Dependability of e-information sources

Jan Capek
University of Pardubice, Faculty of Economics and Administration, Institute of System Engineering and Informatics.
Czech Republic

1. Introduction

The contemporary world is without any doubts based on using information from a plenty of information sources generally and E-based information sources especially. The Web can be considered a good representative of E-information source. Today, the Web is a medium which allows remote, fast and easy access to information. In general, the main aim of the Web is to allow people to share information. Information can be distributed over the whole world but users do not need to care about it. The architecture of the Web was proposed to be simple and undemanding. The Web is loosely coupled. It means minimum coordination between client and server is required. Their communication is based on a simple request and response transaction (Shirky, C., 2002)

The Web focuses on information activities – like Information Needs, Seeking and Use (INSU) – on various professional and other everyday life settings. There are very few INSU studies that are based on individual tasks. Most studies, and especially those which relate INSU to task complexity, have considered the phenomenon studied on the basis of jobs (i.e., as a host of certain tasks) (e.g., Tiamiyu, 1992; Culnan, 1983, Hart & Rice, 1991; Van de Ven & Ferry, 1980). In this respect, the present study covers an area that has not previously been addressed within INSU research. Since no conceptual model concentrates sufficiently clearly on the aspects of tasks and INSU, one was created to serve the present work (Byström K., & Järvelin, 1995; Byström K., 1996; Byström K., 1997, Byström K,, 1999).

An illustrative pyramid diagram as per Byström, (Byström K.,1999) for the information activities is presented in Figure 1. Each corner of the pyramid represents one of the four main dimensions emphasised in information activities. One corner of the pyramid is occupied by the *means* of information seeking (e.g., information systems, information services, information seeking channels and information sources), another by *information* (e.g., type of information, content of information, usability of information), a third by *individuals* (e.g., cognitive styles, information seeking styles, information profiles, and demographic factors), and a fourth by *contexts* (e.g., aspects of work organizations, jobs, individual tasks, and everyday life situations).

In the following sections we focus our attention on one corner of pyramid from Figure. 1, only. The selected corner is *means* of information seeking and from this problem point of view there are information sources represented by the Web.

Most of information sources nowadays are concentrated in the Web and the information access ability through information sources placed on the net rest on dependability of these sources.

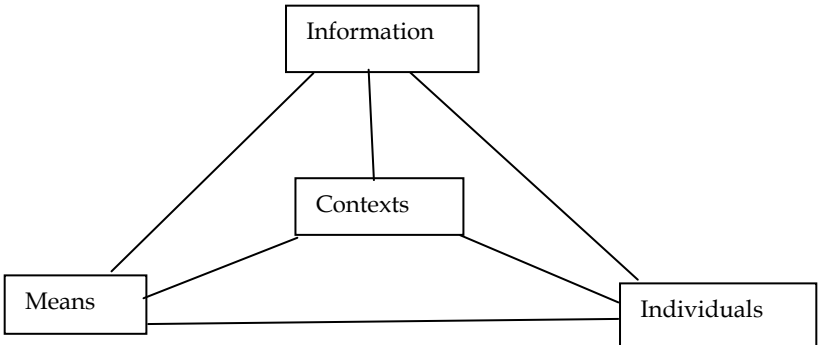


Fig. 1. Information activities as per Byström (Byström K., 1999)

1.1 Related works

Web based information sources described as Web information systems (Schewe & Thalheim, 2009) are extending in portfolios associated with content and functionality. Within the information portfolio it is distinguished between the information need and the information demand. The information need is generally related to objectives such as becoming informed. The information demand is related to the portfolio under consideration and to the intents.

The service oriented architecture (SOA) was proposed to provide interoperability between different systems but it is still based on the same principle as the Web, i.e. it is loosely coupled as well. An important advantage is that it allows to code client applications against an abstract service, not against a particular server 0. SOA is understood as a form of distributed system architecture of the following nature (Booth et al 2004):

- The service is designed to provide some operation so it is a logical view of software application, database, business process, etc.
- The service is formally described by messages exchanged between participants, not by participants' properties and structure
- Messages are platform-neutral and well standardized and they are delivered through appropriate interfaces
- The service is described by meta-data which can be processed by a machine
- Services are usually used over network

Distributed system can be implemented by means of various technologies, e.g. COM/CORBA or Web services (Booth et al 2004).

Web services solutions by Web Ontology Language for Service (OWL-S) and connection with Petri nets were done by Miao and He (Miao & He 2009). Within this work there is a nice overview of the related works associated with this topic. Authors proposed Petri net based algebra for composing Web service, as well.

(Krekora & Caban 2007) presents that failures of hardware are now relatively rare due to development of new design and materials technologies. The traditional meaning of

reliability measures does not reflect the real dependability of systems. The principle sources of the failures causing unavailability of the services are faults introduced to the system through the installed software and conscious or unconscious activities of users. System reconfiguration proposed by (Krekora & Caban 2007) is realized by modifying the routes and by moving the services between nodes Figure 2
For example Puustjärvi (Puustjärvi 2009) assumes that, for instance a composed Web service is made up of Flight reservation Web service and Hotel Web service. In this case the success of the hotel reservation may be useless if the flight reservation fails. This failure of service was done probably by technical system malfunctions or human lapse or both. The problems of reliability to system safety and its role within system risk analysis was showed in the review article by Zio (Zio 2009) In this paper Zio shared some considerations with respect to a number of problems and challenges which researchers and practitioners face in reliability engineering when analyzing today's complex systems.
An interesting work which contributed to the research in the field of information fusion for computer security was presented by Bass (Bass 2000). Corona et al. continue in Bass's ideas (Corona et al. 2009) by introducing data fusion decomposition into two parts: data organization and data reconciliation. Data organizations solve mainly topology problem e.g. where data is acquired, data reconciliation solves data content problem.

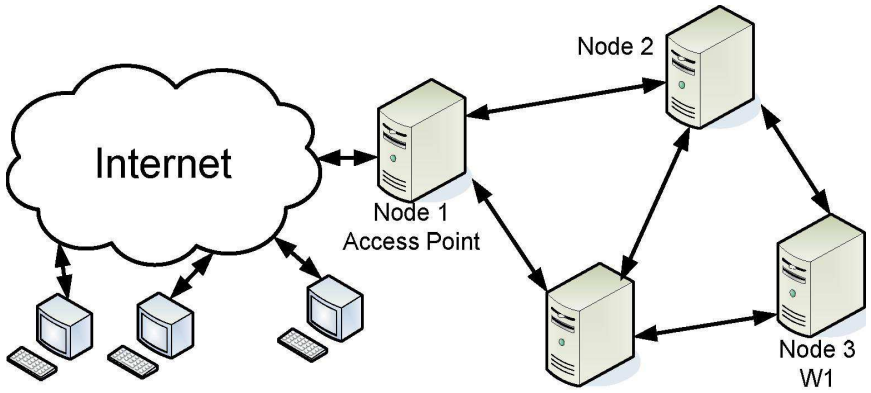


Fig. 2. Example of system providing access to a particular service by (Krekora & Caban 2007)

Within following sections the proposed solutions will be described.

2. Essential characteristics of web services

Web services were designed to further improve information sharing thanks to increased interoperability between different software applications (Booth et al 2004). Web services belong to distributed, platform independent Internet-based computing technologies. They can be understood as a successor to Electronic Data Interchange (EDI) (Papazoglou & Georgakopoulos 2003), (Samtani & Sadhwani 2004), (Shirky 2002).
Definition of a web service provided by W3C (Booth et al 2004): "A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-process-able format (specifically WSDL).

Other systems interact with the Web service in a manner prescribed by its description using SOAP (Simple Object Access Protocol) messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards."
In other words, services can be characterized as (Papazoglou 2003) "self-describing open components that support rapid, low-cost composition of distributed applications."
At first, a service has to be published. Then, three phases of interaction between caller and callee can be

- Service discovery – search of a services by caller based on repositories (e.g. UDDI)
- Service Selection – caller chooses an instance of a desired service
- Service Binding – caller begins to use the service

As it was noticed above, distributed application can be built from independent service components. Communication between client (caller) and server (callee) is based on standardized SOAP over e.g. HTTP or SMTP (Khoshafian 2006)
Resulting application (composite service) must be able to provide the following functions (Papazoglou.2003):

- Coordination of component services, their controlling and management of data flow among services
- Monitoring of component services and publishing event information
- Conformance – ensuring the integrity of component services
- Quality of service (QoS) to ensure overall costs, performance, security, authentication, privacy, (transactional) integrity, reliability, scalability, and availability.

Today, several architectural styles are available: at least SOAP and REST (Representational State Transfer) based architectures can be used. Among others, they vary in a level of tightness of loose coupling and they are more suitable for different situations (Fielding 2002), (Pautasso, & Wilde 2009).
Modern web services allow various ways of communication between participants – see Fig. 3 .

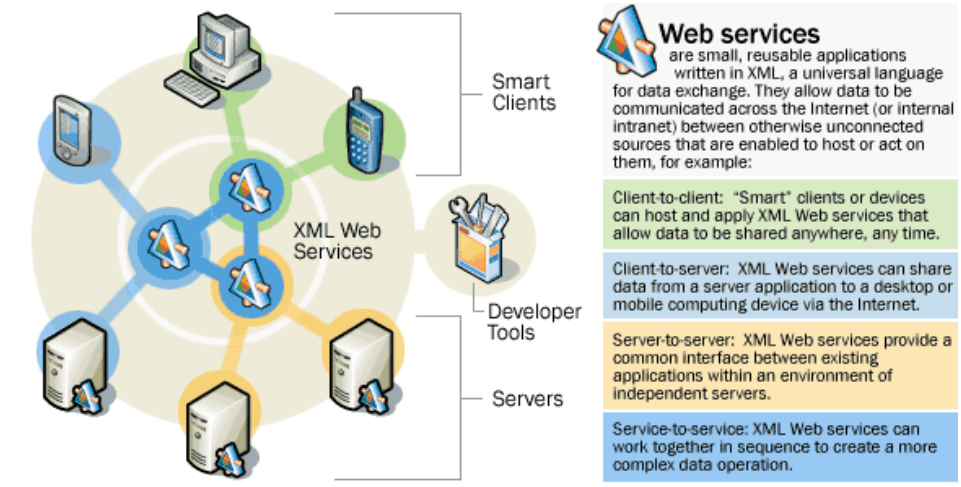


Fig. 3. Modern Web Services (MSDN.NET 2009)

Some challenges of web services are latency and unreliability of the underlying transport layers, concurrent access to remote sources and fragility of distributed system (partial failures) (Booth et al 2004).
A fully regular way of communication between caller and callee can be applied in the case of GIS for example see Fig.

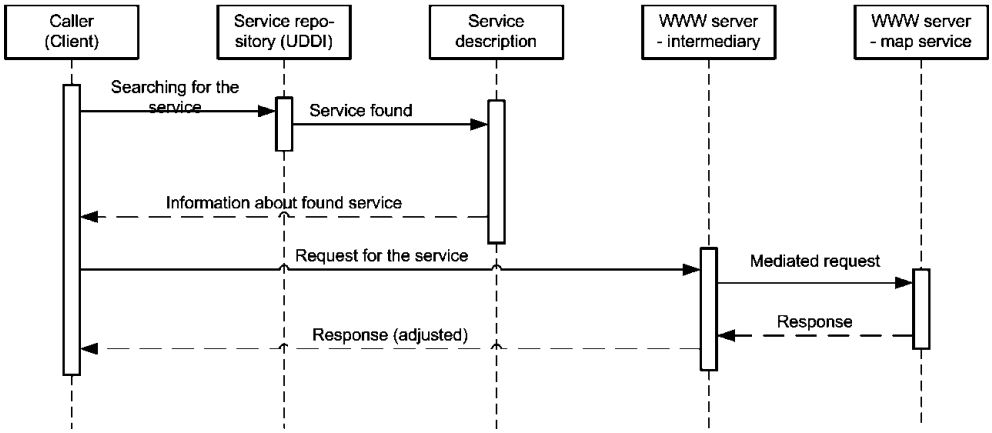


Fig. 4. Scenario of Communication between Caller and Callee (based on (Khoshafian 2006)).

The technological leaps of the past decades in computers, electronics, optics and advance high –performance, complex control system have created the needs for extra reliability and safety. An underlying feature of all "safety critical"systems entails a reliable fault-detection (and then isolation and reconfiguration) system. For the reason, we focus our future steps into these boundary elements. Information sources are usually accessible though Web technologies, so the connection of information sources generally and Web services lead to narrowing of thinking on the E-information sources, only with taking into mind the Web services. The crucial problem of the E-information sources, apart from the content of acquired information, is dependability of the whole system. First of all is the need to notice that the term reliability as is obvious defined (Wikipedia 2010) as"...ability of system or component to perform its required functions under stated conditions for a specified conditions for a specified period of time" began to become overloaded and was being used outside of its originally intended definition, as a measurement of failures in a system to encompass more diverse measures which would now come under other classifications such as safety, integrity, etc. With the term reliability is connected well known standby coefficient K, according to formula (1)

$$K = \frac{MTBF}{MTBF - MTTR} \tag{1}$$

Where: MTBF is the Mean Time Between Failures, MTTR is the Mean Time to Restart.
Jean Claude Laprie thus first used term Dependability (Laprie 1985) to encompass these related disciplines in general; quantitative definition of dependability is the ability to deliver service that can justifiably be trusted.

As developed over the past three decades, dependability is an integrating concept and Avizenis showed (Avizienis et al. 2001, 2004) that the general, qualitative, definition of *dependability* is: the ability to deliver service that can justifiably be trusted (Fig. 5). This definition stresses the need for justification of trust. The alternate, quantitative, definition that provides the criterion for deciding if the service is dependable is: dependability of a system is the ability to avoid service failures that are more frequent and more severe than is acceptable to the user(s). Dependability covered 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 alterations;
- **maintainability**: ability to undergo, modifications, and repairs.

As these definitions suggested, only Availability and Reliability are quantifiable by direct measurements whilst others are more subjective. For instance Safety cannot be measured directly via metrics but is a subjective assessment that requires judgmental information to be applied to give a level of confidence, whilst Reliability can be measured as failures over time.

Threats are things that can affect a system and cause a drop in Dependability. There are three main terms that must be clearly understood (Avizienis et al. 2001, 2004):

- Fault: A fault (which is usually referred to as a bug for historic reasons) is a defect in a system. The presence of a fault in a system may or may not lead to a failure, for instance although a system may contain a fault its input and state conditions may never cause this fault to be executed in such a way that an error occurs and thus never exhibits as a failure.
- Error: An error is a discrepancy between the intended behaviour of a system and its actual behaviour inside the system boundary. Errors occur at runtime when some part of the system enters an unexpected state due to the activation of a fault. Since errors are generated from invalid states they are hard to observe without special mechanisms, such as debuggers or debug output to logs.
- Failure: A failure is an instance in time when a system displays behaviour that is contrary to its specification. An error may not necessarily cause a failure, for instance an exception may be thrown by the system but this may be caught and handled using fault tolerance techniques so the overall operation of the system will conform to the specification.

Dependability is defined as the capacity of systems to provide services regardless the reasons of obstacles in accessing them. This concept covers the terms connected with the classical reliability as well as software reliability, user faults, intruder activities and network security. (Krekora & Caban 2007)

The dependability of the information systems is more complex problem then Avizenis et al. (Avizenis et al., 2001, 2004) showed. It is needed to include risk dimensions into this scheme, because many damages of information systems are due to hackers and intruders on the one, Internet side, and own employees on the other side. The modified dependability tree which includes risks is on the figure 7.

Internet is a hideaway for hackers and intruders who are ready to hack organizations connected to the global Internet. New ways to attack and damage are continuously being developed and so there are many kinds of threats. Risk from the Internet can be divided into

a) external attacks
b) intrusions
c) malicious software like viruses and worms

It is still important to notice that often security problems have their roots inside the company.

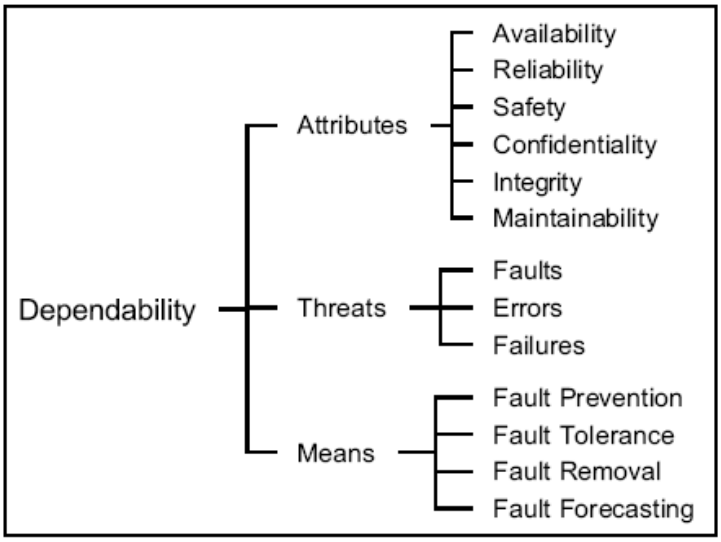


Fig. 5. The dependability tree as per Avizenis (Avizenis et all, 2001, 2004)

Risk is a function of the likelihood of given threat-sources utilizing a particular potential vulnerability and the resulting impact of that adverse event on the organisation (OISRMH 2006) According Ryan (Ryan & Ryan 1995) we can put the previous opinion into the following formula with adding the countermeasures:

$$\text{Risk} = \frac{\text{Threat} \quad \text{x} \quad \text{Vulnerability} \quad \text{x} \quad \text{Impact}}{\text{Countermeasures}} \tag{2}$$

Threats are posed by organizations or individuals who both intend to us harm and have the capability to accomplish their intentions, see for example Figure 6. These types of threat and measures that that may be taken to reduce or eliminate the risks, which may appear in the form of enemy forces, spies, criminals, terrorists, psychotics, computer hackers, drug lords, or saboteurs, are based on human activities Threats must be coupled with threat sources to become dangerous. So these types of threats are different from threats describes by Avizenis (Avizenis et al., 2001, 2004)
System vulnerability is defined to be the *intersection* of a system susceptibility or flaw, access to the flaw, and the capability to exploit the flaw (SPI 2007)

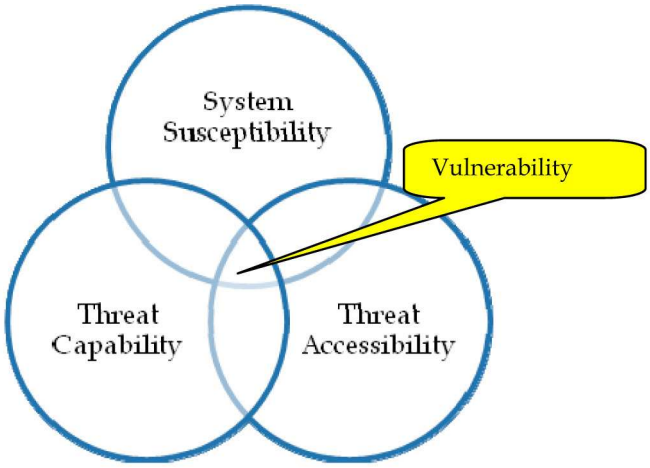


Fig. 6. The threat model by SPI (SPI 2007)

Basically one can study the risk form countermeasures point of view in the two limit cases (3), (4).

$$\text{Risk} = \lim_{C \to 0} \frac{\text{Threat} \quad x \quad \text{Vulnerability} \quad x \quad \text{Impact}}{\text{Countermeasures}} \tag{3}$$

Where in formulas (3) and (4) "C" under limits denotes countermeasure.
The first limit case supposes that no countermeasure was done so risk arises to infinity. In fact it is not true, but risk without countermeasure will be increasing while the cost for countermeasure is zero. The second limit case supposes that the cost for countermeasure is unlimited or in fact very high, so the risk is depressing. But one cannot forget that despite unlimited cost for countermeasure the risk can never be eliminated to zero.

$$\text{Risk} = \lim_{C \to \infty} \frac{\text{Threat} \quad x \quad \text{Vulnerability} \quad x \quad \text{Impact}}{\text{Countermeasures}} \tag{4}$$

A simplified diagram of the quantitative risk assessment is shown in the Figure 7

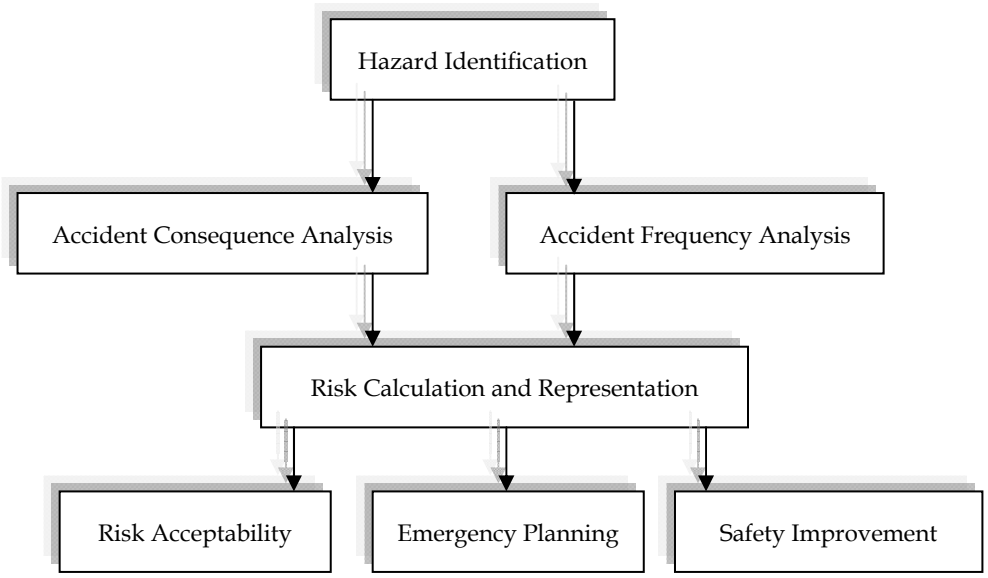


Fig. 7. Simplified diagram of the quantitative risk assessment modified according Contini (Contini at all 2000)

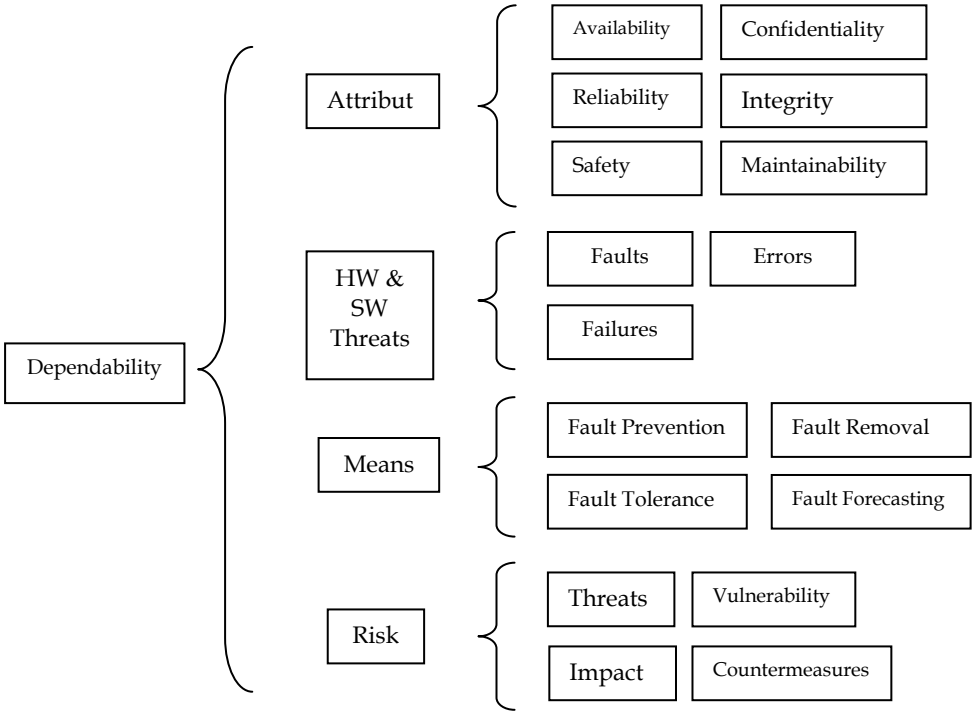


Fig. 8. Modification of Avizenis dependability tree by Capek (2008)

3. E-Information sources

An interesting work which contributed to the research in the field of information fusion for computer security is presented in (Bass T., 2000). In that paper the author proposed a general scheme to perform information fusion for intrusion detection in computer systems. The proposed scheme (Figure 9) is structured in 5 layers, and fill up the semantic gap between the abstraction level and its (higher) subsequent. Such a scheme is composed from the following stages: Level 0. Block "Data collection", acquired from a set of sensors (e.g. network sniffers, information acquisition).
Level 1. Block "Object improvement". A common framework is used to align all information. Here a spatial and temporal correlation of data carrying information is performed.
Level 2. Block "Situation refinement." Multiple objects are correlated in the context of an information base, using high level features, like their behaviour, dependencies, common targets and origin, protocols, attack rates etc.
Level 3. Block "Threat assessment". Multiple objects and predefined Intrusion Detection templates applied to the current situational knowledge are used to assess the threats related to. Through the correlation of information at this level with the security policies, implications associated to the current situation base are obtained.
Level 4. Block "Resource management".
Final block "Knowledge". The output of this block is information source (warehouse).

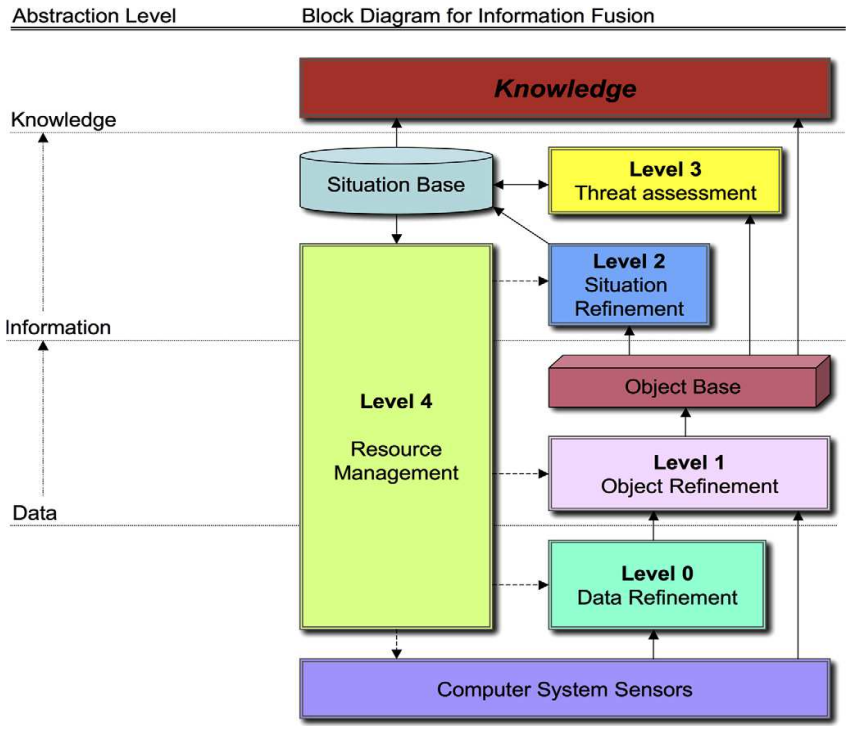


Fig. 9. Bass's suggestion on information fusion in information source (Bass T., 2000).

For important e-information sources the information fusion can be obtained when the information sources are parallelized. It increases not only reliability (see Table 1) from the technical point of view, but also information contents credibility. If one supposes that the probability of the errorless information source's activity has the exponential division we can obtain the following table of reliability set of information sources. An example can be found in (O'Connor 1988). From Table 1 it is clear that increasing number of information sources of the same quantity leads to increasing the reliability set of information sources, but from a certain number of information sources the output reliability increases slowly. If two information sources are used instead of one, the reliability increases but it is hardly to possible discover which of those information sources has valid information, when one of them has a nontrivial error.

Number of information sources	Reliability set of information sources
1	0.8000
2	0.9600
3	0.9920
4	0.9984

Table 1. Reliability set of information sources (O'Connor 1988).

From this point of view, it is clear that the number of information sources must be equal to or more than three for the possibility to determine not only that all outputs of the information sources are the same, but also to determine which element of set of the information sources has an error.

3.1 Majority system of the set of information sources.

A simple majority system of n- information sources is shown in Fig. 10. It is supposed that we use the minimal number of information sources, i.e. three information sources. Let us denote the output signal from the first information source o1, from the second information source o2 and from the last information source o3. The majority of the same output signals from the information sources is supposed to be the right value which goes from the evaluating algorithm.

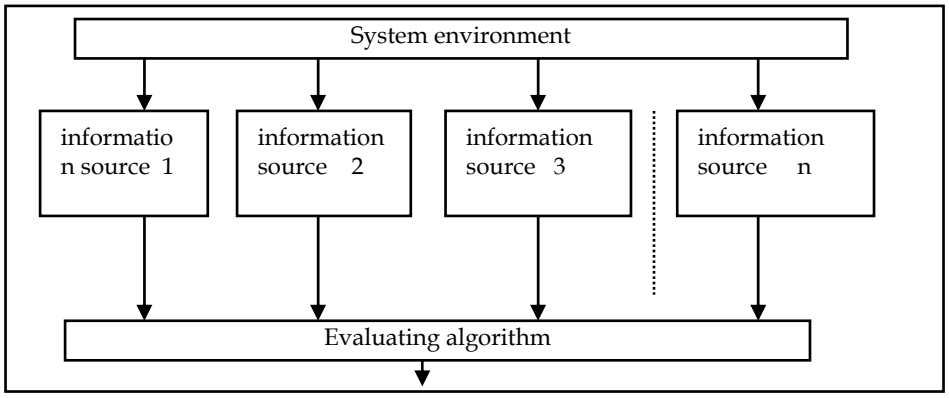


Fig. 10. The simple majority system (Capek 2001)

The evaluating algorithm works too simply. The problem gives the nearest output signals i.e. if all the values of signals are different and only one is good. Better results are given by following major systems with average evaluation algorithm; see Fig. 11.
If we denote b as the average of immediate outputs of a set of information sources, we obtain:

$$b = \frac{1}{n}\sum_{i=1}^{n} o_i \tag{5}$$

The wrong information source is recognized from the following differences:

$$\Delta 1 = \left| o1 - b \right| ; \Delta 2 = \left| o2 - b \right| ; \ \ldots . \ \Delta n = \left| on - b \right| \tag{6}$$

Example: Again it is supposed that the minimal number of information sources, i.e. three information sources will be used. If $\Delta 1 \neq \Delta 2 \neq \Delta 3$ and alongside with this fact $\left| \Delta 2 - \Delta 3 \right| = \varphi$ holds true, where φ denote permit error, the information source No 1 is faulty and its information is untrustworthy. For the set of information sources we can make such transformation that we try to transform signals from the information sources into trustworthy information and denoting the possible wrong information source we can transfer the set of information sources into safety systems.

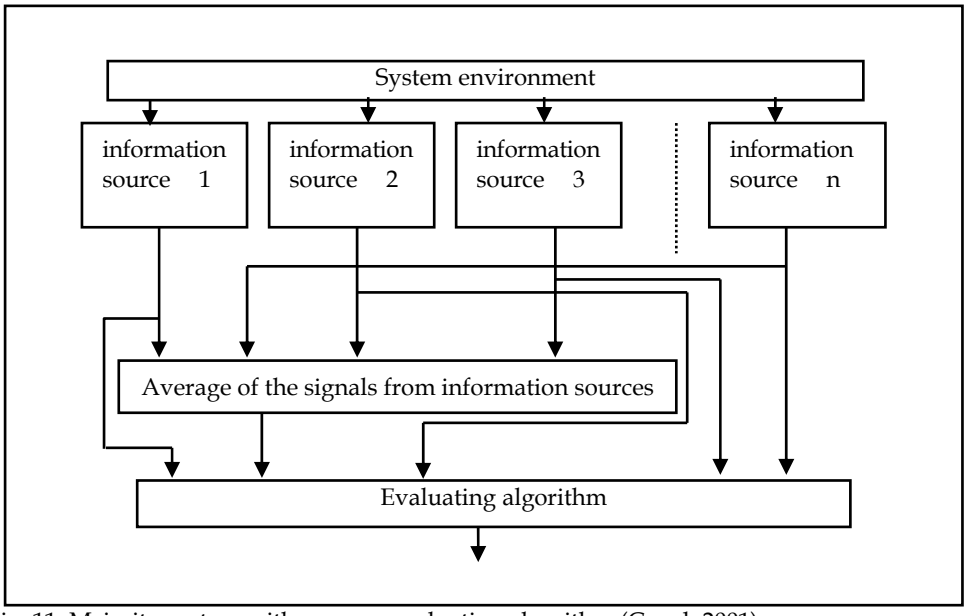


Fig. 11. Majority system with average evaluation algorithm (Capek 2001)

For a set of information sources we can make such a transformation that we try to transform signals from the information sources into trustworthy information and denoting the possible wrong information source we can transfer the set of information sources into safety systems. (Bariova & Tomasov 2001).

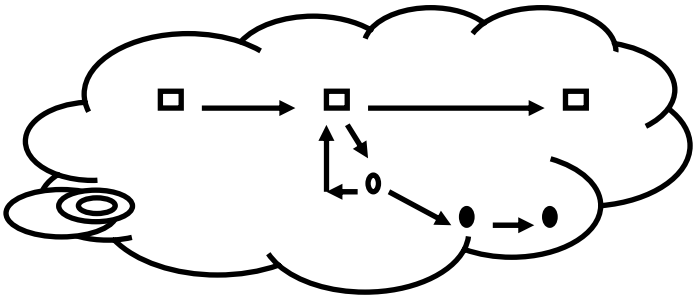


Fig. 12. The selection of an appropriate status set of information sources by (Bariova & Tomasov 2001).

In Figure 12 the dot ● denotes dangerous failure state, ○ denotes safe failure state (only two information sources are in good conditions). The state of information source system now is changed from the safe failure state (2 information sources are good) into the dangerous failure system. (At least one information source is good). If the information sources system is in the safe failure state or dangerous failure state, it is necessary to replace the malfunctioned information sources and bring the information sources system into the regular state. This replacing procedure has difference in time based on the state of information source system. If the system has safe failure state the replacing procedure should be as soon as possible, in the other case must be immediately done. This situation was modelled by Petri nets.

3.2 Modeling by Petri nets.

A gentle introduction into Petri net modelling approach is made for example by WoPeD (WoPeD 2005) where Petri nets are described as follows: "**Petri Nets** are a graphical and mathematical modelling notation first introduced by Carl Adam Petri's dissertation published in 1962 at the Technical University Darmstadt (Germany). A Petri Net consists of **places**, **transitions**, and **arcs** that connect them. Places are drawn as circles, transitions as rectangles and arcs as arrows. Input arcs connect places with transitions, output arcs connect transitions with places. Places are passive components and are modelling the system state. They can contain **tokens**, depicted as black dots. The current state of the Petri Net (also called the **marking**) is given by the number of tokens on each place. Transitions are active components modelling activities which can **occur** and cause a change of the state by a new assignment of tokens to places. Transitions are only allowed to occur if they are **enabled**, which means that there is at least one token on each input place. By occurring, the transition removes a token from each input place and adds a token on each output place. Due to their graphical nature, Petri Nets can be used as a visualization technique like flow charts or block diagrams but with much more scope on concurrency aspects. As a strict mathematical notation, it is possible to apply formal concepts like linear algebraic equations or probability theory for investigating the behaviour of the modelled system. A large number of software tools were developed to apply these techniques, a comprehensive overview can be found in the Petri Net tools database." The model from Figure 12 rewritten into the HPSim

environment is on the following Fig. 13. The HPSim environment was chosen due to its being easy to use and its simplicity.

4. Results

The simulation results from simplification done by a Petri Net show how information source working state is changed from failure-less state (correct working state) to failure state (incorrect working state). The failure state (incorrect working state) was divided into safe failure state (restoration - able working state) and dangerous failure state (restoration - unable state or incorrect working state). Comparison of the division into two failure states (safe and dangerous failure state) in Table 2 given by probabilities is expressed by percents from proportion 10/90 % of the dangerous failure state to safe failure state to 90/10 % of the same proportion. The row "Safe failure state -1"shows increasing number of reconfigured information sources. The row "Regular state" shows decreasing number of information sources with dependence of dangerous failure state. The dangerous failure state can be calculated as supplement to Safe failure state -1. This simple simulation procedure shows the decomposition of the safe failure and dangerous failure working state of information sources with dependency on the probability of the reconfiguration possibilities.

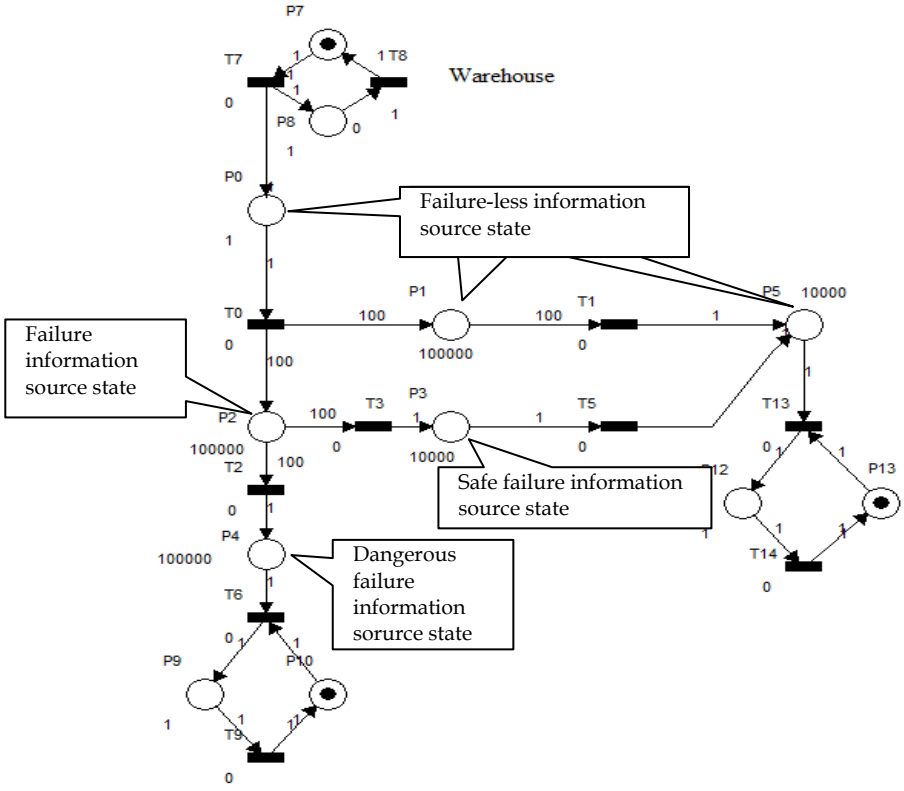
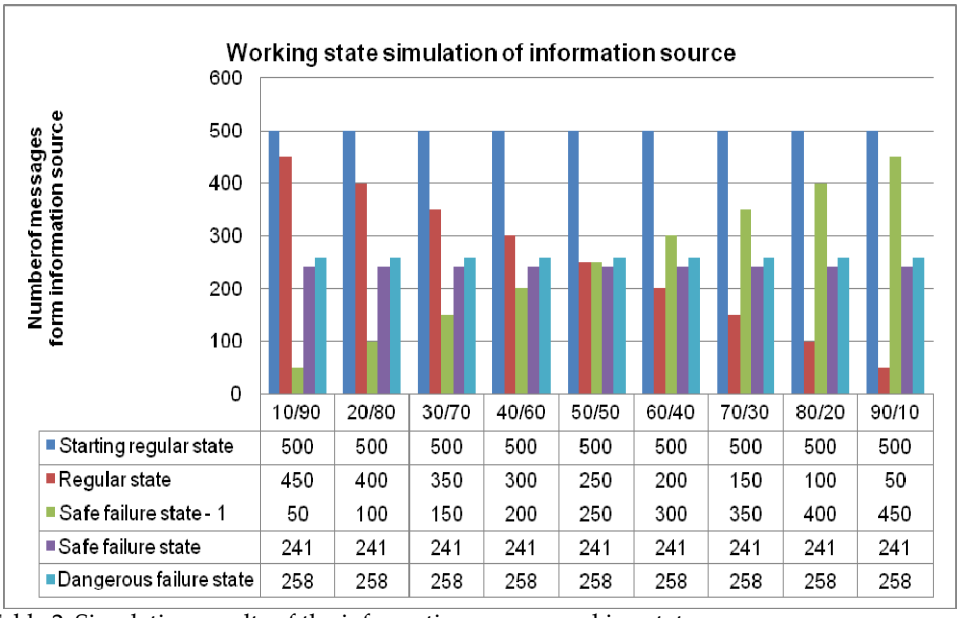


Fig. 13. Petri net model of information source working state

5. Conclusion

Recently, "new economy" exposed the growing importance of non-tangible assets that are at the heart of business processes. Dependability of e-information sources with data carrying information and/or knowledge certainly play a special role here. The dependability of the information sources is more complex problem than Avizenis et al. (Avizenis et al., 2001, 2004) showed. It is necessary to include risk dimensions into this scheme, because many damages of the information systems are due to hackers and intruders on the one, Internet side, and own employees on the other side. The modified dependability tree is in Figure 7. E-information sources based on the computing systems are characterized by five fundamental properties: functionality, usability, performance, cost, and dependability. Dependability of a computing system is the ability to deliver service that can justifiably be trusted. The service delivered by a system is its behaviour as it is perceived by its user(s); a user is another system (physical, human) that interacts with the former at the service interface. The function of a system is what the system is intended to do, and is described by a functional specification. Correct service is delivered when the service implements the system function. A system failure is an event that occurs when the delivered service deviates from correct service. The idea of the division system failure to safe failure and dangerous failure leads to better understanding the reconfiguration possibilities of the information sources. Dangerous failures are unreconfigurable. In other words a failure is a transition from correct service to incorrect service, i.e., to not implementing the system function. The delivery of incorrect service is a system outage. A transition from incorrect service (from safe failure state, only) to correct service is service restoration. The paper showed that the working states of the e-information source are possible to be modelled by Petri Nets, for better understanding of transition between situations from the service point of view.



	10/90	20/80	30/70	40/60	50/50	60/40	70/30	80/20	90/10
Starting regular state	500	500	500	500	500	500	500	500	500
Regular state	450	400	350	300	250	200	150	100	50
Safe failure state - 1	50	100	150	200	250	300	350	400	450
Safe failure state	241	241	241	241	241	241	241	241	241
Dangerous failure state	258	258	258	258	258	258	258	258	258

Table 2. Simulation results of the information source working state

6. References

Avizienis A, Randell B. Laprie J.C (2001). Fundamental Concepts of Dependability. *Technical report, LAAS - NewCastle University - UCLA, 2001*. LAAS Report no. 01-145, NewCastle University Report no. CS-TR-739, UCLA CSD Report no. 010028

Avizienis,A,. Laprie J.-C,. Randell B, and. Landwehr C, (2004) Basic Concepts and Taxonomy of Dependable and Secure Computing, *IEEE Transactions on Dependable and Secure Computing*, vol. 1, pp. 11-33, 2004.

Bariova H.,Tomasov,P. (2001). The safe systems identification by Information theory exploitation. *TRANSCOM 2001* Zilina Slovakia 2001

Bass T. (2000) Intrusion detection systems and multisensor data fusion, *Communications of the ACM* 43 (4) (2000) 99–105, ISSN 0004-5411

Byström, K (1999) Task Complexity, Information Types and Information Sources: Examination of Relationships, University of Tampere, Faculty of Social Sciences, Tampere Finland

Byström, K. (1997) Municipal administrators at work – Information needs and seeking (IN&S) in relation to task complexity: A case-study amongst municipal officials. In Vakkari & Savolainen & Dervin (eds) *Information Seeking in Context*. London: Taylor Graham, 125–146.

Byström, K. (1996) The use of external and internal information sources in relation to task complexity in a journalistic setting. In Ingwersen & Pors (eds) *Information Science: Integration in Perspective*. Copenhagen: The Royal School of Librarianship, 325–341.

Byström, K. (1997) Municipal administrators at work – Information needs and seeking (IN&S) in relation to task complexity: A case-study amongst municipal officials. In Vakkari & Savolainen & Dervin (eds) *Information Seeking in Context*. London: Taylor Graham, 125–146.

Byström, K. (forthcoming) Information seekers in context: An analysis of the "doer" in INSU studies.In .*Proceedings of the 2nd international conference on research in information needs, seeking and use in different contexts*, 13–15 August 1998, Sheffield, UK.

Byström, K. & Järvelin, K. (1995) Task complexity affects information seeking and use. *Information Processing & Management*, 31(2), 191–213.

Capek J.(2008) Dependability and security of the information systems . In. *19th International DAAAM Symposium "Intelligent Manufacturing & Automation. Focus on Next Generation of Intelligent Systems and Solutions*", pp. 1-2, (2008), ISSN 1726-9679.

Capek J (2001) Trustworthy Information from system of sensors., In. *The 12th INTERNATIONAL DAAAM SYMPOSIUM "Intelligent Manufacturing & Automation: Focus on Precision Engineering"* 24-27th October 2001

Corona I. at all (2009) Corona, I., Giacinto G., Mazzariello C., Roli F., Sansone C., *Information fusion for computer security: State of the art and open issues* Information Fusion 10 (2009) *274–284* ***ISSN: 1566-2535***

Contini at all (200) Contini, S., Bellezza, F., Christou, M.D.,and Kirchsteiger, C. The use of geographic information systems in major accident risk assessment and management. Journal of Hazardous Materials 78, 1-3, (November 2000), 223-245.

Fielding, R.T., and Taylor, R.N. 2002. Principled design of the modern Web architecture. ACM Transactions on Internet Technology 2 (May 2002), 115-150.

Järvelin, K (1986) On information, information technology and the development of society: An information science perspective. In Ingwersen & Kajberg & Mark Pejtersen (eds) *Information Technology and Information Use: Towards a Unified View of Information and Information Technology*. London: Taylor Graham, 35–55.

Krekora P. & Caban D.(2007) Dependability analysis of reconfigurable information systems. In: *Proceedings of the 2nd International Conference on Dependability of Computer Systems, 2007*. DepCoS-RELCOMEX '07. Sklarska Poreba, Poland 14-16 June 2007 ISBN: 0-7695-2850-3
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?reload=true&punumber=4272875

Laprie, J.C..(1985) "Dependable Computing and Fault Tolerance: Concepts and terminology," in *Proc. 15th IEEE Int. Symp. on Fault-Tolerant Computing*, 1985

Maximilien, E.M., and Singh, M.P. (2004). Toward autonomic web services trust and selection. In Proceedings of the 2nd international conference on Service oriented computing, (New York, NY, USA, November 15 – 19, 2004). ACM Press, New York, NY, 212 – 221. DOI= http://doi.acm.org/10.1145/1035167.1035198.

MSDN.NET (2009) Getting Started: MSDN.NET Framework Developer Center. 2009. [online]. URL=http://msdn2.microsoft.com/en-us/netframework/aa569294.aspx.

O'Connor (1988). Reliability Engineering. Hemisphere publishing corp. London 1988

Randell, B (1995) Software Dependability: A Personal View, in the Proc of the 25th International Symposium on Fault-Tolerant Computing (FTCS-25), California, USA, pp 35-41, June 1995.

Pautasso, C., and Wilde, E. 2009. Why is the web loosely coupled?: a multi-faceted metric for service design. In Proceedings of the 18th international conference on World wide web (Madrid, Spain, April 20 – 24, 2009). ACM Press, New York, NY, 911-920. DOI=http://doi.acm.org/10.1145/1526709.1526832

Puustjärvi J. (2009) Ensuring Recoverability in Composing Web Services. In. *Proceedings of the*
iiWAS2009, December 14-16, 2009, Kuala Lumpur, Malaysia, pp517-526, ISBN 978-1-60558-660-1

Samtani, G., and Sadhwani, D. 2004. Web Services Monitoring and Performance Management. *Web Services Journal 2*, 10 (2004), [online]. URL=http://www2.sys-con.com/ITSG/virtualcd/WebServices/archives/0210/sadwami/index.html.

Shirky, C. (2002) Planning for Web Services: Obstacles and Opportunities. O'Reilly & Associates, ISBN 0-596-00364-1

Schewe K,D. & Thalheim B. (2009) Pragmatics of Storyboarding – Web Information Systems Portfolios.In. *Proceedings of iiWAS 2009* Kuala Lumpur, Malaysia ISBN 978-1-60558-660-1

SPI (2007) Software protection initiative. http://www.spi.dod.mil/index.htm

Wiki (2010) http://en.wikipedia.org/wiki/Dependability

WoPeD (2005) http://193.196.7.195:8080/woped/PetriNets

Zio E., (2009) Reliability engineering: Old problems and new challenges. *Reliability Engineering and System Safety* 94 (2009) 125– 141, ISSN 0951-8320

Engineering the Future
Edited by Laszlo Dudas

ISBN 978-953-307-210-4
Hard cover, 414 pages
Publisher Sciyo
Published online 02, November, 2010
Published in print edition November, 2010

This book pilots the reader into the future. The first three chapters introduce new materials and material processing methods. Then five chapters present innovative new design directions and solutions. The main section of the book contains ten chapters organized around problems and methods of manufacturing and technology, from cutting process optimisation through maintenance and control to the Digital Factory. The last two chapters deal with information and energy, as the foundations of a prospering economy.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Jan Capek (2010). Dependability of E-Information Sources, Engineering the Future, Laszlo Dudas (Ed.), ISBN: 978-953-307-210-4, InTech, Available from: http://www.intechopen.com/books/engineering-the-future/-dependability-of-e-information-sources

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821