Hands on Dependability Economics

Theodosios Tsiakis
Department of Informatics
Aristotle University of Thessaloniki
Thessaloniki, Greece
tsiakis@uom.gr

Panagiotis Katsaros
Department of Informatics
Aristotle University of Thessaloniki
Thessaloniki, Greece
katsaros@csd.auth.gr

***Abstract*—Contemporary societies (from individuals to organizations) depend on services delivered by systems to achieve individual goals, meaning that a system must have engineered and guaranteed dependability, regardless of continuous, rapid and unpredictable technological and context changes. The simplest questions that brought out in the surface are to understand on how to evaluate and how much (money) should we spend on dependability. Dependability risk management is an effective process that with simplicity can determine the likelihood of an accident and the severities of the consequences. On the other hand, we also need quantitative methods, in order to assess the cost of the various measures which can be taken to reduce the dependability risk. In this paper, we survey quantitative methods that can play an important role in Dependability Economics. These methods aim in providing estimations for the economic consequences of lowering dependability levels and the costs to implement dependability.**

Keywords-Dependability;Risk;Qualitative;Quantitative Analysis, Economics

I. INTRODUCTION

In the past, the use of highly-dependable, fault-tolerant computing systems has been limited to industries that had the mission priority and the financial – economic support to afford their considerable costs [1]. Today, the picture has changed. Many systems in different application domains need to be dependable. Adequate dependability is a key requirement for many different systems, such as safety-critical systems, telecommunication systems, and mission-critical software systems [2].

In current article, we treat dependability as a measure of system trustworthiness defined in the context of the stakeholders' economic needs. The generic motivation for the research presented in this paper can be identified by the following directions

- How can dependability be measured and evaluated
- How can we balance the economic consequences of lowering dependability levels and the costs to implement dependability

Section 2 reviews the considered scope of dependability as a property that characterizes a system's runtime behaviour. We also examine the particular aspects that affect the economics of dependability. Section 3 introduces a risk-based perspective of dependability and section 4 presents the risk-driven economic analysis perspectives that motivate the proposed treatment of dependability. Last section summarizes the conclusions of the present article and comments on the identified future research prospects.

II. THE ECONOMIC PARAMETERS OF DEPENDABILITY

Following the principles proposed in [3] in order to be able to understand and ensure dependability, we must study:

a) the threats that can lead us to a situation in which the system in not dependable,
b) the attributes that we want to maintain in the system, and
c) the means we can adopt to ensure overall dependability.

In our view, dependability is defined as the trustworthiness of a computing system that allows reliance to be justifiably placed on the services it delivers. Dependability is a system property that imbricates a plethora runtime behavior aspects including:

- Availability
- Reliability
- Safety
- Security (including Confidentiality and Integrity)
- Performance
- Survivability
- Maintainability

Dependable systems implement the required means to

1. detect sources of non-dependable performance
2. isolate and contain them and
3. recover, while still maintaining a high level of service.

Dependability can be accomplished by a wide spectrum of approaches that are generally grouped into the following categories:

1. Fault prevention, i.e. methods preventing the occurrence or introduction of faults
2. Fault tolerance, i.e. methods providing service compliance with the service specification, even under the presence of faults
3. Fault removal, i.e. methods that reduce the presence of faults, in terms of the number and the seriousness encountered in the system's behaviour.
4. Fault forecasting, i.e. the methods used in estimating the present number, the future incidence and the consequences of fault modes.

Measuring dependability quantitatively is a research field of great importance, due to the versatile nature of dependability as a system property bound on the actual system context. Reference [4] stated that quantitative evaluation aids in the analysis of the system behaviour in the presence of faults and provides estimations for the system parameters that provide a higher trustworthiness. But what is needed is to have in mind that dependability is contextually subjective and reflects the particular stakeholders needs [5].

As [6] prophetically observed the focus of security engineering has shifted from what is technically possible to what is economically optimal. Looking ahead to the future, we need to address the economic aspects of dependability and this prospect is justified by the fact that economic analysis often explains technological failure better than technical analysis. The majority of proposals for introducing dependability from an economic perspective (Dependability Economics or Economics of Dependability) address the following:

- The additional design, implementation, and validation effort that is required for dependable systems, increases the overall development cost
- More expensive development techniques and hardware are required to achieve higher levels of reliability
- Increased testing and validation are required to convince users that higher levels of dependability have been achieved
- The costs of system failure may be much higher than the system development costs
- The cost versus dependability curve is exponential, so it is impossible to achieve 100% dependability *"Fig. 1"*

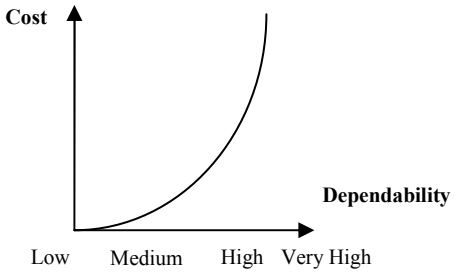

Figure 1. Cost vs Dependability.

The simplest questions now that brought out in the surface are to understand on how to evaluate and how much (money) should we spend on dependability? The generic motivation for the research presented in this paper can be identified by the following directions

- How can dependability be measured and evaluated
- How can we balance the economic consequences of lowering dependability levels and the costs to implement dependability

III. DEPENDABILITY RISK MODELLING

Risk has been studied from many perspectives. Reference [**7**] studied risk in a detailed theoretical analysis of the anatomy of risk and risk and uncertainty in the context of the value of information. Risk for example in e-commerce transactions is the danger of a negative outcome. From the customer's perspective, it is paying for goods and either getting unexpected goods or getting nothing. In merchant's point of view, risk is to provide the goods and getting no payment. As risk implies a potential loss, there are two elements at issue here: firstly the probability of an unsatisfactory outcome and secondly the consequences of such an outcome [8].

Risk = probability (of an unsatisfactory outcome) * loss (to the parties affected if the outcome is unsatisfactory)

Under the dependability umbrella risk with simplicity could be defined as the mixture of the likelihood of an accident and the severity of the potential consequences. Mathematically ditto Risk is equal to the Probability of failure multiplied by Severity. The failure condition refers to a combination of failures modes applied to functions of the system under study [9].

Reference [10] acknowledge that every risk has a cost, and that cost can be (more or less precisely) quantified. The cost of a particular risk during a period of time is the probability of an adverse event occurring during the time period multiplied by the downside consequence of the adverse event. The interrelationship between risk and cost is shown in *"Fig. 2"*) where risk is denoted by *R* and cost by *C*. If we decrease risk *R* from R_1 to R_2 the cost *C* will decrease from C_1 to C_2. Is now apprehensible that *C* is positively influenced by *R* (downward movement from point *A* to point *B* shows this).

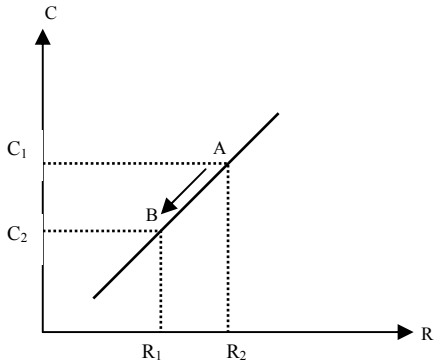

Figure 2. Correlating cost and risk.

Conceptualizing that the risk is mentioned in a business context, the probability of an event occurring is a number between zero and one, with zero representing an event which will definitely not occur and one representing an event which definitely will occur. The consequence of an event is the worth of the amount of the reduction in business value which the event will cause if it occurs. Attributing this in a form of equation [11]:

Risk = probability (failure) * consequence (failure)

Risk needs to be further assessed in terms of the probability of the events and the subsequent financial impact on the organization. A simple matrix commonly used for insurance decisions can be developed to classify the sources of risk as in Table 1 below.

Probability / Impact	Low	High
Low	I Ignore	II Contain and control
High	III Insure and /or have Backup Plan	IV Avoid / Prevent

TABLE I. PROBABILITY VS. IMPACT

A. Risk Analysis

[12] The concept of analysis is usually understood to be a three-stage process, namely:

1. taking apart the thing to be understood;
2. trying to understand the behaviour of the parts taken separately; and
3. trying to assemble this understanding into an understanding of the whole.

The risk analysis process is a very common activity. The goal of risk analysis is usually to find vulnerabilities so that they can be patched [13]. A review of the literature suggests that the process of risk analysis is usually broken down into three stages [12]:

1. risk identification;
2. risk estimation; and
3. risk evaluation.

This analysis should identify the unique risks related to the dependability system, suitable controls that address these risks, and the inter-relationships between these controls [14].

Risk analysis is a systematic process used firstly to identify, secondly to estimate and thirdly to evaluate the risks [15], apprehend that the analysis of risks is performed in four stages:

1. Asset identification and valuation
2. Threat identification and assessment
3. Vulnerability assessment
4. Risk assessment

Nevertheless the steps might be involved in a risk analysis framework, risk analysis enables to apprize the importance of the value of assets to be secured in a cost effective manner. We look it as three stages process (*"Fig. 3"*)

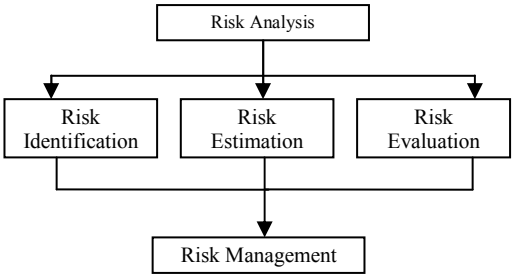

Figure 3. Risk Analysis Process.

Risk analysis has been proposed as a solution for prioritizing failures by analyzing their likelihood and effects [16] [17], [18].

B. Risk Management

Risk management strategies are oriented towards identifying different types of risks, assessing their relative importance for the project, and implementing strategies for managing risk [7].

Reference [19] divides risk management into the following key components:

1. assets,
2. threats, vulnerabilities and risks,
3. safeguards,
4. economic analysis and
5. reiterative processes.

Similarly [20] looks at risk management as an essential practice consisting of the following processes:

1. establish the context;
2. identify risks;
3. analyse risks;
4. evaluate risks;
5. treat risks;
6. monitor and review; and
7. communicate and consult.

According to [21], [22] the first step in a typical risk management programme is the *identification* of risk, the next step is the *analysis* of the risks and the final step is risk *monitoring*.

But the design of the risk management process has been based on an analysis of the existing risk approaches and the contingency approaches, sometimes called situational approaches [23]. Risk management actions can be viewed as being of two types [7]:

1. The first is oriented towards reducing the degree of risk
2. since risk cannot be completely eliminated the second type is insurance measures in order to minimize the negative impact of risk

It is well established that risk is an inescapable fact and there are only four things we can do about it: accept it; ignore it (which is the same as accepting it); assign it to someone else; or mitigate it [24].

IV. RISK AND ECONOMICS

Reference [16] mention that in order to deploy dependable systems, designers need to detect and remove errors and limit damage caused by failures. Risk management benefits come from two types of savings [25]:

a) Cost avoidance - is the difference between possible cost without risk resolution and the actual cost with risk resolution.
b) Cost reduction - is the difference between planned and actual costs.

From the moment that the probability of a hazardous event has been assessed, the cost of the various measures which can be taken to reduce that risk is inevitably considered [26]. Therefore two approaches are taken into consideration, Quantitative and Qualitative analysis. Quantitative and Qualitative analysis are both seeking to minimize the occurrence of systematic failures.

A. Quantitative Risk Analysis

Quantitative risk analysis aspires to cede precise numeric monetary values to assets. It designates the financial risk of threats impact and frequency, costs of control and loss.

One simply method for calculation of risk exposure is to multiply the projected cost of a dependability failure (Single Loss Exposure, or SLE) with its estimated annual rate of occurrence (ARO). The result is called the Annual Loss Exposure (ALE) [27] [28].

Annual Loss Expectancy (ALE) can be defined as the cost (loss in monetary units) of the damage resulted by a failure, multiplied by its frequency in a period of one (1) year. The calculation of ALE is simply the multiplication of the cost of any potential failure by the times the risk will occur (1).

$$ALE = SLE * ARO \quad (1)$$

Where (ARO) is Annual Rate of Occurrence meaning the probability that a risk will occur in this particular period of one year

And Where (SLE) is the Single Loss Expectancy that means the expected cost (loss in monetary units as we mention it before) every time a risk occurs. Single Loss Expectancy is calculated multiplying Asset Value (AV) by exposure factor (EF) showing in following formula (2):

$$SLE = AV * EF \quad (2)$$

B. Qualitative Risk Analysis

There are cases in which monetary values appointed by quantitative analysis cannot be assigned to risk elements. In such cases, qualitative risk analysis can be used to approach risk assessment and rank severity of threats by using classes such as low, medium and high of probabilities and damages.

C. The case of Return on Investment (ROI)

Return On Investment (ROI) is based on the evaluation of the Annual Loss Expectancy (ALE) [29] Return on Investment is the actual measure of financial performance because it focuses on the combination of the three principle factors that affect profit: sales, costs, and total assets. For the calculation of ROI, the cost of dependability implementation is weighed against the expected returns over the life of the item [30].

$$ROI = \frac{\text{Expected Returns - Cost of Investment}}{\text{Cost of Investment}}$$

Based on the financial benefits and costs of that investment ROI is expressed as the net gain divided by the investment. In the simplest of terms [31]:

(what I gained totally) − (what I invested) / (what I invested)

V. CONCLUSIONS

Economic value attribution and particularly over adequate quantitative measures of dependability is a challenging prospect. In the dependability literature it is generally difficult to perceive general quantitative evaluation methods of the overall system dependability, that as we pointed out it is contextually subjective and reflects the particular stakeholders' needs. The majority of the published works refer to the general framework of risk management. We stand forward to illustrate that dependability is relative economic measure of dependability attribute risk factors [32] since failures result to economic losses. In current work, we indicate the risk process that can be followed from the literature perspective and we address the economic quantitative models and methods that could simply assign monetary values to dependability and so to measure it.

In the future we both want and need to extend our research focus on defining dependability risk analysis assessment, dependability risk factors that could address them with certain monetary values and new quantitative methods and models.

REFERENCES

[1] A. Cox, K. Mohanram, and S. Rixner, "Dependable # Unaffordable", Proc. of the ASID'06, 2006 pp. 58–62.

[2] M. Jiang, and Z. Yang, "A Model-Driven Approach for Dependable Software Systems," Proc. of the Seventh International Conference on Quality Software (QSIC 2007), 2007, pp. 100–106.

[3] L. Baresi, S. Guinea, and M. Plebani, "Business Process Monitoring for Dependability," Architecting Dependable Systems IV, LNCS 4615, 2007, pp. 337–361.

[4] G. Chaparro-Baquero, N. Santiago, W. Rivera, F. Vega-Riveros, "Measuring quantitative dependability attributes in Digital Publishing using Petri Net Workflow Modeling," Proc. of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, 2006, pp. 119–128.

[5] P. Donzelli, and V. Basili, "A practical framework for eliciting and modeling system dependability requirements: Experience from the NASA high dependability computing project" The Journal of Systems and Software vol. 79, 2006, pp. 107–119.

[6] R. Thieme, "What Insurance Can – and Can't – Do for Security Risks," Secure Business Quarterly: Defining the Value of Strategic Security, 4th Quarter, vol. 1, iss. 2, 2001, pp. 1–7.

[7] R. Kumar, "Managing risks in IT projects: an options perspective," Information & Management vol. 40, Issue 1, 2002, pp. 63–74.

[8] A. Gemmer, "Risk Management: Moving Beyond Process," IEEE Computer vol. 30, 1997, pp. 33–43.

[9] P. Bieber, J. Blanquart, G. Durrieu, D. Lesens, J. Lucotte, F. Tardy, M. Turin, C. Seguin, E. Conquet, "Integration of formal fault analysis in ASSERT: Case studies and lessons learnt," Proc. of the International Conference : ERTS EMBEDDED REAL TIME SOFTWARE, 2008.

[10] B. Blakley, E. McDermott, D. Geer, "Information security is information risk management," proc. of the 2001 workshop on New security paradigms, New Security Paradigms Workshop, 2001, pp. 97–104.

[11] R. Chellappa and P. Pavlou, "Perceived information security, financial liability and consumer trust in electronic commerce transactions," Logistics Information Management vol. 15, 2002, pp. 358–368.

[12] D. White, "Application of systems thinking to risk management: a review of the literature," Management Decision, vol. 33 No. 10, 1995, pp. 35–45.

[13] A. Stewart, "On risk: perception and direction," Computers & Security, vol. 23, 2004, pp. 362–370.

[14] M. Gerber, and R. von Solms, "Management of risk in the information age," Computers & Security vol. 24, 2005. pp. 16–30.

[15] E. Loukis and D. Spinellis, "Information Systems Security in the Greek Public Sector," Information Management and Computer Security, vol. 9, 2001, pp. 21–31.

[16] Y. Asnar, P. Giorgini, F. Massacci, and N. Zannone, "From Trust to Dependability through Risk," Technical Report DIT-06-079, Informatica e Telecomunicazioni, University of Trento, 2006.

[17] A. Ponnam, B. Harrison, and E. Watson, "An Audit and Control Control Approach," Handbook of research on information security and assurance, chapter on Information Systems Risk Management, 2009 IGI Publications.

[18] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, "Security Ontologies- Improving Quantitative Risk Analysis," proc of the 40th Hawaii International Conference on System Sciences, 2007, pp. 156a.

[19] M. Myerson, "Risk Management Processes for Software Engineering Models," Artech House Publishers, Boston,MA, 1997.

[20] D. Baccarini, G. Salm, and P. Love, "Management of risks in IT projects," Industrial Management & Data Systems, vol. 104, 2004, pp. 286–295.

[21] K. Padayachee, "An interpretive study of software risk management perspectives," proc. of the ACM International Conference of the 2002 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology, 2002, pp. 118–127.

[22] L. Tchankova, "Risk identification – basic stage in risk management," Environmental Management and Health, vol. 13, 2002, pp. 290–297.

[23] D. Verhoef, and M. Franckson, "Risk Management for IT in the Large," proc. of the 11th International Conference on Advanced Information Systems Engineering CAiSE'99, 1999, pp. 57–72.

[24] D. Brink, "A Guide to Determining Return on Investment for e-Security," RSA Security Inc., 2001.

[25] E. Hall, "Risk Management Return on Investment," Journal of the International Council on Systems Engineering, vol. 3, 1999, pp. 1770–1800.

[26] D. Smith, Reliability, Maintainability and Risk, Elsevier, 2005.

[27] S. Bistarelli, F. Fioravanti, P. Peretti, "'Defense trees for economic evaluation of security investments," proc. of the First International Conference on Availability, Reliability and Security (ARES'06), 2006, pp. 416–423.

[28] C. Lin, W. Yu, and K. Lin, "Apply Cost-Benefit Analysis Methods to Information Security Assets in Taiwanese Local Government - An Initial Study," proc. of the 13th Asia Pacific Management Conference, Melbourne Australia, 2007, pp. 1076–1080.

[29] M. Cremonini, and P. Martini, "Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)," proc. of the 4th Workshop on the Economics on Information Security, 2005.

[30] W. Sonnenreich, J. Albanese, and B. Stout, "Return On Security Investment (ROSI) - A Practical Quantitative Modell," Journal of Research and Practice in Information Technology 38, 2006, pp. 207–220.

[31] Purser "Improving the ROI of the security management process" Computers & Security vol. 23, 2004, pp. 542–546.

[32] D. Port, and L. Huang, "Software Dependability Risks and the Insurance Process," The Fifth International Workshop on Economics-Driven Software Engineering Research (EDSER-5), 2003, pp. 66–70.