EVALUATION OF TECHNICAL SYSTEMS DEPENDABILITY WITH THE USE OF FUZZY LOGIC AND EXPERTS' KNOWLEDGE

Lech Bukowski
Faculty of Management, AGH University of Science and Technology
Cracow, Poland

and

Jerzy Feliks
Faculty of Management, AGH University of Science and Technology
Cracow, Poland

ABSTRACT

The paper proposes a general concept of technical systems dependability and describes a new dependability tree. In this vector based approach, the term dependability is composed of two main elements: availability, described by reliability, maintainability and maintenance support performance, as well as credibility, based on safety and security. A framework for evaluation of technical systems' dependability was developed, based on fuzzy logic and a system of rules of the „if … then" type, that were appropriately weighted. The model is based on a three-stage procedure of evaluating linguistic variables with the WinFACT tools and BORIS and FLOP simulation package. The results of the simulation, presented as 3-D graphs may be used to optimize the reliability of the system being evaluated.

Keywords: Dependability, Availability, Credibility, Safety, Security, Fuzzy Logic, Expert System.

1. INTRODUCTION

Usability of technical systems was previously characterized by three fundamental properties: functionality, performance and cost. Since late 1940s, artificial systems became more and more complicated and sophisticated, but also less and less reliable. The first generation of electronic computers used unreliable components, therefore practical techniques were employed to improve their reliability. In 1956 J. von Neumann [1], E. F. Moore and C. E. Shannon [2] developed theories of using redundancy to build reliable logic structures from less reliable components, whose faults were masked by the presence of multiple redundant components. The theories of masking redundancy were unified by W. H. Pierce as the concept of failure tolerance in 1965 [3]. In 1967, A. Avizienis integrated masking with the practical techniques of error detection, fault diagnosis, and recovery into the concept of fault-tolerant systems [3] and 8 years later work on software fault tolerance was done by B. Randell [4].

The emergence of a consistent set of new concepts and terminology resulted in the 1992 book *Dependability: Basic Concepts and Terminology* by J.-C. Laprie [5] and a new research area of "Dependable Computing" was born. Since that time, computing systems are characterized by four fundamental properties: functionality, performance, cost and dependability.

Dependability [6, 7] of a computing system is the ability to deliver service that can be justifiably trusted. The **service** delivered by a system is its behavior, as it is perceived by its user(s); a **user** is another (physical, human) system that interacts with the former one at a **service interface**. The **function** of a system is what the system is intended for and is described by system specifications. Dependability is an integrative concept that encompasses the following attributes:

Availability - readiness for correct service;
Reliability - continuity of correct service;
Safety - absence of catastrophic consequences on the user(s) and the environment;
Confidentiality - absence of unauthorized disclosure of information;
Integrity - absence of improper system state alterations;
Maintainability - ability to undergo repairs and modifications.

Security is the concurrent existence of:
a) availability for authorized users only,
b) confidentiality, and
c) integrity with 'improper' meaning 'unauthorized'.

The above attributes may be emphasized to a greater or lesser extent depending on the application: availability is always required, although to a varying degree, whereas reliability, safety and confidentiality may or may not be required. The extent to which a system possesses the attributes of dependability should be interpreted in a relative, probabilistic sense, and not in an absolute, deterministic sense. Due to the unavoidable presence or occurrence of faults, systems are never totally available, reliable, safe or secure. Definitions of availability and reliability emphasize the avoidance of failures, while safety and security emphasize the avoidance of a specific class of failures (catastrophic failures, unauthorized access or handling of information, respectively). Reliability and availability are thus closer to each other than they are to safety on one hand, and to security on the other; reliability and availability can be grouped together, and collectively defined as the avoidance or minimization of service outages.

2. GENERAL CONCEPT OF TECHNICAL SYSTEMS' DEPENDABILITY

The concept of "Dependable Computing" became very successful in the area of information technology (IT) and computer science (CS), but was not general enough, to cover all types of technical systems, e.g. production systems and logistics processes. The authors of this paper proposed at the International Conference on System Engineering in Las Vegas 2008 [8] a general concept of technical systems' dependability, which connected the computer oriented concept of dependability with experience from another areas of technical devices and equipments. We were trying to study such complex systems as:

- Intelligent building systems [9],
- Power supply and distribution systems [10],
- Manufacturing systems [11],
- Supply chain and network systems [12],

and we had many problems with defining their performance and quantitative characteristics, because every subsystem has a typical definition of attributes and characteristics (some of them even have standards, e.g. IEC 50 191, IEC 1069). The goal of this idea was to create one uniform set of attributes for all these systems as a base to analyze, design and optimize complex technical systems. The proposed general dependability tree is shown below [8].

DEPENDABILITY
- AVAILABILITY
  - Reliability
  - Maintainability
  - Maintenance Support Performance
- CREDIBILITY
  - Safety
  - Security

The various concepts included in this diagram in a hierarchical tree-type structures are defined as follows.

Dependability of a technical system is the ability to deliver service that is available and credible under given conditions at a given instant or in a given time interval.

Availability (AV) – the ability of a system to be in a state of performing a required function under given conditions at a given instant or in a given time interval, assuming that the required external resources are provided.

Reliability (REL) is a feature of the performance system achieving the required level by using elements characterized by proper values of reliability measures (frequency or time) as well as by applying proper dependability structures (e.g. surplus ones).

Maintainability (MAI) is a feature of the performance system characterizing the compliance of the system itself for detecting dangers, identifying the state as well as executing the actions (both planned and unplanned) connected with servicing the system. Maintainability indicators are both frequential (e.g. probability of servicing, temporary and average intensity of repair) and temporal (e.g. expected reparation time, p-row quintile of reparation time).

Maintenance Support Performance (MSP) is the measure of dependability of logistic processes supporting servicing the performance system. These are usually processes of providing with proper resources, while indicators of provisions of servicing are usually temporal (e.g. presumed logistics delay, p-row quintile of logistics delay).

As it derives from the above approach, the readiness of the performance system shall be expressed in a vector format, not the hitherto applied scalar one, by one of indicators such as momentary availability $A(t)$ or average availability $A(\Delta t)$.

When applying relative measures of indicators or providing balances for specified components of the vector, it is possible to find the value of availability as the scalar ratio of separate components of the vector and their balances.

Credibility (CR) – the extend to which a system is able to recognize and signal the state of the system and to withstand incorrect inputs or unauthorized access.

Credibility of the system is defined by two components:

Safety (SAF) is displayed by
- ✓ absence of critical damages (active actions),
- ✓ securing the environment against the effects of any potential critical damages (passive actions),

Security (SEC) is displayed by
- ✓ confidentiality (unavailability to unauthorized users),
- ✓ integrity (impossibility of introducing changes into the system by unauthorized users) and
- ✓ availability (accessibility for authorized users only).

It is proposed to accept the following model for a quantitative measure of dependability:

$$D = \{AV, CR\}$$

$$AV = \{REL, MAI, MSP\}$$

$$CR = \{SAF, SEC\}$$

3. FRAMEWORK FOR EVALUATION OF TECHNICAL SYSTEMS‘ DEPENDABILITY

For evaluating the availability of a system, it is proposed to apply linguistic variables, quantified in various ways, depending on the type of the system. Fuzzy sets were used at several stages of building experts system. Inputs for a fuzzy system are REL, MAI and MSP variables. The evaluation procedure was described in [8].

For evaluating the credibility of the system, it is proposed to also apply linguistic variables, quantified in various ways, depending on the type of the system, SAF and SEC. Examples of applying measures in the form of linguistic variables for evaluating the components of a credibility vector are presented in [13]. Methods for describing parameters with the use of linguistic variables allow using fuzzy sets as a tool for building expert systems, in which linguistic variables are used as input variables of the system. The application of fuzzy sets theory in this case is suitable because experts’ knowledge can be used to build a suitable rule base.

The software WinFACT was used for building a system for evaluating the components of the availability and credibility vector. WinFACT provides FLOP tools for creating and editing fuzzy inference systems or integrating our fuzzy systems into simulations with BORIS. The fuzzy shell FLOP (Fuzzy Logic Operating Program) allows the design and the analysis of rule based systems on the basis of fuzzy logic. The program offers the following options: definition of linguistic variables and corresponding terms, creation of rule bases, realization of inference processes, evaluation of transfer characteristic curves and maps, simulation based on recorded data and creation of fuzzy controller files for the block oriented simulation system BORIS [14]. The block orientated simulation hardware BORIS allows the simulation of nearly any structured dynamic system and is therefore in - connection with the hardware interface and the optional C-code-generation - suitable for the following applications: measurement and signal analysis as well as analysis and synthesis of feedback control systems. In addition to the known conventional systems, even systems with fuzzy or neural components can be handled.

Classical fuzzy sets with trapezoidal membership functions were used in building the credibility evaluation system. Linguistic variables SAFETY (SAF) and SECURITY (SEC) were assigned five classes by defining for both of them ranges of trapezoidal membership functions. Membership ranges are shown in figure 1. Membership in class 1 in the case of the SAFETY variable indicates the highest probability of no critical failure whereas for the SECURITY variable, it indicates the highest level of protection. Thus an increase in class number corresponds to a decrease in both safety and security. Class 5 represents the lowest level of safety and security.

Class number	Safety (SAF)	Security (SEC)
Class_1	Very high (>99,99%)	Very high (>99,99%)
Class_2	High (99,7% – 99,99%)	High (99,7% – 99,99%)
Class_3	Moderate (98% - 99,7%)	Moderate (98% - 99,7%)
Class_4	Low (90% - 98%)	Low (90% - 98%)
Class_5	Very low (< 90%)	Very low (< 90%)

Figure 1. Membership ranges

The structure of the credibility evaluation system is show in figure 2.

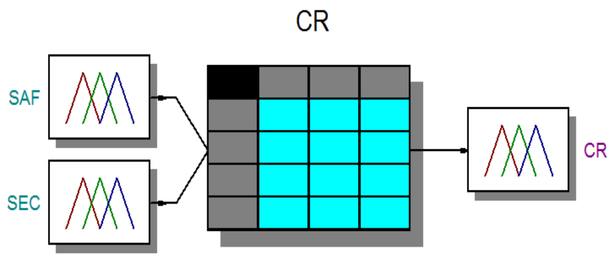


Figure 2. System structure

The definition of fuzzy sets and ranges of the membership function for the input variable SAFETY are show in figure 3.

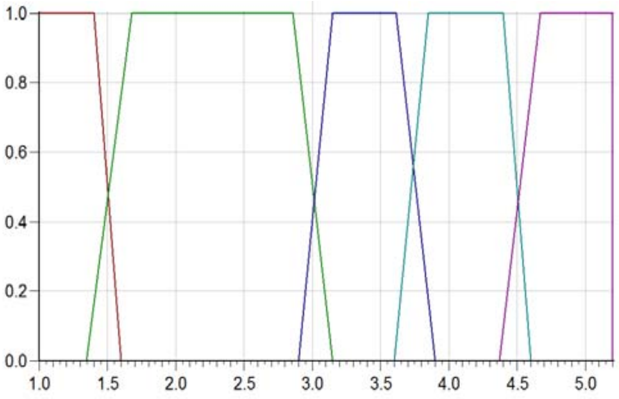


Figure 3. Definition of fuzzy sets and ranges of the membership function (SAF)

The ranges and shape of the membership function for the SECURITY variable are show in figure 4.

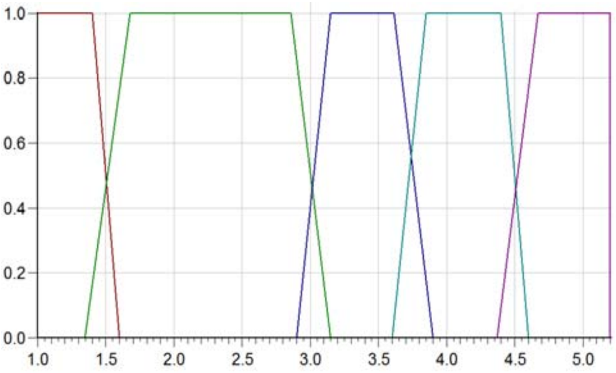


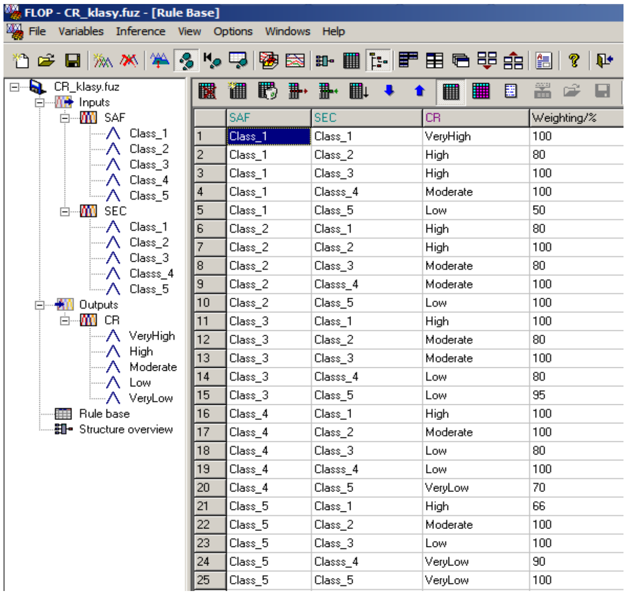
Figure 4. Ranges and shape of membership function for the security variable (SEC)

Based on input variables defined in this way for the CREDIBILITY evaluation system, an appropriate rule base was designed. Experts' knowledge can be represented in the form of "if – then" rules. A single „if – then" rule assumes the form:

if x is A then y is B (w)

where A and B are linguistic values defined by fuzzy sets. The if-part of the 'x is A' rule is called the antecedent or premise, while the then-part of the 'y is B' rule is called the consequent or conclusion. The number 'w' in the parentheses above represents weights between zero and one that can be applied to each rule if desired.

The „if … then" rules make it possible to evaluate complex fuzzy statements. The knowledge encoded in the rule base is inputted based on human experience and intuition as well on the basis of theoretical and practical understanding of the studied object's properties. The main task of this evaluation system is to calculate an approximate value of the output variable on the basis of each rule from the rule base weighted by an appropriate factor determining the degree of rule "validity"



	SAF	SEC	CR	Weighting/%
1	Class_1	Class_1	VeryHigh	100
2	Class_1	Class_2	High	80
3	Class_1	Class_3	High	100
4	Class_1	Classs_4	Moderate	100
5	Class_1	Class_5	Low	50
6	Class_2	Class_1	High	80
7	Class_2	Class_2	High	100
8	Class_2	Class_3	Moderate	80
9	Class_2	Classs_4	Moderate	100
10	Class_2	Class_5	Low	100
11	Class_3	Class_1	High	100
12	Class_3	Class_2	Moderate	80
13	Class_3	Class_3	Moderate	100
14	Class_3	Classs_4	Low	80
15	Class_3	Class_5	Low	95
16	Class_4	Class_1	High	100
17	Class_4	Class_2	Moderate	100
18	Class_4	Class_3	Low	80
19	Class_4	Classs_4	Low	100
20	Class_4	Class_5	VeryLow	70
21	Class_5	Class_1	High	66
22	Class_5	Class_2	Moderate	100
23	Class_5	Class_3	Low	100
24	Class_5	Classs_4	VeryLow	90
25	Class_5	Class_5	VeryLow	100

Figure 5. Rule base example

Fuzzy logic based systems are a kind of expert system built on a knowledge base that contains inference algorithms in the form of a rule base. What distinguishes fuzzy inference in terms of concept from conventional inference is the lack of an analytical description. The approximate inference mechanism transforms knowledge from the rule base into a non-fuzzy form. The non-fuzzy form of the result is obtained in the process of defuzzification. There are several known methods of defuzzification – the algorithms used in the FLOP software include: center of gravity, center of gravity with extender border sets, first maxima and last maxima. Defuzzification is interpreting the membership degrees of fuzzy sets into a real value. A rules base for a system with two inputs and one output, where every variable was divided into 5 linguistic categories (VeryLow, Low, Moderate High and VeryHigh), includes 25 elements. The correctness of selection of rules as well as the shape and ranges of the membership function is verified with a rules viewer and simulation. The rules viewer displays a roadmap of the whole fuzzy inference process. It also shows how the shape of certain membership functions influences the overall result. The ranges and shape of the membership function for the CREDIBILITY variable are show in figure 6.

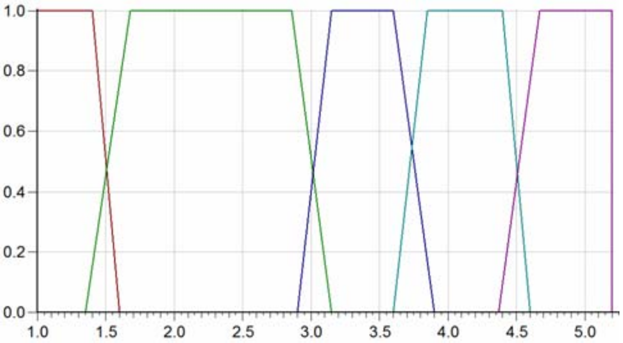


Figure 6. Ranges and shape of membership function for the credibility (CR) variable

Figure 7 presents a simulation model of a credibility evaluation system and figure 8 the results of a simulation in the form a graph showing the dependence of the output variable on the input variable.

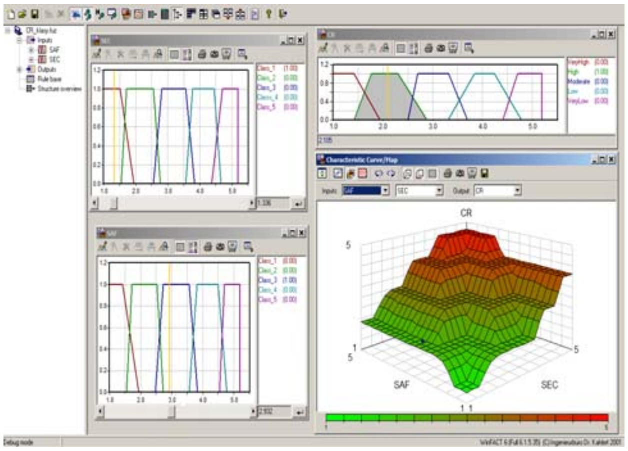


Figure 7. Credibility simulation model

The output signal of the model is a number ranging from 1 to 5 specifying class membership. Credibility expressed as a number ranging from 1 to 5 and availability also expressed as a number ranging from 1 to 5 are inputs for the dependability evaluation system. This system is implemented using fuzzy sets. Its inputs are values generated by the credibility evaluation system described above and the availability evaluation system presented in (8).

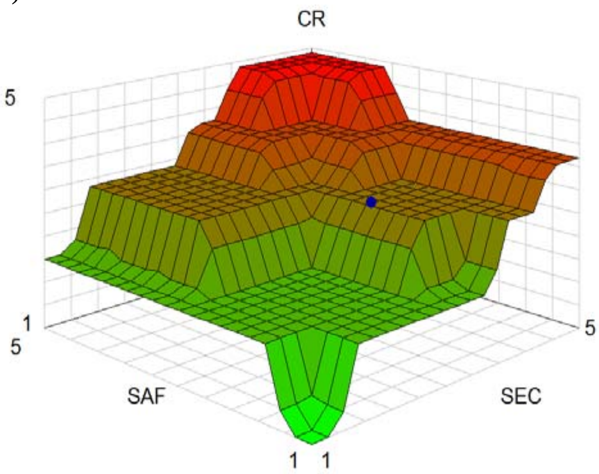


Figure 8. Credibility (CR) model simulation results

The hierarchical structure of the system for evaluation of technical systems DEPENDABILITY is show in figure 9.

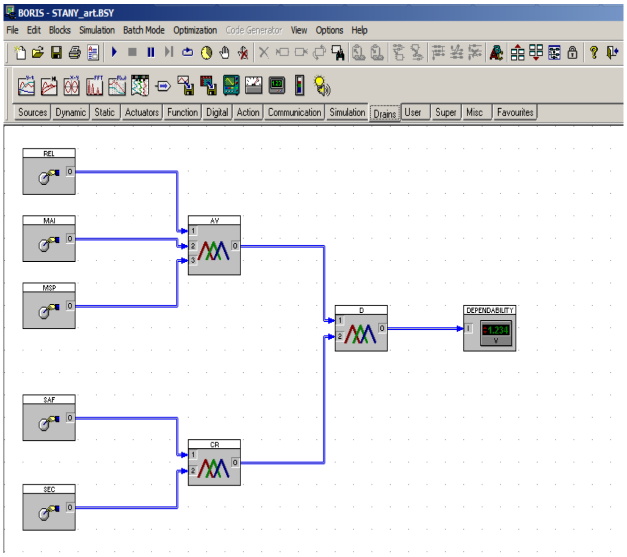

BORIS - STANY_art.BSY
File Edit Blocks Simulation Batch Mode Optimization Code Generator View Options Help
Sources Dynamic Static Actuators Function Digital Action Communication Simulation Drains User Super Misc Favourites
REL
MAI
MSP
SAF
SEC
AV
CR
D
DEPENDABILITY

Figure 9 Model dependability (D) structure

As before, fuzzy sets with trapezoidal membership functions were used for the implementation of the model. Ranges of individual membership functions for input variables credibility and availability are shown in figure 10 and figure 11.

As in the previous case for a system with two inputs and one output, a complete rule base made up of 25 if … then type rules was designed. Each rule was assigned an appropriate weighing factor w that was chosen by a method of “trial and error” based on simulation studies.

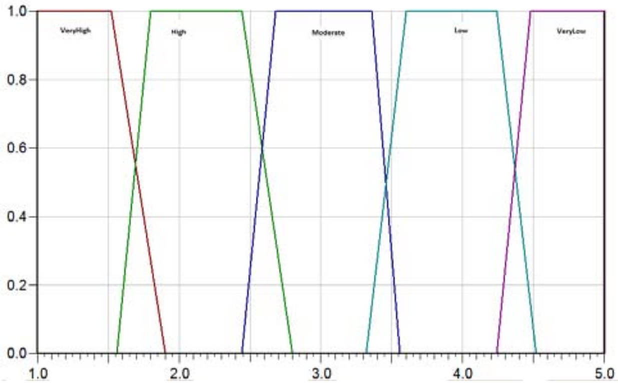


Figure 10. Availability (AV) membership functions

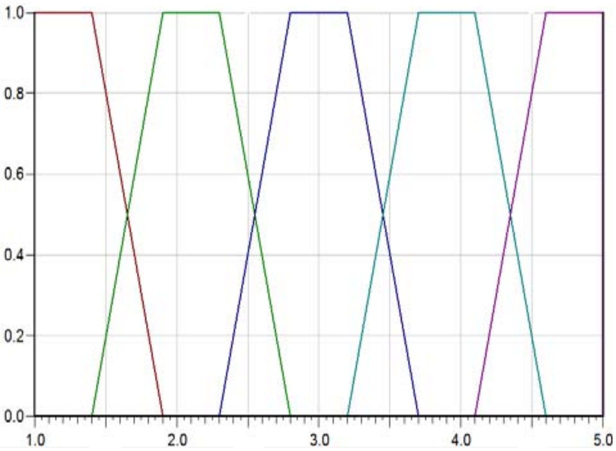


Figure 11. Credibility CR membership functions

Simulations were carried out in the BORIS software to observe the impact of changes in five input parameters on the output of the hierarchical model.

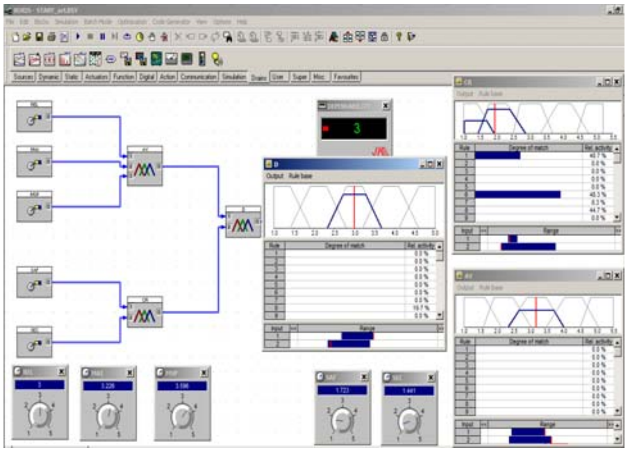


Figure 12. Dependability (D) simulation model

Each input parameter can be set at a level ranging from 1 to 5. The implemented simulation system allows for continuous observation of changes in output depending on the value of input signals. Simulation of the system can run in a specified time interval or continuously until it is ended with the press of a special button. Input signal levels are set in a range from 1 to 5 using dials operated by a computer mouse or by typing on a keyboard. In addition, during the simulation, it is possible to observe the degree to which credibility, availability and dependability variables belong to given membership functions and it is also possible to identify the rules involved in generating system output as well as changes in credibility and availability variables that are functions of changes in input values.

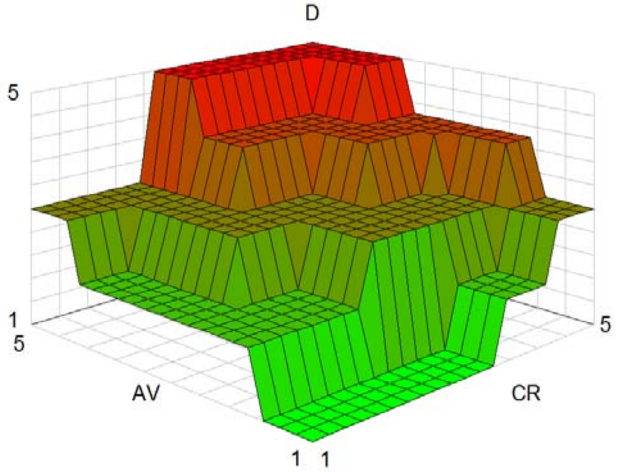


Figure 13. Model dependability D simulation results

Figure 13 shows the results of the dependability evaluation simulation model depending on values of variables credibility and availability. Dependability is evaluated on 5 levels with the first level corresponding to the highest degree of system reliability. As shown in figure 13, the variable availability, most frequently associated with the operation of objects, has a higher impact on system reliability evaluation results.

4. CONCLUSION

The framework for evaluation of technical systems dependability proposed in this paper is a universal, "shell" type model that can be applied to verifying and validating the reliability of various types of technical and sociotechnical systems, especially at the design stage. Adapting this tool to the needs of a particular type of system or a specific practical case requires the estimation of numerical values (or ranges) corresponding to each parameter class. In the case of using triangular or trapezoidal membership function models for linguistic variables, one may assume that that the measure of uncertainty in quantitative estimates is the angle of inclination of the sides of the triangles or trapezoids (a right angle corresponds to a lack of uncertainty in the estimate, and the smaller the angle, the larger the uncertainty).

Acknowledgments

The work was supported by research grant nr N N509 3114 33 from the Ministry of Science and Higher Education.

5. REFERENCES

[1] J. von Neumann: *Probabilistic logics and the synthesis of reliable organisms from unreliable components*. In C. E. Shannon and J. McCarthy, editors, Annals of Math Studies, numbers 34, pages 43-98. Princeton Univ. Press, 1956.

[2] E.F. Moore and C.E. Shannon: *Reliable circuits using less reliable relays*. J. Franklin Institute, 262:191-208 and 281-297, Sept/Oc. 1956.

[3] W.H. Pierce: *Failure-Tolerant Computer Design.* Academic Press, 1965.

[4] A. Avizienis: *Design of fault-tolerant computers*. In Proc. 1967 Fall Joint Computer Conf., AFIPS Conf. Proc. Vol. 31, pages 733-743, 1967.

[5] B. Randell: *System structure for software fault tolerance.* IEEE Transactions on Software Engineering, SE-1:1220-232, 1975.

[6] J.C. Laprie, editor. *Dependability: Basic Concepts and Terminology*. Springer-Verlag, 1992.

[7] A. Avizienis, J.-C. Laprie, and B. Randell: *Dependability of computer systems: Fundamental concepts, terminology, and examples*. Technical report, LAAS-CNRS, October 2000.

[8] L. Bukowski, J. Feliks: *Vectorial Concept of Dependability – Theoretical Framework and Examples.* Proceedings of the 19-th International Conference on Systems Engineering – Las Vegas 2008, IEEE CS.

[9] L. Bukowski, M. Karkula: *Reliability Assurance of Integrated Automation Systems by Applying the Redundancies.* 3rd International Congress on Intelligent Building Systems, Cracow 2004.

[10] L. Bukowski, M. Karkula: *Modeling and simulation of logistics processes in heat and power plants – a hybrid approach.* Proceedings of the Twentieth International Conference on Systems Engineering – ICSE 2009, ISBN 978-1-84600-0294; Coventry, United Kingdom, 2009.

[11] L. Bukowski, A. Lichota: *Capability indices analysis for processes revealing significant asymmetry with respect to tolerance limits*. Effectiveness of the machines maintenance and processes; Novosibirsk State Technical University, 2009.

[12] L. Bukowski: *Concept of supply chain resilience – how secure is secure enough?*. Proceedings of the 14-th International Conference on Total Logistic Management – Zakopane, December 2010.

[13] L. Bukowski, J. Feliks: *Application of Fuzzy Sets in Evaluation of Failure Likelihood.* Proceedings of the 18-th International Conference on Systems Engineering – Las Vegas 2005, IEEE CS.

[14] *WinFACT User Guide.*