MODELING INFORMATION SYSTEM AVAILABILITY BY USING BAYESIAN BELIEF NETWORK APPROACH

Semir Ibrahimović[1, 2, *] and Nijaz Bajgorić[2]

[1]BBI Bank Sarajevo
 City of Sarajevo, Bosnia and Herzegovina

[2]School of Economics and Business Sarajevo
 City of Sarajevo, Bosnia and Herzegovina

ABSTRACT

Modern information systems are expected to be always-on by providing services to end-users, regardless of time and location. This is particularly important for organizations and industries where information systems support real-time operations and mission-critical applications that need to be available on $24 \times 7 \times 365$ basis. Examples of such entities include process industries, telecommunications, healthcare, energy, banking, electronic commerce and a variety of cloud services. This article presents a modified Bayesian Belief Network model for predicting information system availability, introduced initially by Franke, U. and Johnson, P. (in article "Availability of enterprise IT systems – an expert-based Bayesian model". Software Quality Journal 20(2), 369-394, 2012) based on a thorough review of several dimensions of the information system availability, we proposed a modified set of determinants. The model is parameterized by using probability elicitation process with the participation of experts from the financial sector of Bosnia and Herzegovina. The model validation was performed using Monte-Carlo simulation.

KEY WORDS

CLASSIFICATION

Corresponding author, η: semir.ibrahimovic@efsa.unsa.ba +387 61100254;
 BBI Bank Sarajevo and School of Economics and Business Sarajevo, Mišćina 9
 71000 City of Sarajevo, Bosnia and Herzegovina

INTRODUCTION

In today's world, most of the business activities are associated with the use of information technology (IT). Information technologies enable and facilitate business, while, at the same time, a success of an organization is becoming increasingly dependent on the proper use of information technologies and managing risks associated with this dependency. The availability of information system (IS) is an essential requirement that business presents to IT departments. Forrester pointed out that across all industries, there is less and less tolerance for any kind of downtime [1]. According to Aberdeen Report, the average cost of an hour of downtime for large companies is 686 250 US$, 215 638 US$ for medium companies and 8 581 US$ for small companies [2]. Gartner noted that 5 600 US$ per minute is an average cost of downtime [3]. Butler reported that a 49 minutes failure of Amazon's services on 31st January 2013, resulted close to 5 million US$ in missed revenue [4].

According to ITIL, availability is the characteristic of the IS to perform its agreed action at the request of an authorized user [5]. Availability in the broader sense implies that the information system is ready to serve end users, even in the event of unforeseen and catastrophic events. At the same time, IS has to be protected from various security threats.

In this study, an information system is defined in a broader sense, as a combination of interrelated components that, through their interactions, deliver the desired output. That means, information system, besides hardware and software, includes people, processes, culture and environment, which are all crucial for understanding, explaining and modeling availability and risk [6]. From the availability perspective, in this study, the system was regarded as a set of services that are available to end users. The total availability of the IS is the result of summarizing the availability of individual services that are components of the system. It is assumed that each service has an agreed-upon operation time (if service is to be continuously available 24×7 or only 8×5). The percentage of users affected by the outage of individual systems is also considered.

This article contains a thorough review of the literature in the IS availability field, addressing the problem from various perspectives. The primary goal of this research is to determine a set of factors that have the greatest influence on IS availability in BiH financial institutions. The second aim of the research is to compare the results of model parameterization with the results of Franke and Johnson [7]. As IS availability depends on local factors, especially of telecommunication and power network, climate and seismic factors, this study aims to determine whether the factors that affect the availability of IS in Bosnia and Herzegovina are the same as for the US and Western Europe and whether they have equal 'weights'.

AVAILABILITY OF INFORMATION SYSTEMS

IEEE defined the IS availability as "The degree to which a system or component is operational and accessible when required for use. Often expressed as a probability." [8]. Rauscher defines availability as a measure of the readiness of the system to be used for the purpose for which it was designed, when needed [9]. ISO 27 000 series of standards tied availability to the concept of organizational assets. The asset is available if it is accessible and ready for use at the request of an authorized person. In the context of this standard, the assets include information system components, facilities, networks and computers [10]. Singh gave a more quantitative definition: "Ps-system availability of the observed system S, is the probability that a system is operational and ready to provide services. As the Ps number should be close to 100 % as possible. The usual way to represent the IS availability is

counting nines. So 99,999 % availability is called five nines." [11]. Availability is also defined as a combination of three concepts: reliability, accessibility and timeliness [12].

Most commonly, IS availability is referred to be part of the of the CIA (confidentiality, integrity, availability) information security triangle [13-20]. Also, in literature one can find term 'resilience' of an IS, where this term implies that the system "must remain available and maintain an acceptable level of performance when faced with various types of errors affecting the normal operation" [21] which is very close to the original definition of availability. Bajgorić used this term as a synonym for business continuity [22]. Gaddum discussed the resilience as IT, organizational and business issue, and introduced a model with six layers of resistance: strategy, organization, processes, data and applications, technologies and facilities [23]. Schiesser observed availability as optimization process of the productions systems readiness for accurately measuring, analyzing and reducing the system downtime [24].

Availability is expressed (measured) as the ratio of the time in which the system was available in relation to the total time. The basic formula for the IS availability calculation is

$$\text{Availability} = \frac{\text{System uptime}}{\text{System uptime} + \text{System downtime}} \qquad (1)$$

For a complex system, we can get uptime time as the sum of uptime times for all subsystems. For example, if we have a system that provides the following services with the agreed times of availability: core banking $24 \cdot 7$, SWIFT $8 \cdot 5$, e-banking $24 \cdot 7$, m-banking $24 \cdot 7$, then a contractual system uptime annually $52 \cdot (24 \cdot 7 + 8 \cdot 5 + 24 \cdot 7 + 24 \cdot 7) = 28\,288$ hours. System downtime is collected for each service so that it takes into account the percentage of affected users. For example, the unavailability of a core banking service, affecting 5 % of users, for 20 minutes is equivalent to 1 minute of total unavailability of the core system.

Martin identified six major determinants of IS availability: physical security, audit and evaluation of the system efficiency, security policy, system monitoring and control of operations, business continuity management and backup management [25]. Franke and Johnson in their model [7] used 16 determinants that affect the availability of the system based on the 'Index of availability', introduced by Marcus et al. [26]. Bajgoric identified eight kinds of threats to the IT infrastructure that affect business continuity [22]. Rauscher et al. proposed a model for the reliability of communications infrastructure and identified the following components that affect reliability: the human factor, policies, hardware, software, network, load, environment, and power. In 2001, EMC conducted an extensive study on 250 European companies from different industries and various sizes, to identify causes of system disruptions. The study found that main reasons for disruption are: failures in hardware, interruptions in electric power supply, software errors, downtime of reserve power supply, data errors, errors of external service network), operating system, physical environment and disasters, 40 % were application errors, and 40 % were due to human mistakes [28].

There are different recommendations to raise the IS availability: Liu et al. [29], Raderius et al. [30], Franke and Johnson [31] suggested improvement of IS architecture, Martin recommended improving security policies [13], Gay suggested virtualization [32], Calzolari recommended clustering and virtualization [33] and Bajgoric et al. the application of standards in the IS governance [34]. Chen et al. suggested a strategy of diversification as a possible solution for reducing the IS unavailability, caused by attacks on network resources [19]. Bell proposed the use of the best practices in designing a data center to improve the IS availability [35]. In a study conducted in 2009, IBM recommended the following technologies and processes, to achieve high availability of the system: application management, availability management, capacity management, change management,

measurement management, network management, performance management, service management level and service recovery management [36].

INFORMATION SYSTEMS AVAILABILITY MODELING

Raderius et al. [30] cited block diagrams reliability and Monte-Carlo simulations as the most frequently used reliability modeling tool. They identified an inability to express uncertainty and high model dependency of the modeled system architecture as major problems of these methods. Malek et al. classified availability modeling methodologies into analytical, quantitative and qualitative [37]. Quantitative models are based on measurements and most often used to model availability of hardware components of IS. Research based on qualitative models are conducted less formally, and as primary modeling tools utilize questionnaires and interviews. As a result, they assign availability class to the IS. Trivadi et al. [38] distinguish qualitative and quantitative availability models. They defined qualitative models as models based on verbal descriptions and checklists and quantitative models as stochastic models based on hardware and software structure of the IS. Unlike most IS availability models, which represent availability as binary variable (system available or not available), Tokuno et al. [39] modeled availability of software-intensive systems in a way that recognize declines in the system performance as a condition that affects the availability. As a modeling tool, they used the Markov process. Goyal et al. also used Markov chains as IS availability modeling tool and made a high-level model of failure and recovery of IS components [40]. Immonen et al. defined the framework for the comparison of methods for reliability and availability modeling from the software architecture perspective [41]. Milanovic quoted the following analytical methods for availability modeling: Reliability Block Diagrams, Fault Trees, Reliability Graphs and Complex Configurations, Markov Models, Stochastic Petri Nets, Stochastic Activity Networks and Markov Reward Models, whereas, for qualitative models, he noted CMMI, ITIL, ISO/IEC 15 504-SPICE, CobiT, MOF, MITO, ISO/IEC 27 002 and ISO 12 207/IEEE 12 207 [42]. A method for availability analysis based on Fault Tree Analysis is presented by Narman et al [43]. Torabi, Soufi, and Sahebjamnia proposed a framework for conducting the business impact analysis by using MADM techniques [44].

METHODOLOGY

BAYESIAN NETWORKS

In this research, we used Bayesian Belief Networks (BBN) as a tool for analyzing the factors influencing the IS availability. Neil et al. wrote about the application of BBN to the modeling the operational risk of IT in financial institutions [45]. As the main advantages of BBN they noted enabling a combination of statistical and qualitative data and mapping the causal structure of the process, thus making it easier to understand and communicate with business users. Using BBN one can:

a) combine proactive indicators of losses with a reactive results of measurements,
b) take into account experts judgments,
c) work with incomplete data and still get a reasonable prediction,
d) implement a robust scenario analysis,
e) test the robustness of the results,
f) have a tool for visual reasoning and help in documenting,
g) carry out a comparative analysis of alternative scenarios and robustness testing,
h) assess changes in design of the IT infrastructure.

BBN are graphic models that combine graph theory and probability theory. Each BBN has two elements: a direct acyclic graphs (DAG), which represent the structure, and a set of conditional probability tables (CPT). The nodes in the structure correspond to the observed variables, and the edges are formally interpreted as 'probabilistic independence'. CPT quantifies the relationship between the variable and its 'parent' in the graph [46]. Bayes' theorem is used for inference propagation so that the probability distribution can be quantified for each node if given the likelihood of an initial node and CPT for all nodes. For two events Bayes' theorem states:

$$P(A \mid B) = P(B|A) \, P(A) / \, P(B) \qquad (2)$$

An interpretation of formula (2) is as follows: it is possible to calculate the conditional probability of event A, given the event B, using the conditional probability of event B, for a given event A and the probability of event B and the probability of event A. Although Bayesian networks significantly reduce the number of parameters, which needs to be determined by specifying the joint probability distribution, the number of parameters in the model remains one of the major bottlenecks of this framework. One way to reduce this number is to assume a functional relationship that defines the interaction between all the parents of a node. The most widely accepted and applied solutions for this problem is the Noisy-OR model [47]. Noisy-OR model gives a causal interpretation to the interaction between the parent node and child node. It assumes that all causes (parents) are independent of each other regarding their ability to influence the variable effect (the child). Given these assumptions Noisy-OR model provides a logarithmic reduction in the number of parameters required for the construction of the CPT, which effectively makes the building of large models for real life problems feasible. Noisy-OR model assumes the presence of any of the causes Xi is sufficient to obtain the presence of Y as the effect. The second assumption of Noisy-OR model is the ability of cause Xi to produce an effect is independent of the presence of other causes. However, the presence of the cause Xi in Noisy-OR model does not guarantee that effect Y will happen. In practical models, a situation where the absence of all modeled causes ensures the lack of impact almost never happens. To solve that weakness of Noisy-OR model, Henrion introduced the concept of a leakage or background probabilities that allows modeling the impact of a combination of factors that are not included in the model [48].

BBN have been widely applied in OpRisk, INFOSEC and availability modeling. Raderius et al. presented a case study where the availability of the information system was estimated using the 'extended influence diagrams' combined with an architectural metamodel [30]. Hinz et al. presented BBN model for assessing the risk of IT infrastructure. The parameters of this model were obtained using interviews with experts [49]. Weber et al. used the influence diagrams for the economic analysis of the IS availability [50]. Neil et al. presented the methodology for developing BBN model representing the operational risk of IT infrastructure in the financial institutions [45]. Wei et al. developed an integrated process, based on BBN, for efficient IT services management [51]. Sommestad et al. made a model based on the extended influence diagram, which enables the analysis of the cyber security of different architectural solutions [52]. Cemerlic et al. proposed a system for intrusion detection system (IDS) based on BBN [53]. Simonsson et al. proposed a model for measuring IT governance efficiency based on BBN [54]. Lande et al. modeled the critical information systems, using BBN [55]. Zhang et al. presented an innovative model to improve the availability of the system based on the BBN in which the data for the CPT were obtained from the system logs [56]. Bonafede did a review of statistical methods that can be used to model business continuity and gave an example of BBN use for that purpose [57]. Different models, based on BBN, were made in the area of software reliability [58-60], and management of software development projects [61-63].

Franke and Johnson presented the model for decision support in the area of IS availability based on Leaky Noisy-OR BBN [7]. The model parameters were obtained based on the probability elicitation of 50 experts in the IS availability field. That model, with modifications based on the theoretical part of the study, has been applied in this research. Also, we propose a model that consists of thirteen variables representing thirteen domains affecting information systems availability. Those variables are: the physical environment, availability requirements management, operations management, change management, backup management, storage redundancy, avoiding errors in internal applications, avoiding errors in external services, network management, equipment and location of the DR data centre, resistant client/server systems, monitoring of relevant components, human resources management. If the best practices are implemented in one more of those domains, IS unavailability would be reduced.

The probability elicitation used for determining the model parameters was done by interviewing 23 experts dealing with IT systems availability in the financial sector in BiH. The research focused on information systems in the banking industry which, due to the presence of international and local regulations and regular audit reviews, have the necessary maturity level of IS governance to be suitable for modeling. During the elicitation, most experts agreed that the selection of variables in the model is adequate and that the model is comprehensive. Elicitation was conducted through structured interviews. In the first part of meetings, experts were trained and calibrated, while in the second part experts filled in the questionnaire. The questionnaire consisted of three sets of questions. Experts were first asked to estimate the impact of individual variables on system availability. In the second question, experts gave their assessment of the situation in the areas described by the variables in the financial sector in BiH. To answer the third question, they estimated the necessary investments to bring the field represented by the variable to the level of best practices.

As the system consists of several services provided to internal and external customers, overall system availability is defined as the average availability of each service weighted by a factor of importance of a service (for example different weight is given for a payment card authorization service and a service that calculates fixed assets depreciation). We used the equation bellow for the availability calculation.

$$A_i = \frac{\sum_i A_i k_i}{\sum_i k_i} \tag{3}$$

In formula (3) A represents overall system availability, A_i represents an availability of service s_i, and k_i represents a coefficient significance of service s_i.

When calculating the availability of a particular service one should take into account the service operating time, defined in the service level agreement, as well as the number of clients affected by the service interruption. The availability of a particular service is calculated according to the following formula:

$$A_i = \frac{t_i}{t_i + ut_i \dfrac{un_i}{n_i}} \tag{4}$$

In formula (4) t_i is the total time that service s_i was available under service level agreement, ut_i is the total time for which the system was unavailable, n_i is the total number of the service users, un_i is the number of service users where experienced service interruption during time ut_i.

According to the Leaky Noisy-OR model presented in Figure 1, the following formula applies to calculate the probability of IS availability.

$$P(A) = (1 - p_0)\prod_{i \in [1,n]}(1 - p_i) = (1 - p_0)\prod_{i \in [1,n]}(1 - k V_i(1 - B_i)) \qquad (5)$$

In this formula n represents the number of variables in the model, V_i represents percentage of the improving system's availability if the best practices are applied, B_i represents a state of implementation of the best practices in different system's components, k represents transformation coefficient, p_0 represents a leak representing probability that the system is unavailable in the case that for all domains included in the model, best practices are applied.
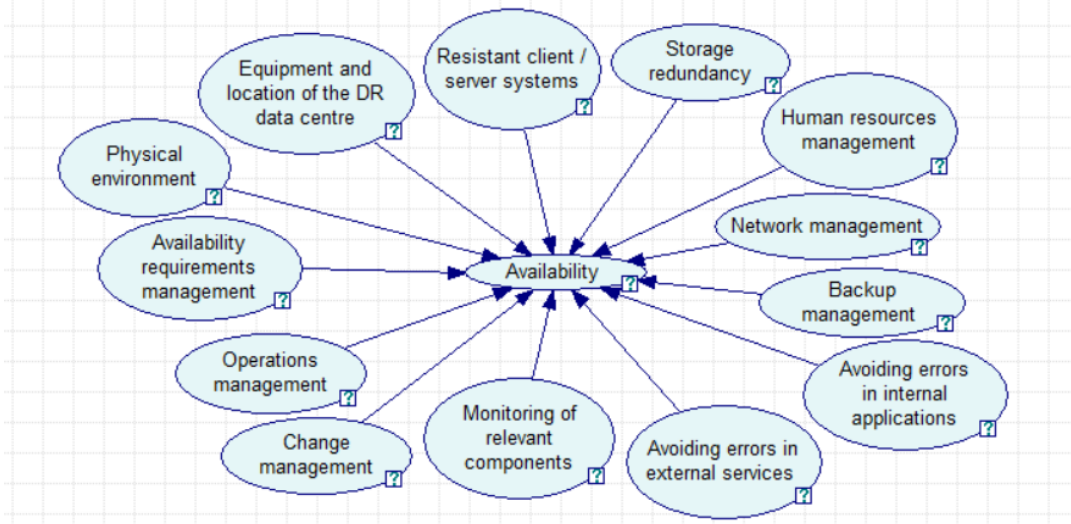

Figure 1. Leaky Noisy-OR BBN model.

RESULTS AND DISCUSSIONS

The research has shown that the 'availability requirements management' has the greatest impact on the availability (23,20 %), followed by 'operations management' (20,54 %) and the 'equipment and location of the DR data center' (19,52 %). The reduction of IS unavailability is the least impacted by 'the physical environment' (10,53 %), followed by 'backup management' (11,05 %) and 'resistant client / server systems' (11,81 %). The research results showed that the state of implementation of the best practices in the areas described by variables ranges from 4,60 to 6,85 on a scale from 1 to 10 depending on the area. The worst situation is in the fields of 'monitoring of relevant components' (4,6) and 'availability requirements management' (4,94). The best state in the IS of financial institutions in BiH is in the basic infrastructure areas: 'backup management' (6,85), 'network management' (6,54), 'resistant client/server systems' (6,39) and 'the physical environment' (6,05). According to the results of this research, the perception of experts is that the state of the essential IS infrastructure elements, including the server room, server and network infrastructure, data redundancy, backup management is much better than the process part, which includes change management, operations management, monitoring and requirements management. Assessment of the current maturity level of backup management may explain why the experts estimated that implementing the best practices in that area would have a small impact on reducing unavailability, as the situation in that field has been assessed as the best compared to all other areas that were part of the model. A similar explanation applies to the physical environment and server infrastructure. The above was the main reason to include assessed states of implementing best practices in the field as the prior probability for each parent node in BBN-based 'Leaky Noisy-OR' model. The conditional probability table for the node that represents availability is filled based on a linear transformation of the elicited impact values. The model is set up assuming the initial system

availability of 99 % and a leak of 0,01 %, which represents the unavailability of the system. Both of these parameters can be subsequently changed.

As part of the research, we compared the results with the study made by Franke and Johnson [7]. To be able to compare the results, it was necessary to transform the research results, since the different methods of calculating variables impact on the IS availability were used. Research findings and comparison are shown in Table 1. The first column represents the effects of each variable on the IS availability, where resulting percent is calculated as a mean of experts' opinions. The second column represents experts' opinions about the maturity level in the financial sector in BiH using scale 1-10. Third columns represent the research results, where as the resulting impact was calculated as the mode of experts' opinions modified with adjacent intervals. The fourth column represents Franke's results. Fourth, fifth and sixth columns represent ranking of data presented in first, third and fourth columns respectively.

Table 1. Elicitation results compared with Franke and Johnson [7].

Variable	Percent median	Maturity level	Percent as mode	Percent Franke	PS	PP	PF
Operations management	20,54	4,94	8,85	23,00	2,00	4,00	4,00
Network management	19,53	5,24	6,99	12,95	3,00	7,00	6,00
Equipment and location of the DR data center	19,52	6,54	2,31	3,35	4,00	13,00	12,00
Avoiding errors in internal applications	17,58	5,28	6,44	16,86	5,00	10,00	5,00
Avoiding errors in external services	17,52	5,93	7,81	8,66	6,00	5,00	7,00
Change management	17,15	5,88	25,65	28,08	8,00	2,00	1,00
Human resources management	15,45	5,76	6,92	-	9,00	8,00	-
Backup management	11,05	5,56	7,65	5,27	12,00	6,00	10,00
Availability requirements management	23,20	5,44	29,64	25,25	1,00	1,00	3,00
Storage redundancy	17,20	4,60	5,00	5,34	7,00	11,00	9,00
Resistant client/server systems	11,81	6,39	3,94	3,65	11,00	12,00	11,00
Physical environment	10,54	6,85	10,00	8,22	13,00	3,00	8,00
Monitoring	12,33	6,05	6,71	26,14	10,00	9,00	2,00

Comparing data from with data from Franke and Johnson research we can notice that according to that research, there are more IS availability determinants with an impact greater than 20 %. In our study, only two variables have an impact greater than 20 % while the other variables impact IS availability with the 10 % and less. Among the four most significant areas,

both studies identified the same three areas: 'availability requirements management', 'change management' and 'operations management'. Also, both studies have shown that least influential are variables 'resistant client/server systems' and 'DR equipment and location'. The biggest differences are in the areas of 'monitoring of relevant components' and 'avoiding errors in internal applications'. In research by Franke et al., they have a greater impact (2nd and 5th position) compared with our research (9th and 10th). Contrary, 'physical environment' has a significant impact according to our results (3th place) in comparison with Franke et al. research (8th place). When interpreting these outcomes, one should consider that we gathered data from the BiH banking sector while Franke et al. research did not have industry boundaries.

One of the disadvantages of the proposed model is a deterministic determination of parameters. In other words, each parameter in the network is set using the weighted mean values, obtained in the elicitation process, and not reflecting the diversity of experts' opinion. For this reason, the same mathematical model was implemented using Microsoft Excel and Oracle Crystal Ball software. The base values of the input variables were set using values from CPT tables of the BBN model. However, each input variable was represented not only by the mean value but by also using the entire distribution obtained in the elicitation process. Figure 2 shows the distribution of impact of 'availability requirements management' variable on IS availability as an illustration how the distribution for each variable was modeled.
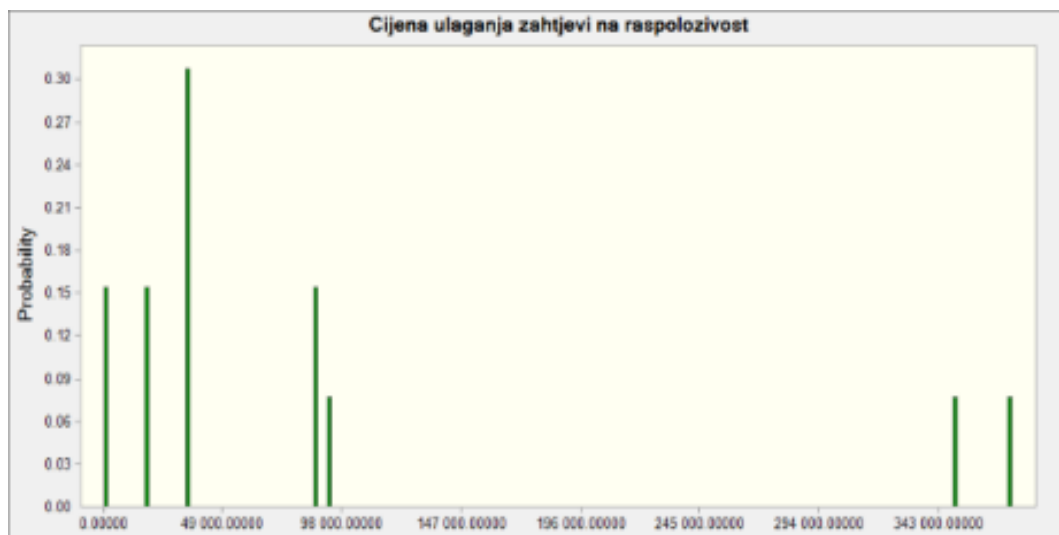

Figure 2. Input distribution.

In this way, we got the stochastic equivalent of the BBN model. We used this model to run Monte-Carlo simulations. The first simulation was run without optimization, just applying the distributions obtained by elicitation. Each simulation had a total of 10 000 trials. Resulting availability probability distribution and certainty intervals are shown in Figure 3 and Figure 4.

Diagrams in Figure 3 and Figure 4 show the stochastic nature of availability prediction. If there are 13 variables, which can affect the availability and which are not at the best practices level, it is not possible to precisely determine the time and the effect that this weakness may cause. Thus it is not possible accurately to predict the IS availability percent, rather it is possible to predict that availability will be inside the predicted range with particular certainty level. According to the results of the simulation, we got IS availability range from 98,33 % to 99,76 % with 90 % confidence for the case in which best practice are not applied. Mean and median values were 98,93 % and 98,97 % respectively, which was close to the initial assumption of 99 %.

CONCLUSION

The study presented an extensive literature review in the areas of availability and applications of BBN-based methods to decision-making in the fields of operational risk and IS. Based on the theoretical part of the research we the adapted model that was constructed by Franke et al. in two aspects. We changed input variables of the model, and incorporated information on the previous states of the variables, which improved the predictability of the model. Also, we
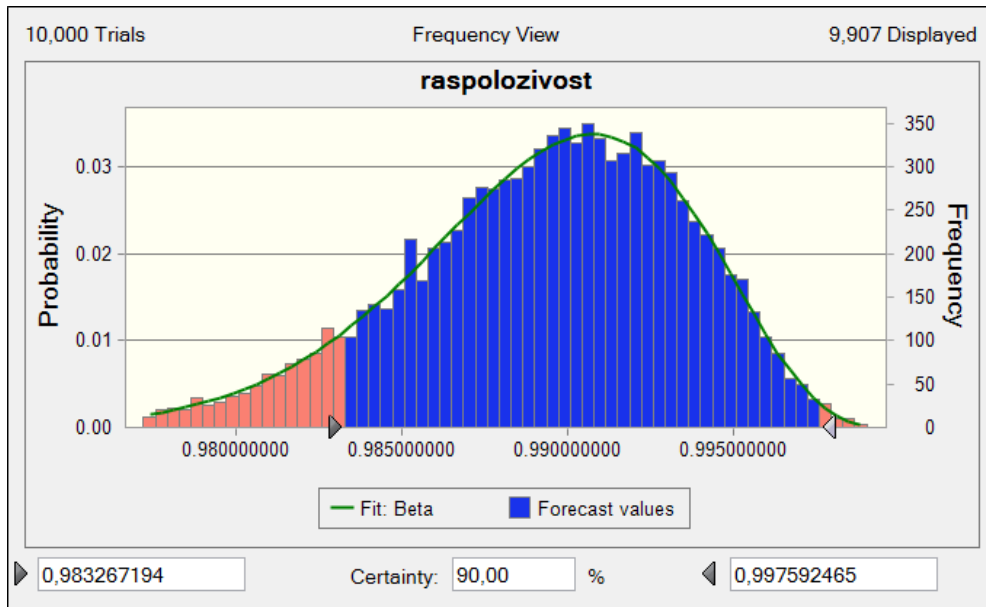

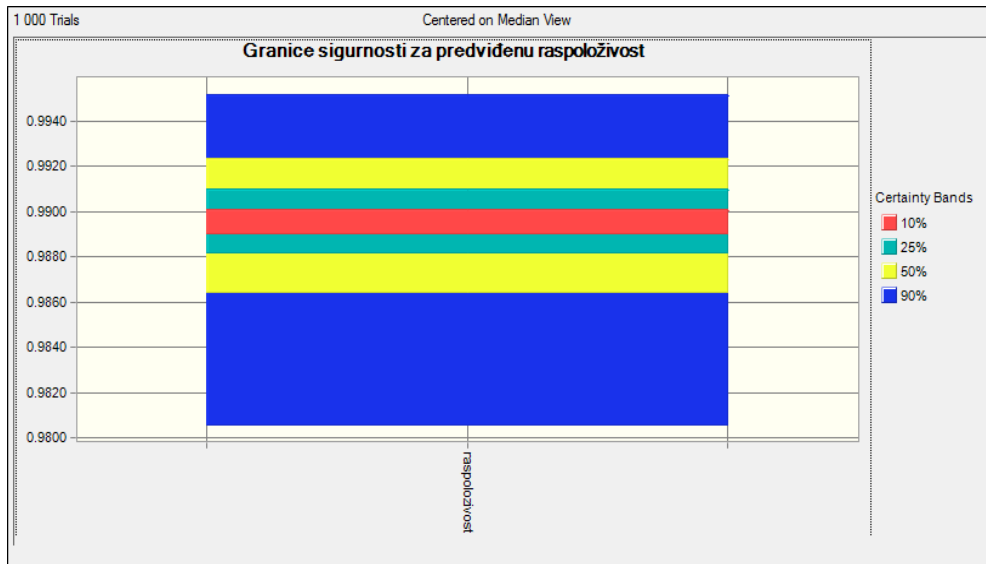**Figure 3.** Availability distribution.

Figure 4. Availability certainty intervals.

conducted an extensive field research, providing the probability elicitation on the entire population of InfoSec, IS audit and IS management experts from the BiH banking sector. This research resulted in a picture of the state of implementation of best practices in the fields that affect the IS availability in BiH banking sector. We performed a comparative analysis of the research results, with results that are Franke and Johnson get in a study conducted in Western Europe. From a practical point of view, this work identified, taking into account local and regional specificities, which are the most influential factor for the IS availability of BiH banks.

LIMITATIONS AND DIRECTIONS FOR FURTHER RESEARCH

The fundamental assumption built into this model is the independence of the variables that enabled application of Leaky Noisy-OR approach. Another limitation is the binary representation of variables. Investment in a domain does not always results in bringing the domain to the level of best practice, but can improve the situation in the field, thus reducing the impact to the IS unavailability. Further study could lead to a model that would overcome this limitation by using continuous variables instead of using binary and Noisy-MAX node instead of Noisy-OR.

The empirical research was done on IS of banks in Bosnia and Herzegovina as the most mature in the field of availability management. In a situation where other industries are becoming increasingly dependent on IT and increase standards of IS governance, it would be interesting to conduct a similar survey of the general population, not limited to one industry. This would verify the applicability of the model to other industries and enable comparative cross-industry analysis.

Also, more empirical research based on real data of the IS unavailability incidents and their causes of would lead to empirical validation of the model.

REFERENCES

[1] Forrester Report.: *How Organizations Are Improving Business Resiliency With Continuous IT Availability.*
http://www.emc.com/collateral/analyst-report/forrester-improve-bus-resiliency-continuous-it-avail-ar.pdf, accessed 11th November, 2013,

[2] Aberdeen Report: *Preventing Virtual Application Downtime.*
http://www.aberdeen.com, accessed 21st November, 2014,

[3] Lerner, A.: *The Costs of Downtime.*
http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime, accessed 1st July, 2014,

[4] Butler, B.: *Amazon.com suffers outage: Nearly $5M down the drain?*
http://www.networkworld.com/article/2163191/cloud-computing/update--amazon-com-suffers-outage--nearly--5m-down-the-drain-.html, accessed 12th December, 2014,

[5] Taylor, S.: *The Official Introduction to the ITIL Service Lifecycle.*
The Stationary Office, TSO, London, 2007,

[6] Fenton, N.: *Risk Assessment and Decision Analysis with Bayesian Networks.*
CRC Press, Bosa Roca, 2012,

[7] Franke, U. and Johnson, P.: *Availability of enterprise IT systems – an expert-based Bayesian model.*
Software Quality Journal **20**(2), 369-394, 2012,
http://dx.doi.org/10.1007/s11219-011-9141-z,

[8] IEEE: *IEEE Standard Glossary of Software Engineering Terminology.*
IEEE Standards Office, New York, 1990,

[9] Raucsher, K.F.: *Availability and robustness of electronic communications infrastructures.*
European Commission, Brussels-Luxemburg, 2007,

[10] ISO/IEC: *ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements.*
ISO/IEC, Geneva, 2005,

[11] Singh, J.: *Modeling application availability.*
Spring Simulation Multiconference, Society for Computer Simulation International, San Diego, 2009,

[12] Somasundaram, G. and Shivastava, A.: *Information Storage and Management.*
John Wiley & Sons, Indianapolis, 2012,

[13] Martin, A.P. and Khazanci, D.: *Information Availability and Security Policy.*
12th Americas Conference On Information Systems. Association for Information Systems, 2007,

[14] Bodin, L.D.; Gordon, L.A. and Loeb, M.P.: *Evaluting Information Security Investments Using the Analytic Hierarchy Process*.
Communications of the ACM **48**(2), 79-83, 2005,
http://dx.doi.org/10.1145/1042091.1042094,

[15] Bodin, L.D.; Gordon, L.A. and Loeb, M.P.: *Information security and risk management.*
Communications of the ACM **51**(4), 64-68, 2007,
http://dx.doi.org/10.1145/1330311.1330325,

[16] Ioannidis, C. and Pym, D.: *Investments and trade-offs in the economics of information security*.
In: *Financial Cryptography and Data Security*. Vol. 5628, Springer, Berlin and Heidelberg, pp.148-166, 2009,

[17] Faisst, U. and Prokein, O.: *Management of Security Risks - A Controlling Model for Banking Companies*.
In: Seese, D.; Weinhardt, C. and Schlottmann, F., eds.: Handbook on Information Technology in Finance. Vol. 4801, Springer, Berlin and Heidelberg, 2008,

[18] Kouns, J. and Minoli, D.: *Information technology risk management in enterprise environments*.
John Wiley & Sons, Inc., Hoboken, 2009,

[19] Chen, P.; Kataria, G. and Krishnan, R.: *Correlated failures, diversification, and information security risk management.*
MIS Quarterly **35**(2), 397-422, 2011,

[20] Hole, K.: *Toward risk assessment of large-impact and rare events.*
IEEE Security & Privacy **8**(3), 21-27, 2010,
http://dx.doi.org/10.1109/MSP.2010.55,

[21] Liu, D.; Deters, R. and Zhang, W.J.: *Architectural design for resilience.*
Enterprise Information Systems **4**(2), 137-152, 2010,
http://dx.doi.org/10.1080/17517570903067751,

[22] Bajgoric, N.*: Continuous Computing Technologies for Enhancing Business Continuity*.
IGI Global, Hershey, London, 2008,

[23] Gaddum, R.: *Business resilience – the next step forward for business continuity*.
http://www.continuitycentral.com/feature083.html, accessed 27th April, 2014,

[24] Schiesser, R.: *IT systems management.*
Pearson Education, Inc., 2010,

[25] Martin, A.P.: *Key determinats of information availability: A multipe case study.*
University of Nebraska, 2003,

[26] Marcus, E. and Stern, H.: *Blueprints for high availability.*
Wiley Publishing Inc., Indiniapolis, 2003,

[27] Raucsher, K.F.; Krock, R.E. and Runyon, J.P.: *Eight ingredients of communications infrastructure: A systematic and comprehensive framework for enhancing network reliability and security*.
Bell Labs Technical Journal **11**(3), 73-81, 2006,
http://dx.doi.org/10.1002/bltj.20179,

[28] Scott, D.: *Making Smart Investments to Reduce Unplanned Downtime*.
GartnerGroup, 1999,

[29] Liu, D.; Deters, R. and Zhang, W.J.: *Architectural design for resilience.*
Enterprise Information Systems **4**(2), 137-152, 2010,

[30] Raderius, J.; Narman, P. and Ekstedt, M.: *Assessing System Availability Using an Enterprise Architecture Analysis Approach.*
ICSOC International Workshops, Sydney, 1st December, 2008,

[31] Franke, U.; Flores, W.R. and Johnson, P.: *Enterprise architecture dependency analysis using fault trees and Bayesian networks*.
Spring Simulation Multiconference, San Diego, 2009,

[32] Gay, S.: *An examination of virtualization's role in contingency planning.*
Information Security Curriculum Development Conference, Kennesaw, 2007,

[33] Calzolari, F.: *High availability using virtualization.*
Universita di Pisa, Pisa, 2006,

[34] Bajgoric, N.; Spremic, M. and Turulja, L.: *Implementation of the IT governance standards through business continuity management: Cases from Croatia and Bosnia and Herzegovina.*
33rd International Conference on Information Technology Interfaces, Proceedings, pp.43-50, 2011,

[35] Bell, M.A.: *Use Best Practices to Design Data Center Facilities.*
Gartner, 2005,

[36] IBMGlobalServices: *Improving Systems Availability.*
IBMGlobalServices, Atlanta, 1999,

[37] Malek, M.; Milic, B. and Milanovic, N.: *Analytical Availability Assessment of IT Services.*
5th International Service Availability Symposium, ISAS 2008 Tokyo, Japan, May 19-21, 2008, Proceedings of 5th International ServiceAvailability Symposium, Springer, Berlin- Heildelberg, 2008,

[38] Trivedi, K. et al.: *Achieving and Assuring High Availability.*
5th International Service Availability Symposium, ISAS 2008 Tokyo, Japan, May 19-21, 2008, Proceedings of 5th International ServiceAvailability Symposium, Springer, Berlin- Heildelberg, 2008,

[39] Tokuno, K. and Yamada, S.: *Markovian software availability measurement based on the number of restoration actions.*
IEICE Transactions on Fundamentals **E83-A**(5), 835-841, 2000,

[40] Goyal, A. and Lavenberg, S.S.: *Modeling and analysis of computer system availability.*
IBM Journal of Research and Development **31**(6), 651-664, 1987,
http://dx.doi.org/10.1147/rd.316.0651,

[41] Immonen, A. and Niemelä, E.: *Survey of reliability and availability prediction methods from the viewpoint of software architecture.*
Software & Systems Modeling **7**(1), 49-65, 2007,
http://dx.doi.org/10.1007/s10270-006-0040-x,

[42] Milanovic, N.: *Models, Methods and Tools for Availability Assessment of IT-Services and Business Processes.*
Technische Universitat Berlin, Berlin, 2010,

[43] Narman, P.; Franke, U.; Konig, J.; Buschle, M.and Ekstedt, M.: *Enterprise architecture availability analysis using fault trees and stakeholder interviews.*
Enterprise Information Systems **8**(1), 1-25, 2014,
http://dx.doi.org/10.1080/17517575.2011.647092,

[44] Torabi, S.A.; Rezaei Soufi, H. and Sahebjamnia, N.: *A new framework for business impact analysis in business continuity management (with a case study).*
Safety Science **68**, 309-323, 2014,
http://dx.doi.org/10.1016/j.ssci.2014.04.017,

[45] Neil, M.; Marquez, D. and Fenton, N.: *Using Bayesian networks to model the operational risk to information technology infrastructure in financial institutions.*
Journal of Financial Transformation **22**, 131-138, 2008,

[46] Darwiche, A.: *Bayesian Networks.*
Communications of the ACM **53**(12), 80-90, 2010,
http://dx.doi.org/10.1145/1859204.1859227,

[47] Pearl, J.: *Probabilistic Reasoning in Intelligent Systems.*
Morgan-Kaufmann, San Francisco, 1988,

[48] Henrion, M.: *Practical issues in constructing a Bayes' belief network.*
3rd Conference on Uncertainty in Artificial Intelligence, Seattle, 10-12 July, 1987,

[49] Hinz, D.J. and Malinowski, J.: *Assessing the Risks of IT Infrastructure – A Personal Network Perspective.*
39th Annual Hawaii International Conference on System Sciences , Kauai, 4-7 Jan. 2006,

[50] Weber, P. and Suhner, M.: *System architecture design based on a Bayesian Networks method.*
10th Internationnal Symposium on Applied Stochastic Models and Data Analysis, Compiègne, June 2001,

[51] Wei, W.; Wang, H.; Yang, B. and Liu, L.: *A Bayesian Network Based Knowledge Engineering Framework for IT Service Management.*
IEEE Transactions on Services Computing **6**(1), 76-88, 2013,
http://dx.doi.org/10.1109/TSC.2011.34,

[52] Sommestad, T. and Ekstedt, M.: *Cyber security risks assessment with bayesian defense graphs and architectural models.*
42th Annual Hawaii International Conference on System Sciences. Kauai, 2009,

[53] Cemerlic, A.; Yang, L. and Kizza, J.: *Network intrusion detection based on bayesian networks.*
20th International Conference on Software Engineering & Knowledge Engineering. San Francisco, 2008,

[54] Simonsson, M.; Robert, L. and Johnson, P.: *A Bayesian network for IT governance performance prediction.*
10th international conference on Electronic commerce, Innsbruck, 18-22 August, 2008,

[55] Lande, S.; Zuo, Y. and Pimple, M.: *A Survivability Decision Model for Critical Information Systems Based on Bayesian Network.*
5th Annual Symposium on Information Assurance, New York, 16-17 June, 2010,

[56] Zhang, R.; Cope, E. and Heusler, L.: *A Bayesian Network Approach to Modeling IT Service Availability using System Logs.*
SOAP Workshop on the Analysis of System Logs., New York, 14th October 2009,

[57] Bonafede, E. and Cerchiello, P. *Statistical models for business continuity management.*
Journal of Operational Risk **2**(4), 79-96, 2007,

[58] Yu, Y.; Zheng, G. and Qian, Z. *Software Reliability Model Analysis Including Internal Structure Based on Bayesian Network.*
4th International Conference on Cooperation and Promotion of Information Resources in Science and Technology. Proceedings, IEEE, 2010,

[59] Dejaeger, K. and Verbraken, T.: *Towards comprehensible software fault prediction models using Bayesian network classifiers.*
Transactions on Software **1**(1), 1-22, 2012,

[60] Gran, B.: *Use of Bayesian Belief Networks when combining disparate sources of information in the safety assessment of software-based systems.*
International Journal of Systems Science **33**(6), 529-542, 2002,
http://dx.doi.org/10.1080/00207720210133589,

[61] Fenton, N.; Hearty, P.; Neil, M. and Radliński, Ł.*: Software project and quality modelling using Bayesian networks.*
In: Meziane, F. and Vadera, S., eds.: *Artificial Intelligence Applications for Improved Software Engineering Development: New Prospects*, IGI global, Hershey, 2009,

[62] Fineman, M.: *Improved Risk Analysis for Large Projects: Bayesian Networks Approach.*
Queen Mary, Unversity of London, 2010,

[63] Radliński, Ł.; Fenton, N. and Neil, M. *Improved decision-making for software managers using Bayesian networks.*
11th IASTED Internaional Conference on Software Engineering and Applications. Cambridge, 2007,

[64] Oniśko, A.; Druzdzel, M.J. and Wasyluk, H.: *Learning Bayesian network parameters from small data sets: Application of Noisy-OR gates.*
International Journal of Approximate Reasoning **27**(2), 165-182, 2001,
http://dx.doi.org/10.1016/S0888-613X(01)00039-1.