 1. Disaster Recovery/Business Continuity plans level of formalization – survey of the practice

No.	*Organization / source*	*Level of formalization*
1	The Australian National Herbarium Canberra – the aim of the plan is to protect and restore the Collection. http://www.anbg.gov.au/cpbr/disaster-plan/	Low – DR plan represented as textual enumeration organized into chapters and subchapters.
2	University of Arkansas – the aim of the plan is to restore all computer operations without loss of any data. http://www.uark.edu/staff/drp/	Low – DR plan represented as textual enumeration organized into chapters and subchapters.
3	University of California – the aim of the plan is to protect and restore the book collection of the general library. http://palimpsest.stanford.edu/bytopic/disasters/plans/ucdaviis_disasterplan2004.pdf	Low-medium – emergency plans represented as textual enumerations, short sentences are used. There is a lot of white space used between each step in printable version to make easy the orientation in the plan.
4	Systems Support Inc. – the aim of the MIS Contingency Plan is to protect corporate resources and employees. http://www.drj.com/articles/drpall.html	Medium – detailed recovery plans presented as textual enumerations, actions are presented in tabular form with explicate naming heading, executing person and action.
5	Massachusetts Institute of Technology – the aim of the plan is to restore critical functions of MIT and the resources required to support them. http://web.mit.edu/security/www/pubplan.htm	Low – recovery processes are presented as textual enumerations. Teams and their emergency actions have been described.
6	University of Arkansas Computing Services Disaster Recovery Plan http://www.uark.edu/staff/drp/	Medium – disaster recovery plans are presented in textual form (including both, actions and resources). Detailed description of roles, actions and resources, but without logical connections between them.
7	NIH Data Center http://datacenter.cit.nih.gov/pdf/disasterplan.pdf	Low – detailed recovery plans are presented in enumerated text form. People have not been explicitly assigned to the recovery actions.
8	Abilene Christion University http://www.acu.edu/technology/is/recovery.html#PCRecovery	Low – recovery action plans are presented in textual form. Disaster recovery teams and their responsibilities are described.

support. The efficiency of manual analysis methods is strongly limited by the textual form of BC/DR plans. Full assessment can be achieved only through real execution of a plan or its part. Apart from the costs of such an execution it is worth noting that there are important cases, in which such experiments

are risky themselves and probably would not be accepted by the appropriate authorities: consider case of an art gallery with a collection of precious paintings or sculpture.

The literature on the properties of BC/DR plans and their analysis is rather sparse – the problem has not been so far treated in its entirety – only narrow publications are available e.g. [10], [12].

3 Modeling BC/DR Plans as Business Processes

As a first step to resolve, the issues raised above we present how to model BC/DR plans using Sheer's ARIS methodology and notations – see [14], [15], [16]. The major competitors to ARIS seem to be Business Process Modeling Notation (BPMN) by Object Management Group as well as Unified Modeling Language. Both of them lack models of organization, data (resources) and products while they are focused on the flow of processing and documents (data). This is a major deficiency as all these elements are an integral and important element of every BC/DR plan. ARIS methodology, in turn, defines five views of an organization – organizational, data, function, product/service, process. All the elements comprising BC/DR plans can be assigned to one of those perspectives, which has been shown in table 2.

Table 2. Representation of BC/DR elements in ARIS Methodology

BC/DR element	*ARIS view*	*ARIS model element*
Role/Team Responsibility	Function	Function
Critical function	Function	Function
Supporting equipment and supplies	Data	Entity type
BCMS Documentation	Data	Entity type
Organizational structure	Organization	Organizational chart
Groups and Roles	Organization	Organizational chart
Senior Management	Organization	Position/Group
Stakeholders	Organization	Person type
Staff resources	Organization	Internal person
External services and supplies	Organization	External person
Activity	Function	Function
Business Continuity Plan	Process / Control	EPC diagram
Incident management plan	Process / Control	EPC diagram
Incident	Process / Control	Event
Business interruption	Process / Control	Event
Products and services	Product / Service	Product/Service
Business Continuity Management Life cycle	Process / Control	Value Added Chain Diagram

The modeling of BC/DR plans in each of the above perspectives has been presented below in Section 3.1 – 3.5 and illustrated on DR plan for the general library of the University of California [17] (see also table 1, pos. 3).

3.1 Organizational View of BC/DR Plans

The main model of the Organizational View is Organizational Chart. It models the internal structure of the teams engaged in BC/DR plans representing the relations between different members of those teams.

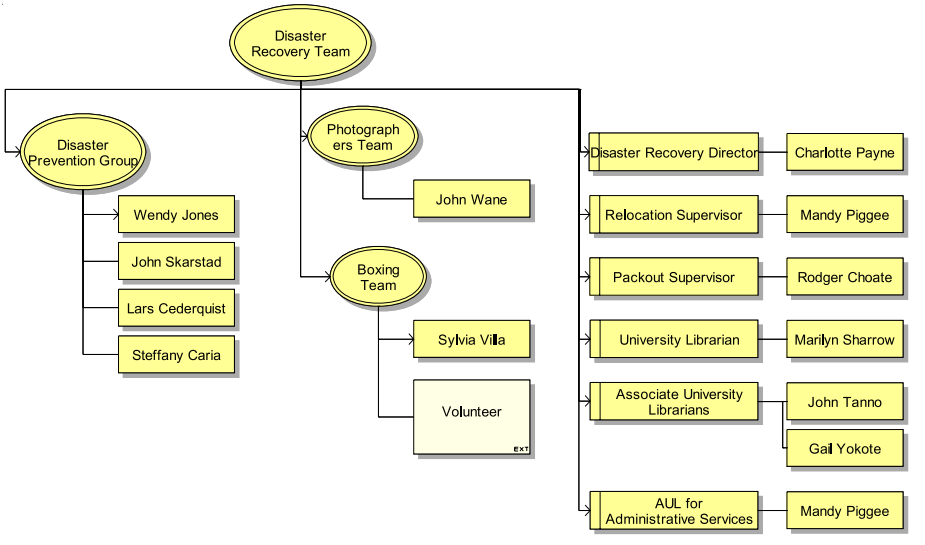

Fig. 1. The Organizational Chart of the Disaster Recovery Team

The Organizational Chart in figure 1 defines Disaster Recovery Team of the University of California. The enclosed diagram shows DR team consists of groups (Boxing Team) and positions like Disaster Recover Director. More information about the teams and their members can be registered as attributes of appropriate objects (see table 2).

3.2 Data View of BC/DR Plans

Data view models resources (excluding human resources) used in BC/DR plan. The relations between them are modeled as Entity-Relationship Model (ERM).

Figure 2 models some of the resources used in DR Plan of University of California, i.e. emergency box consisting of such first aid kit, camera and the other.

3.3 Function View of BC/DR Plans

The function view models functions (i.e. technical tasks or other activities) and their hierarchy. The latter is modeled with Function Tree Diagram. Functions are characterized by the attributes of costs or execution time, which are useful for simulation.

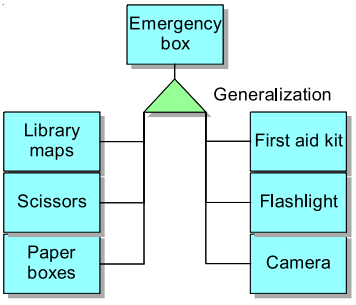

Fig. 2. The Entity-Relationship Model – The content of emergency box

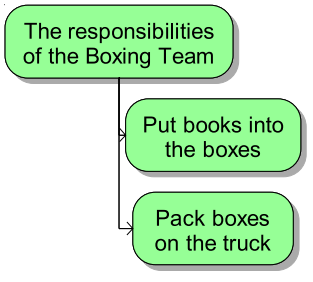

Fig. 3. The Function Tree - Responsibilities of The Boxing Team

The diagram in figure 3 presents the role (function) of Boxing Team in disaster recovery: they are responsible for putting the books into paper boxes and packing them onto the truck.

3.4 Product/Service View of BC/DR Plans

Product or Services are results of the execution of BC/DR plan. They are typically of different levels of abstraction constituting product/service hierarchy – several partial products make an entire higher-level product. This hierarchy is represented by the Product/Service Tree diagram.

The Product Tree diagram in figure 4 shows the partial products comprising "The pack out final report", which is one of the final products of the "Pack out process". It consists of budget, packing report and photographs. The budget is a product of function "Prepare a recovery budget", which is one of the functions in "Pack out process".

3.5 Process/Control View of BC/DR Plans

A Process View consists of two main models: Value-Added Chain Diagram (VACD) and Event-Driven Process Chain (EPC). They have been used to model the processes of BC/DR plans putting the data contained in all the other views into a single, legible model.

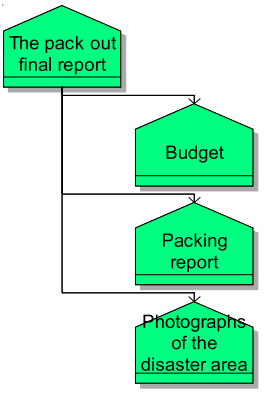

Fig. 4. The Product Tree - The partial products of The pack out final report

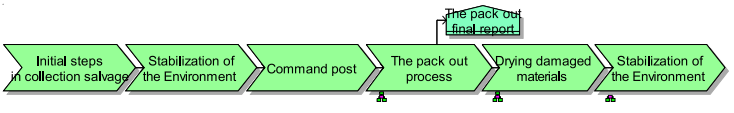

Fig. 5. Value-Added Chain Diagram – the simple processes of DRP

The VACD describes the top-level functions or processes. They usually form a chain illustrating the process of gradual achieving of a higher level goal (product).

Figure 5 shows process of Disaster Recovery Plan of the University of California, which consists of several subprocesses, among them is "The pack out" subprocess modeled below with EPC diagram.

The Event-Driven Process Chain models the procedures of BC/DR plan integrating the information from all the other views:

- resources defined in data views become inputs to the functions;
- products become outputs of the functions;
- elements of the organization view are assigned to the functions (activities) to show the responsibility of the BC/DR teams and/or their members.

The process is event-driven, as every functions is activated with the occurrence of an event and its completion also generates one or more events. Events are graphically represented as hexagons.

The EPC diagram in figure 6 models "The pack out" process. It starts when fire department gives permission to enter the affected area and finishes when the "Final report" is ready. Note that EPC diagram integrates all the information needed to understand and manage the modeled process. It makes possible simulation of a process providing information about cost, time and workload.

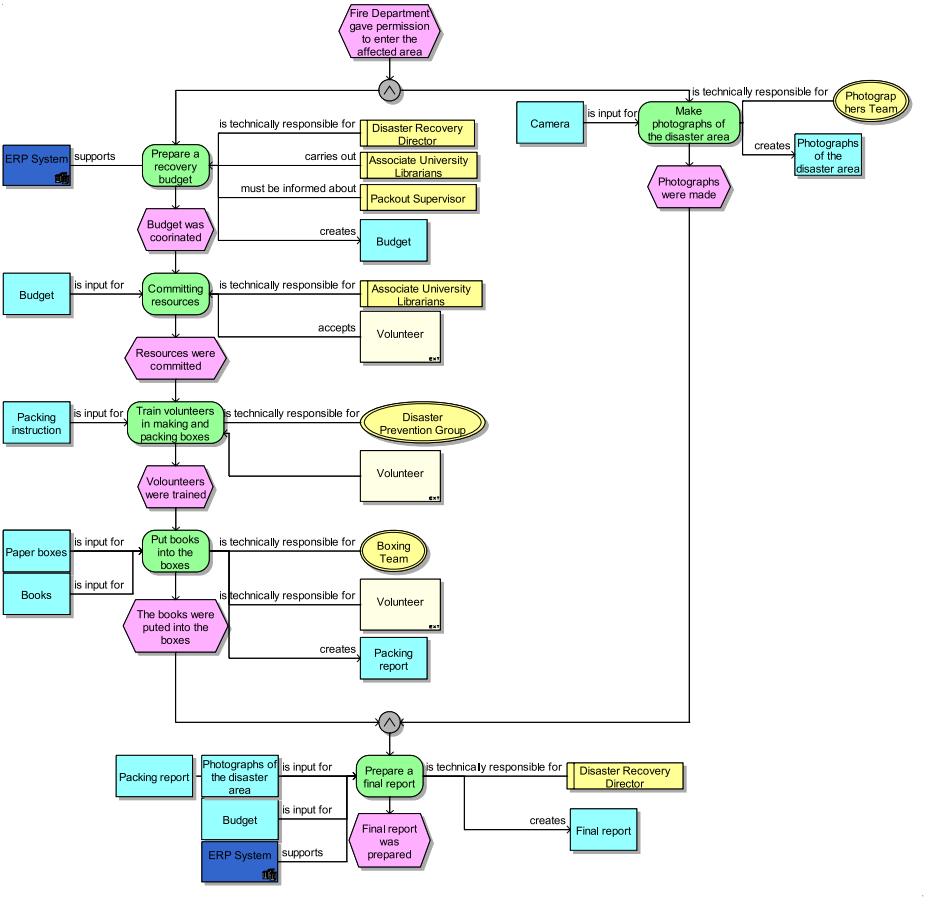

Fig. 6. The Event-Driven Process Chain - The pack out process

4 Analyzing Properties of BC/DR Plans

EPC representation of BC/DR plan makes possible analysis of its timing and dynamic behaviour, completeness and resource utilization properties. This can be achieved by the simulation of EPC models of BC/DR procedures or the analysis of data collected in the ARIS perspectives and their inter-relations. An automated software tools support can be easily developed to support such analyses. At the same time manual analysis techniques like walk-through, manual simulation or desk-checks become more efficient – obviously, it is easier to analyze diagrams than textual documents.

4.1 Simulation

Full formalization of all the ARIS models used to represent BC/DR plans exceeds the scope of this paper. Therefore, the concepts presented below, especially the

definitions of the properties of BC/DR plans are semiformal but the ideas behind them are clear and easy to implement in practice.

In our approach BC/DR plan is modeled with a set of EPC diagrams. The execution of a plan can be simulated with discreet event simulation techniques. Necessary prerequisites are:

- Duration times assigned to the functions – these should typically be worst-case durations of the modeled activities;
- Simulation scenarios defined as:
  - times of occurrence of certain events – typically external ones – this typically defines the sequence of process activations due to the occurrence of external events;
  - indicating which choices to select during the simulation in case of conditional constructs – here various strategies can be applied – random choices, selection of either negative or positive choices, user-defined choice.

The simulation can be carried out with computer support – it is possible to use standard modeling tools or develop some of one's own. The result of a simulation of a set of EPC models has been referred to as *event trace*.

Definition 1. ***Event Trace*** *of a simulation of a set of EPC diagrams is a sequence of 3-tuples (e, t, p), where e stands for unique identifier of an event, t – time of occurrence of event e measured from the start of the simulation, p – process in which event e has occurred.*

4.2 Timing and Dynamic Behaviour

Timing properties of BC/DR plans are obviously of highest interest to the stakeholders as such plans are usually aimed at bringing the length of the disruption period to a minimum. Analyzing event trace of a given simulation, it is possible to calculate the time between any pair of events that happened during the course of the simulation. This makes possible to estimate the whole duration of BC/DR procedures and relates them to the Business Continuity requirements, expressed in terms of Maximum Tolerable Period of Disruption or Recovery Time Objective. A number of simulations can provide worst-case estimates on the duration of BC/DR procedures.

Definition 2. *If the duration of a given EPC process is predictable, than the directed graph made of EPC diagram limited to events, functions, conditions and logical operators is acyclic. (necessary condition)*

The above definition indicates that if the BC/DR plan contains any conditional construct leading to the functions performed earlier some sequences of function executions can be performed more than once and the number of such repetitions cannot be deduced just from the diagram. Such situations indicate potential errors in BC/DR plan or a risky organizational solution.

4.3 Completeness

Definition 3. *The BC/DR plan is* ***complete*** *if:*

1. *Each team has at least one team member,*
2. *Each team/team member is assigned to at least one activity (function),*
3. *Each resource has been assigned to at least one activity (function),*
4. *Each product has been assigned as a result of at least one activity,*
5. *Each function is performed at least once in any EPC model comprising BC/DR plan.*

As the data of all the modeling perspectives is strongly interconnected – analysis of these connections can uncover defined but unused resources, teams or team members taking parts in no activities as well as activities defined but not performed during the course of the plan. This indicates potential error in BC/DR plan. Completeness can easily be verified automatically by analyzing the data gathered in each of the ARIS perspectives and its interconnection with appropriate other perspectives – e.g. to verify that all the functions have been utilized it is necessary to compare the set of functions from function view against all the EPC models of process views.

4.4 Technical and Human Resource Utilization

Event traces can be algorithmically transformed to the function (activities) execution traces (basing on the assignment of teams/roles/persons and resources to functions), which model the occupation of given resources during the simulation of BC/DR plan.

Definition 4. ***Function Execution Trace*** *of a simulation of EPC diagram D is a sequence of 4-tuples (a, s, f, p), where a stands for unique identifier of an activity (function), s, f – respectively: time of the start and the end of the execution of activity a, p identifies the process containing executed function f.*

Event trace makes it possible to establish:

- The total occupation of a given resource r by all the processes comprising BC/DR plan – it is given by the sum of execution times of functions f to which are assigned resources r;
- The utilization of given resource r – it is the occupation of resources r related to the total duration of BC/DR plan execution;
- The action that possibly conflict on given resource r – such a conflict may take place when two actions use the same resource and their execution periods overlap.
- The timing of the potential resource usage conflicts.

All the above analyses can be automated with appropriately developed software tools.

5 Discussion

Preparing the example illustrating the concepts of modeling BC/DR plans in ARIS approach we tried to represent the DR plan for the library of the University of California using ARIS models. This experiment revealed both drawback of traditional textual forms of BC/DR plan as well as the advantages of modeling such plans with ARIS models.

Although the analyzed plan defines all the necessary components of BC/DR plan, i.e. roles, team member, resources, products, activities and their sequencing, it is very difficult to put all these things together. The connections between activities and teams or team members responsible for performing them, activities and necessary resources and products resulting from these activities are very difficult to locate as all this vital information is spread all over the text document – the references between them are unclear and difficult to maintain. This may lead to incompleteness of BC/DR plans. In fact, we have found the following flaws:

- several activities without any responsible role or person assigned,
- a few activities with undefined resources or incomplete resources assigned,
- resources indicated as needed for a given activity but remaining undefined (the need for rooms for book drying has been specified, however, even potential rooms have not been indicated),
- ambiguous and potentially conflicting roles – e.g. photographing was a duty of the Recovery team, however there is also photographer mentioned in the whole plan whose role does seem to be conflicting with the recovery team unless he is a member of this team, which is not quite clear – the diagram presented in figure 1 is a proposition of resolving this ambiguity,
- one of the persons is probably overloaded with the assigned duties.

All the connections between the components of BC/DR plan, which are so difficult to identify in the textual form of BC/DR plan are explicitly and legibly expressed in ARIS models, especially in EPC diagrams. This makes traditional verification techniques like walkthroughs and desk-checks easier to perform and more efficient, while providing the ability of analyzing properties of BC/DR plan as described in Section 4. Of course full assessment of such a plan is only achievable with its full execution, however precise expression and prior analysis should help to avoid exercising a defective BC/DR plan.

The properties and analysis techniques described in Section 4 provide for basic verification and analysis of BC/DR plan properties. They can help to identify serious flaws in BC/DR plans. The properties of resource utilization, resource conflicts, loops in processes require in-depth analysis, usually requiring more detailed information than defined in our approach. Exemplary issues have been listed below:

- Some resources may be used only exclusively by single person or team at a time. This can force other teams to wait until necessary resource has been released by the other person or team. This situation has not been included in our model. To account for that our model has to be enhanced.

- Conflicts on resources may in extreme cases lead to deadlocks – as they do in case of all parallel systems. To detect such situations it is necessary to convert ARIS model to a fully formal model that makes appropriate analysis possible.
- The resources can also be characterised by their capacity e.g. the capacity of a team is number of man-hours that certain team can work during a unit of time. Again this may be subject to further research.

6 Conclusion and Future Research

There are numerous advantages of modeling BC/DR plans as business processes with ARIS models and methodology:

- It increases preciseness of expression and consistency of BC/DR plan;
- It ensures legible and easily understandable way of documenting and communicating BC/DR plan;
- It increases the efficiency of traditional verification techniques like desk-checks and walkthroughs;
- It makes BC/DR maintenance, on-demand adjustment and audit easier;
- Assessment of BC/DR plan can be performed prior to its execution by means of simulation or using analysis techniques and property definitions described in this paper. The analysis encompasses timing and dynamic behaviour, completeness and resource utilization properties;
- Monitoring and supervision of the execution of BC/DR plan is easier and more efficient when it is modeled as business process with appropriate diagrams;
- It ensures considerable money savings as only plans validated and verified on ARIS models could be exercised in reality;
- It might help to standardize BC/DR plans within a distributed organization.
- ARIS models of BC/DR plans are a common language to be used by all the stakeholders. As it's level of formalism is considerably higher than in the case of a textual form it makes the communication between different stakeholders more precise and unambiguous.

The main directions for the further research are:

- Extension of the model presented in this paper to enable in-depth analysis of resource utilization and resource access conflicts,
- Further formalization of ARIS model – precise expression of the models used for BC/DR modeling in algebraic terms,
- Conversion of ARIS models or its formal form to one of the models of dynamic, parallel systems (like Petri Nets, CSP, Lotos),
- Defining further properties of BC/DR plans that can be subject to analysis,
- Extending analysis techniques with the analysis of dynamic properties (e.g. liveness), resource utilization, conflicts on resource usage.

References

1. BSI: Standard BS 25999-1:2006. Business continuity management. Code of practice, http://www.bsi-global.com
2. ISO/IEC: Information technology – Service management – Part 1: Specification (ISO 20000-1), Part 2: Code of practice (ISO 20000-1). ISO/IEC (2005)
3. ITGI: COBIT 4.1: Control Objectives for Information and related Technology. IT Governance Institute (2007)
4. NFPA: NFPA 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs. National Fire Protection Association (2007)
5. Swanson, M., et al.: Contingency Planning Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, pp. 800–834. NIST Special Publication (June 2002)
6. Snedaker, S.: Business Continuity and Disaster Recovery for IT Professionals. Elsevier, Amsterdam (2007)
7. Barbara, M., et al.: Effective Strategies to Ensure Business Continuity/Disaster Recovery. Dr. Mueller.Verlag
8. Thejendra, B.: Disaster Recovery and Business Continuity. IT Governance Ltd (2007)
9. Nelson, K.: Examining Factors Associated with IT Disaster Preparedness. In: Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS 2006), p. 205b. IEEE, Los Alamitos (2006)
10. Zambon, E., et al.: A Model Supporting Business Continuity Auditing & Planning in Information Systems. In: Second International Conference on Internet Monitoring and Protection (ICIMP 2007), pp. 33–33. IEEE, Los Alamitos (2007)
11. Kepenach, R.: Business Continuity Plan Design. 8 Steps for Getting Started Designing a Plan. In: Second International Conference on Internet Monitoring and Protection (ICIMP 2007), p. 27. IEEE, Los Alamitos (2007)
12. Cloth, L., Haverkort, B.R.: Model Checking for Survivability! In: Proceedings of the Second International Conference on the Quantitative Evaluation of Systems (QEST 2005), pp. 145–154. IEEE, Los Alamitos (2005)
13. Hayes, P., Hammons, A.: Picking up the Pieces: Utilizing Disaster Recovery Project Management to Improve Readiness and Response. In: IEEE Industry Applications Magazine, November/December 2002, pp. 27–36. IEEE, Los Alamitos (2002)
14. Scheer, A.W.: ARIS – Business Process Frameworks. Springer, Heidelberg (1999)
15. Scheer, A.W., et al.: Business Process Automation. Springer, Heidelberg (2004)
16. Weske, M.: Business Process Management: Concepts, Languages, Architectures. Springer, Berlin (2007)
17. University of California: Disaster Prevention, Preparedness and Recovery Plan, http://palimpsest.stanford.edu/bytopic/disasters/plans/ucdaviis_disasterplan2004.pdf