Reliability and Security - Convergence or Divergence

Emil BURTESCU
Department of Accountancy and Management Informatics
Faculty of Economics, University of Pitesti, Pitesti, Romania
emil.burtescu@upit.ro

Reliability, as every technical field, must adapt to the new demands imposed by reality. Started initially as a field designed to control and ensure the smooth functionality of an element or technical system, reliability has reached the stage where the discussion is about the reliability management, similar to the other top-level fields. Security has its own contribution to the reliability of a system; a reliable system is a system with reliable security. In order for a system to be reliable, that means clear and safe, all its components must be reliable. In the following pages we will talk about the two main facts - reliability and security - to determine both the convergence and the divergence points.
Keywords: *Reliability, Security, Failure, Threat, Redundancy, Costs, Investment*

1 Reliability and Security

The notion of reliability is quite old, having mostly links with the technical field, this one gaining lately interdisciplinary values.

In all the definitions of reliability there are direct or indirect references to security, this one being defined as: safety, trust, authenticity, accuracy, endurance, strength, solidity. In French, where the word reliability comes from, safety in functioning is defined as being the capacity of an entity to satisfy one or more necessary functions in specific conditions, functioning safety having as components the reliability, availability, maintainability and security.

Reliability is the probability of the parts, components, products or systems to accomplish their functions which they were designed for without collapsing, in certain conditions, for a certain period of time and with a certain level of trust.

In a qualitative approach, reliability represents the capacity of a system to accomplish the specified functioning demands, in environmental and demanding conditions, in a defined functioning, and in a preset period of time.

In a quantitative approach, reliability represents the probability of the system to accomplish the functions which it was designed for, with a certain performance and with no flaws, in a certain period of time and in given functioning conditions.

As we can see in the previous facts, the basic key element of the discussion is **failure**, understanding from it a functioning outside the parameters of a system [9] (Figure 1).

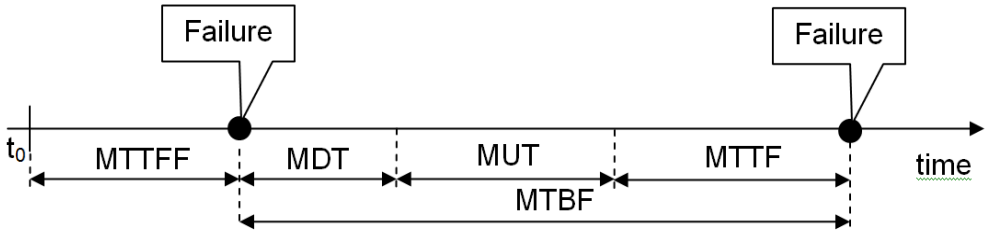

Fig. 1. Some reliability characteristics

MTTF – Mean Time To First Failures, MDT – Mean Down Time, MUT –Mean Up Time, MTTF – Mean Time To Failure, MTBF – Mean Time Between Failures

Reliability can be quantified as being a probabilistic function that has as parameters the components of a system and time:

R(t) = P(T > t) for **t ≥ 0**, where: R – reliability; t – time; T- the functioning time in the established conditions.
For an optimal reliability level to be ensured, different criteria are used, from which the economic one is the most used. Though, this criterion is put on a second plan when lives must be protected.
The evolution of malfunctions in time in a system or in a component of a system is similar to the one in the following figure [8] (Figure 2).

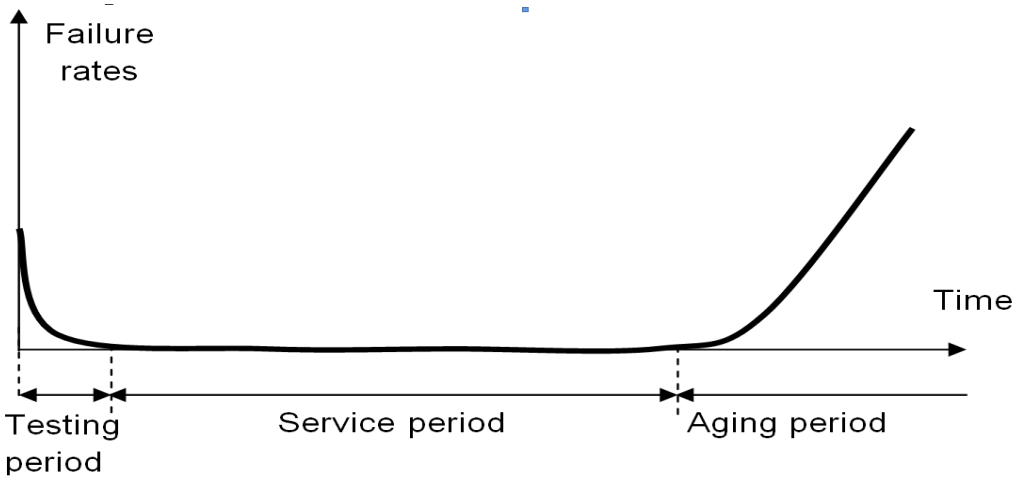

Fig. 2. The evolution of failures reported on time – bathtub curves

Here we have to mention the fact that during the working period, especially regarding the systems made from many components, flaws caused by the malfunction of a certain component may occur. The more complex the system is and the more components the system has, the more the risk of malfunctions may appear.
The testing period is that period in which tests, adjustments and product running-in procedures are made. Here, corrections are made and all the flaws that could occur are fixed. In quite many cases, because of the market pressure this testing period is shortened or is partially transferred to the consumer. This situation can have as result a drastic decrease of reliability, sometimes with major consequences. The service period is that period in which the product accomplishes the duties for which it was made. The aging period is the period defined as being the end of the life of the product. The number of flaws rises significantly and the product is no longer reliable. Locally, many companies ignore this very period, trying to extend the service period with large expenses or with security problems regarding the functioning and not only.
The notion of security is even older, initially having links with the concept of person and finishing with security generally speaking and in our case the informatics security.
Informatics security is defined as being the capacity to protect the data of an organization against unauthorized access or against modifying data in order to ensure availability, confidentiality, integrity and non-repudiation.
Ensuring informatics security will assume the organization to be able to counteract the actions coming from bad-willing entities (espionage, competition) or to reduce the effect of some unpleasant events (natural or human).
For this, the organization will count on a system of specific and well defined measures that will include technology (infrastructure, applications), processes (politics, procedures, standards) and people (training, knowledge, responsibilities, organization) [1] (Figure 3).

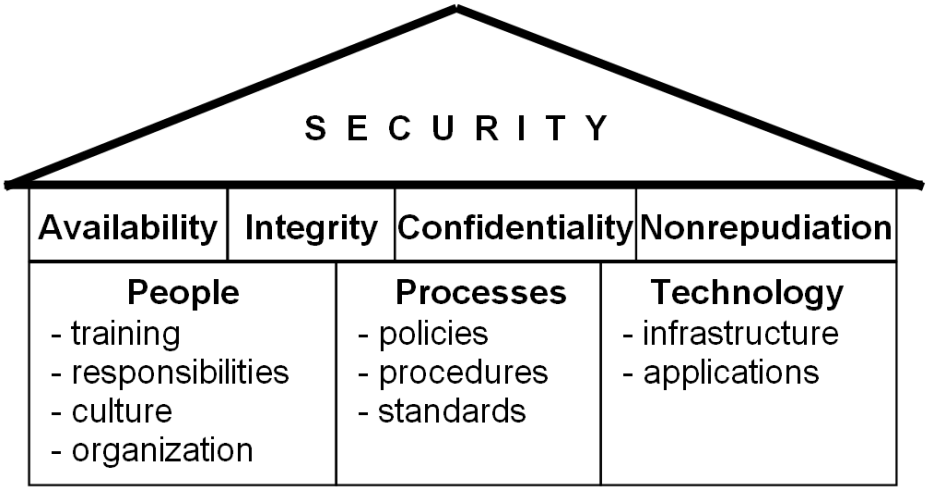

Fig. 3. The security basics

2 Convergences and Divergences

In designing an informatics system, taking into account the previously mentions, a designer must take into consideration the aspects regarding security and reliability.

Next we will detail the interactions between the security of the company and the reliability.

To increase the reliability of a system the first option that is to be used is redundancy. As for the using methods we have spatial and temporal redundancy. Spatial redundancy uses more components that necessary to accomplish a certain duty and the temporal redundancy uses only one device but which makes the same calculus repeatedly and compares the results.

Let's take into discussion the case in which we have a server that must accomplish the functions which it was designed for without flaws, in specified conditions, for a certain period of time and with a given level of trust. In order to work in these conditions, first, the informatics security conditions must be ensured: power supply, adequate environment, a perimeter protected against physical actions, redundant systems in case of malfunctioning of its own components, devices that would stop intrusions etc. These are the security measures. Then we get the conclusion that security is a kind of exterior perimeter of reliability (Figure 4).

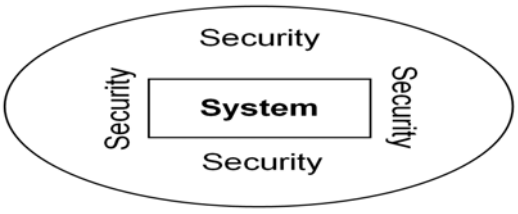

Fig. 4. Links reliability – security

If there is no threat, the system can operate with a minimum security. Now the question arises: in order to be efficient, must not the adopted security measures first be reliable? So, it seems that the two terms are connected. The system must be reliable and it has to provide a reliable security (Figure 5).

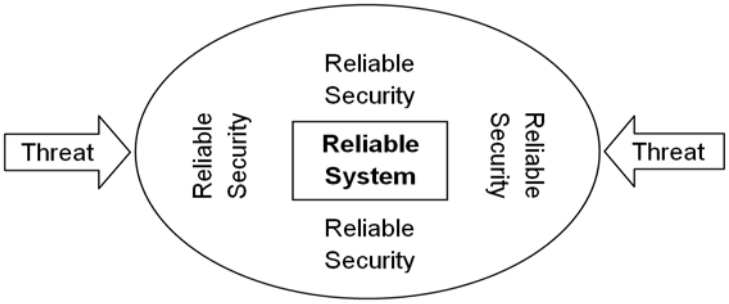

Fig. 5. Links reliability – security. The real world

If we would treat informatics security from the point of view of its components, these two elements might not seem to be connected.

Availability will assume that the data stocked in the computer will be corresponding for access by the authorized persons. This means that the hardware component and software to be reliable. If they are not, then availability is not ensured and so, we have no security.

No Reliability → No Availability → No Security

Let's analyze the case in which the system is reliable but we have no security measures. If no malicious action interferes, the system will work flawless and will deliver the requested information. We have reliability without having security.

Reliability + No Security - Attack → Availability

or

Reliability + No Security + No Attack → Availability

In case a malicious action interferes, then availability may be affected.

Reliability + No Security + Attack→ No Availability

Integrity will assume that all the data stored in the computer can be altered or modified only by authorized persons; a demand that can look quite simple at first sight and that leads us to the thought of security, which is justified if we were to think about unauthorized persons who deliberately intend to alter data. This leads us again to bugs and backdoors which have to be eliminated. But what if the data written on the disk are altered in time because of the media? This obviously leads us to reliability.

Confidentiality will assume denying unauthorized access to private information. This is a simple problem of security: the solution is to design an encryption mechanism. Just that, if this design is being done by applying mechanisms and measures that slow down the system, reliability will suffer. Some tests, unfortunately made by malicious persons showed that any encryption can be broken, so we do have a problem. Is this a problem of reliability? Have we reliability but we have not security anymore? If someone manages to break into a system as a result of breaking the encryption mechanisms and extracts information without the owner noticing it, then we can say that yes, the system is still reliable. But if this intrusion is noticed, then it means the system has lost its reliability because its security isn't assured anymore and there is a possibility that it can be diverted from its specific tasks.

To "read" the competition it is enough to read its data.

Non-repudiation aims to confirm the authenticity of an electronic message. As you can see non-repudiation is involved in the case of electronic transactions. The implementation of a mechanism which confirms the authenticity of an electronic message will assume that it will ensure availability, integrity, confidentiality and of course reliability.

Bringing the system to functioning parameters will assume going through two stages: achieving **reliability** and **security** of the system. In each of these two stages there are three directions to be followed: **hardware**, **software** and **human**.

3 Reliability and Security

Hardware reliability and security

A physical component of a system - hardware component - becomes unreliable in the following cases when:

- Malfunction occurs;
- Event occurs;
- The service period is exceeded.

The occurrence of a malfunction during the service period can have the following causes:
- the existence of a manufacturing flaw;
- functioning in inappropriate environmental conditions;
- functioning in inappropriate technical conditions;
- inappropriate human intervention.

A manufacturing flaw usually appears on cheap components that the systems are equipped with. Another situation occurs on the quality components but on which the testing period has been decreased due to market considerations. In most cases, these manufacturing flaws are critical for the system. It is worth mentioning the case of the company Western Digital which released on the market a hard-disk with the marketing name Caviar and which proved to have manufacturing flaws. After a certain period of time the read-write heads quickly turn back to the track 0, producing a sort of clicking, this being the source of the flaw's name -"The Clicking Caviar".

Functioning in inappropriate environmental conditions will assume that the system is the subject of some efforts that regard the placing environment: temperature, humidity, light etc. If a appropriate environment cannot be ensured for all the systems in an organization, it is necessary to be ensured for the critical systems at least. A server center will not only ensure a constant temperature but will also ensure a specified humidity. Some manufacturers of such equipment impose even a maximum concentration of dusts particles.

Functioning in inappropriate technical conditions will assume that the system to be put to work in other technical conditions than the specified ones. The most common case is the one when the electric current is not provided at functional parameters. In most countries the electric energy indicator systems are made of some quantitative characteristics of slow variations (deviations) or fast variations (fluctuations) of the effective value of intensity, the shape and symmetry in the three-phase power system and also the slow/fast variation characteristics of frequency.

The action of an employee who makes an inappropriate intervention on a system is characterized by the fact that even if the employee apparently does a correct maneuver, this has as effect creating a flaw.

The occurrence of an event is characterized by the external actions over the system. We include in these external actions:
- human actions;
- environment actions.

Human actions are acts of persons, own employees, partners or other types of persons, who willingly perform malicious actions, these leading to the non-work of malfunction of the system. In the majority, these are physical actions that have a destruction purpose: intrusions, hits, vandalism, sabotage, theft, riots etc.

The environment actions are natural events that can disturb the functioning of a system or can even stop its functioning. In this category we include natural disasters: earthquakes, floods, storms etc.

Exceeding the service period is characterized by a high use of the mechanical and electrical components. This is the point in which the hardware component is considered to become unreliable. Exceeding the service period is the most commonly met cause of unreliability in organizations which have a weak management, which do not have a clear evidence of the systems, at least from the critical points, that must be replaced. Another case is the one of the organizations that try to obtain profit from not replacing the systems that are no longer guaranteed, not buying new ones. In some organizations this situation is fortuitous, the organizations having no more money to replace the equipment.

For making the hardware reliable it is necessary that the system contains redundant elements that in case of malfunction of an element, its role to be taken by an automatic one, or that the malfunctioning element could be changed without shutting down the entire system. In the case of a computer, we have the possibility of choosing configurations of disks in RAID 5 matrix (the information is written on 5 disks, 4 containing data and one with parity information), of configurations that would automatically eliminate the flaws and the functions would be taken by some other elements, of some loading balancing mechanisms etc [8]. If it is needed, the components can be changed during the functioning (while the computer is working) with the condition that these would support hot unplug/hot plug-in actions.

Redundancy works from duplicating the disks, the power sources, the cooling system to identical processing pipelines within the microprocessors systems. These microprocessors (IBM G5 from the S/390 system) contain two identical execution pipelines which execute the same operation and in the end they compare the results [8]. If the two results are the same, they go on to the next instruction, and if the results are not the same, the instruction is reviewed.

And as long as reliability has its costs the fact that a system with ECC memories works with almost 5% slower than one with Parity Memories must be specified [8].

The basic idea in building a system is the one that all the components of the system must be similar. The reliability of the new created system is the reliability of the least reliable.

Software

Software reliability

In this case the problem may seem simple because we think about the fact that the software component not having moving elements as the hardware component, things would be more simple, if there isn't anything to get worn.

A software component of a system becomes unreliable in the following cases:

- Bug occurrence;
- Insufficiently tested applications;
- Aging of applications.

Bug occurrence has as effect either unreliability of the system by the appearance of an exception and stopping the functioning, or have an effect over security of the system and consequently over reliability. A bug could be exploited by bad-willing persons to have access to the resources of the system. A software bug is the common term to describe an error, flaw, mistake, failure, or fault in a computer program or system that produces an incorrect or unexpected result, or causes it to behave in unintended ways.

Most of the bug errors occur because of a malfunctioning system or because of the bad generating of the source code. There are situations also when the compilers can generate wrong codes. Another situation when bugs appear is the one known as The Year 2000 problem, Y2K problem, the millennium bug, the Y2K bug, or simply Y2K. In the period when those applications were designed, nobody has taken into consideration four positions for representing the year, but only two.

Insufficiently tested applications will generate security and reliability problems. An observation must be made which is that things must be treated from both points of view: both **the manufacturer** and **the consumer's** points of view. If we go further we could set bounds to the software in O.S. and Application programs.

The O.S. manufacturer has the possibility to deliver on the market a beta version for testing before actually selling it. This way that the testing period would be efficiently used exactly by the potential owners. The possible malfunctions would be noted and subsequently corrected by the producer. If bugs are noticed during the service functioning, then immediate updates must be applied - hot fix and updates are also to be done.

This testing method is used both by the large producers of operating systems and the large producers of Application programs. Other ways that can be used for the same purpose are: shareware, liteware, freeware and public

domain software. Benefiting from these facilities, the software consumer can very well test the operating systems and the applications that are necessary to him. In some cases, these tests are not made on the organization data, but on example data. Subsequently, after acquisition, the product is not the one it should be or it has bugs on working with real data.

The aging of applications is in close connection with the hardware development. We cannot ask that very old applications work on a 64-bit equipped system. Unfortunately, some companies still use very old application due to the fact that the new ones are expensive and demand new systems. However, due to the physical use of the old computers transferring the old applications on the new computers could be done and here problems might occur regarding compatibility so that the applications would not work or could work but with errors. One phenomenon that usually occurs is bit rot [8]. This develops in two ways:

- the new computers do not support or do not read the storage devices or old peripheral devices.
- transferring the old applications on new computers can cause functioning errors.

To make the software reliable, it is necessary that the application that run is sufficiently enough tested before installation and run on an adequate system.

Human

The **human factor**, the most delicate component within an organization gets special treatment since it is known that man is so unpredictable, and that he has a great impact on security as well as on reliability. The CSI/FBI data indicate that the main source of insecurity is the own employee. There are two reasons why this is true: man interacts the most with the assets organization, having the power to alter reliability and man can initiate a malicious action because he has information about the organization, thus altering security and reliability.

If the organization would introduce employee authentication methods and would not explain the way they should be used, then the authentication system isn't reliable because it doesn't allow the employee fast access to a certain facility. This is the case of an insufficiently trained employee that will make the system protect itself and block access by entering a wrong password for several times. We can say the system is reliable because security is assured but at the same time it isn't because there are non-functioning periods of time. The same thing happens if the system becomes "annoying" and the user has to go through too many authentication methods for each and every application he has to work with.

A system is reliable if it is used according to its specific parameters. If the access is forced beyond limits by the employee, the system can become unreliable.

The measures that are taken in order to increase security and that target the personnel are one of the following types: **operational** and **organizational**. The operational ones target preventing and detection of unwilled events and define the maneuverability methods of data, of software components and hardware components by the personnel, here including the general and specific protection elements. The organizational type methods target preventing, detection and answer to the unwilled events and contain procedures and processes that establish the way of action of the personnel in case of certain events. An access control and surveillance system against intrusions is sometimes sufficient to discourage any human malicious action.

Reducing vulnerabilities in an organization must be a part of a complex cyclic security risk management program. In most cases, the cycle of risk management is divided into four different phases. Making a comparison between the two main approaches in the field, there can be distinguished common elements from the point of view of the goal [7] (Figure 6).

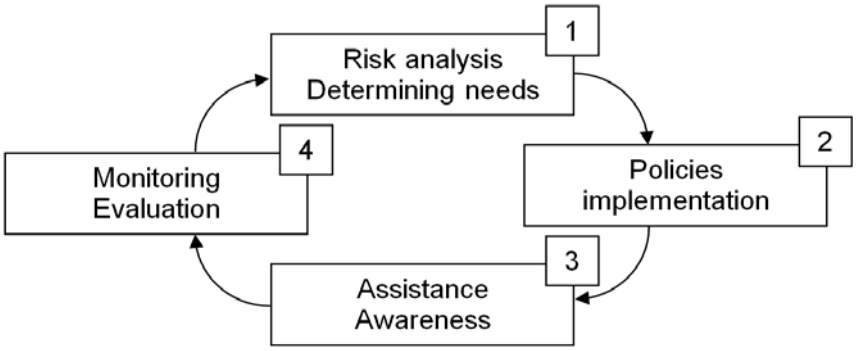

Fig. 6. Risk management cycle

Modeling the security inside an organization will be done based on the security policy. The security policy is made of a set of measures, accepted by the leading department, which provides clear but flexible rules to determine the standard operations and technologies that are necessary for ensuring security.

A bound must also be drawn between terms such as: politics, standard and guidelines.

A standard is made of a set of system or procedural demands that must be known and implemented. A standard will describe, for example how the security of a Windows Server 2003 that is placed in an unsecured area can be increased.

The guidelines represent a set of system or procedural suggestions necessary for a better practical implementation. These are not necessarily to be known but are highly recommended.

To ensure the company data's security and to ensure high reliability, it is sufficient that the organization implements access control and intrusion detection mechanisms. The infrastructure of the buildings must be built in such way that it will permit installing surveillance camera and physical systems of reducing access in some departments (keys, cards etc.). In every department data access control mechanisms of maximum security must be installed. It is necessary that every user passes through an access control mechanism (identification, authentication and authorization), Single-Sign-On (to ensure easy access to multiple applications) and encryption mechanism [4].

4 Reliability and Security versus Costs

As every investment, this one makes no exception from a cost-benefit analysis.

When talking about investments for security and providing reliability, things tend to be uncontrollable. This happens because the two notions and their role are not very well known inside an organization.

A production company will understand better an investment in reliability than an investment in security. This happens due to the fact that the term reliability is perceived as a technical term that has something to do with device functioning. A reliable device will be more productive and will generate more profit. Within the organizations or companies that don't count their activity on devices, security will be a lot easier understood. These must protect the data they work with; these are both their "raw material" and "final product". Because of this, investments related to reliability are perceived as being necessary, while the investments concerned with ensuring security are perceived as exaggerated. Even if both of them are based on probabilistic calculus.

However, an optimal level of security must exist. Optimal is the term that must be used to ensure security, even if some persons make confusion between the minimum of security and optimal. Statistical data show that 20% in security investment will generate an 80% decrease of security risk [4] (Figure 7).

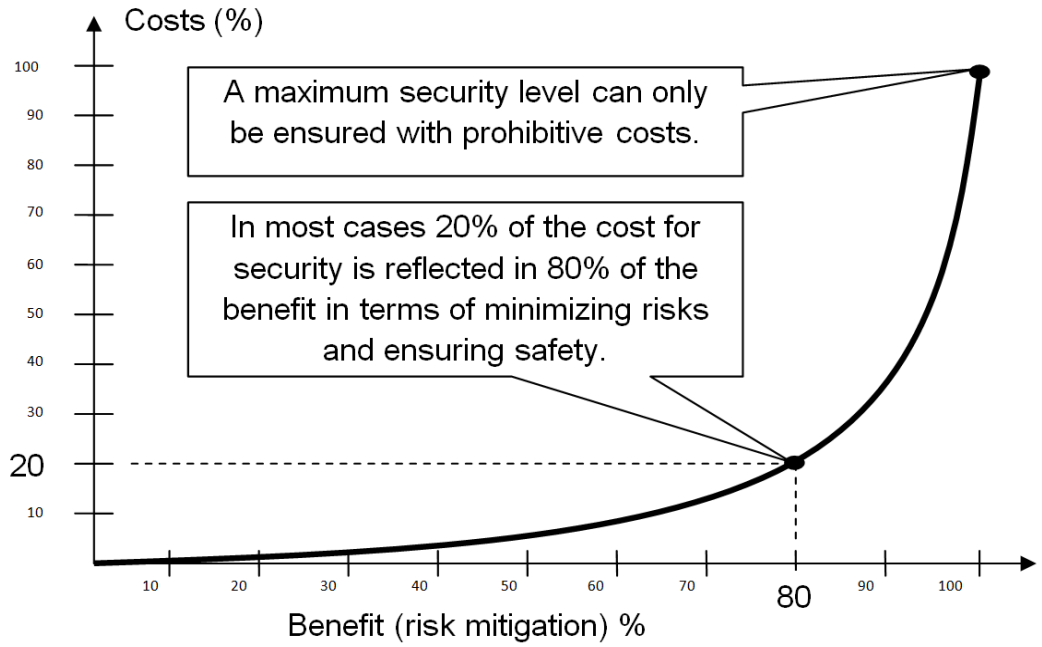

Fig. 7. Benefit and security costs

Estimating the costs for every chosen security solution will be done taking into consideration all the costs (Table 1).

Table 1. Security costs

Cost type	Explanations
Acquisition	Contain software and hardware costs and services necessary for acquiring control. Contain costs necessary for developing and updating the existing ones.
Implementation	Contain costs necessary for the teams or consultants to install and configure the imposed controls
Additional	These are costs that are difficult to estimate. We include the costs associated with the new controls on a certain period of time. There are management, monitoring and maintenance costs. Sometimes there are 24/7 (24/7/365).
Communication	Contain the costs necessary for the communication of personnel about the new policies and procedures for ensuring the security implemented within the organization.
IT personnel training	Contain the costs necessary for training IT personnel for implementing, accounting, monitoring and maintaining the new controls.
User training	Contain the costs necessary for training the personnel for the usual procedures of the new controls.
Productivity	Contain in fact de losses (initial) of productivity until the use of the new controls is a routine. In many cases these losses are due to the lack of communication and lack of personnel training.
Auditing and verification	Contain costs that the organization will periodically support for auditing and regular verification of the adopted controls efficiency. In some cases these costs go to professional companies – outsourcing.

When an investment in security is decided, the following profitability economic indicators will be taken into consideration: Return On Investment (ROI), that is the most used in these cases, Net Present Value (NPV) and Internal Rate of Return (IRR).

5 Conclusions

Security and reliability are two very important elements that must be taken into consideration when we talk about creating or developing an informatics system, with everything this one holds, both hardware and software, without neglecting the human factor. As we have just seen security is a complementary element of reliability. Reliability is concerned with internal aspects of well-functioning, while security deals with the external aspects that are represented by undesirable events. Reliability will be ensured if every component of the system is reliable and works in optimal security conditions. The security of the system, and implicitly its reliability, will be ensured by reducing the associated risks. This is done by implementing an efficient security risk management, with its main component- risk analysis.

References

[1] E. Burtescu. *Securitatea datelor firmei*, Editura Independența economică, Piteşti, 2005.
[2] N. Mărăşescu, *Fiabilitate şi diagnoză*, Editura Dunărea de Jos, Galați, 2004
[3] L. McCarthy, *IT Security: Risking the Corporation*, Prentice Hall PTR, 2003.
[4] P.E. Proctor, F.C. Byrnes, *The Secured Enterprise*, Prentice Hall PTR, 2002.
[5] M. Kaeo, *Designing Network Security*, Second Edition, Cisco Press, Macmillan Technical Publishing, 2003.
[6] A. S. Tanenbaum, *Rețele de calculatoare.* Ediția a IV-a. Editura Byblos, Bucureşti, 2004.
[7] http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default.mspx
[8] http://www.cs.cmu.edu/~mihaib/articles/fiabilitate/fiabilitate-html.html
[9] http://www.univ-angers.fr/docs/etudquassi/Fiabilite.pdf
[10] http://www.eventhelix.com/RealtimeMantra/FaultHandling/system_reliability_availability.htm

Emil BURTESCU has graduated the Polytechnics University of Bucharest, Faculty of Aerospace Engineering, Avionics specialization, in 1990. He holds a PhD diploma in Cybernetics and Economics Statistics at Faculty of Cybernetics, Statistics and Economic Informatics, Bucharest Academy of Economic Studies. Currently he is associate professor/senior lecturer at University of Piteşti, Faculty of Economics, department of Accountancy and Management Informatics. He is the author of more than 10 books and over 25 journal articles in the field. His work focuses on the analysis of security, information system audit and open-source database.