SHAPING SECURITY IN COMMUNICATION INFRASTRUCTURES WITHOUT RESTORING IN CASE OF MALFUNCTION

Gheorghiță PESCARU[1]

Lucrarea îşi propune să analizeze posibilitatea calculării unui coeficient de securitate globală pentru o infrastructură de comunicaţii dată ce poate fi folosită în diferite servicii de comunicaţii ca de exemplu e-sănătate, e-guvernare sau alte servicii de cu cerinţe similare. Ideea de la care se pleacă este aceea că furnizarea unui (unor) servicii de comunicaţii pentru aceste tipuri de aplicaţii trebuie să permită în permanenţă modelarea şi remodelarea configuraţiei unei reţele de comunicaţii pentru perioade variabile de timp. Dar ce se poate spune în aceste cazuri despre securitatea infrastructurilor rezultate, mai ales dacă anumiţi parametri de securitate sînt imperios necesari şi ceruţi anterior?

This paper is an attempt to analyze the likelihood of calculating an overall security coefficient for a given communication infrastructure that can be used in various communication services, such as e-healthcare, e-government, or other similar services. The assumption is that providing (certain) communication services for these types of applications is supposed to permanently allow configuration and reconfiguration of a communication network for variable time frames. But, under these circumstances, what can be said about the security of the resulting infrastructures mainly if certain security parametres are paramount and required beforehand?

Keywords: security coefficient, communication services, security parameters

1. Introduction

The present-day technical and technological progress has required a new field of expertise and security engineering respectively. From the research perspective, security engineering can already be found in many priority branches labelled as ”Space and security”, ”Infrastructures security”, ”Systems security”, ”Communication security”, etc. For more accurate understanding, ensuring security and proper functioning (work) of a communication network are seen as a unitary, self-standing, dynamic, flexible and omnipresent process. Therefore, security regarding proper function of a communication network must perfectly know the system’s vulnerabilities, it must permanently assess risks, prevent

[1] Ph.D student, National Institute of Studies and Research in Communications, Bucharest, Roamania, e-mail:gpescaru@co.cnscc.ro, george_pescaru@yahoo.com

unwanted incidents or damage through its available resources. In the present-day context of ever more poweful development of IT & C, and also considering the shortened lifespan of data, of their processing and communication, it is imperative to provide flexible and versatile communication and IT networks, so that they adapt to new types of communication services, on the one hand, and, on the other, to security of the information items that networks have been ”entrusted” with. Thus, alongside technical and technological development in various fields, especially communication and information processing, security vulnerabilities, on the one hand, increased in number, and so have the final users' demands, on the other hand. All these add up to the fast dynamics of using communication services on an ever shorter time frame, which leads to recurrent configuration and reconfiguration of network infrastructures. These aspects ask for several frame-situations on security and versatility analysis of communication networks and systems. **Let us consider an example**: a remotely perfomed high-risk surgical operation requires the use of a communication service between two consecutive moments, and the respective service be provided with a range of security parameters. The application runs between two geographic points having in between several communication operators using various transmission supports. In this case, network configuration will be established iteratively, together with the security decision-maker(s).

2. Decision-making in functional security

In today's context of the ever stronger development of IT & C technology and also considering the shortened lifespan of data, data processing and comunication, it is imperative that, on the one hand, some flexibility and versatility of IT & C networks to various kinds of services and communication be provided and, on the other hand, security of information items that networks have been ”entrusted” with must be granted as well.

Starting with the above-mentioned statements, we can analyze a global security coefficient of the application generated by the relationship between communication service and network.

The communication networks and systems security, as a major component of the provided communication services, represents a discipline within the newer field called 'security engineering'. This field uses multiple interdisciplinary knowledge in order to reach the following goals:

1. ensuring performant decision-making processes on communication systems and networks security and

2. efficient economic management of (a) communication network(s) and service(s) with inclusive security factors.

Given the facts presented above, proper work security (of a communication network) can be defined as maintaining technical and quality performances of the services provided, within a certain time frame.

The proper work security performances of a communication network are to be materialized/ quantified from the very stage of technical design and, further on, reshaped depending on the security demands of the various communication services requested/ offered. This goal is attained through optimal selection of network infrastructure, equipment, geographic placement and physical protection zones, of software, hardware and - mainly - orgware[2] resources, followed by hypotheses verification performed by means of laboratory simulations.

The appearance of a security theory as a factor of the provided communication service was prompted by the increased mobility and complexity of systems/ networks, by services needs for flexibility, loss prevention of any kind, the increase of communication service quality, of security and safeguard levels, etc.

That is why it is useful to know the real security level of a network, the versatility of its components/ equipment in order to decide on the ways and periods of intervention (maintenance) depending on the estimated values.

The meaning of the above-mentioned statements is concentrated in the process algorithm illustrated in fig. 1. According to this algorithm, starting from various beneficiaries' requests for communication services, an operator that owns various communication infrastructures is to configure (or reconfigure) various segments of the whole infrastructure in order to optimize costs and to reach an optimal model which is necessary for the required service and parameters.

[2] Orgware = a term that describes organizing information and data flows within a certain activity so as to contain "**maximum information concentrated into a minimal semantic resource"**, in order to optimize the respective activity.

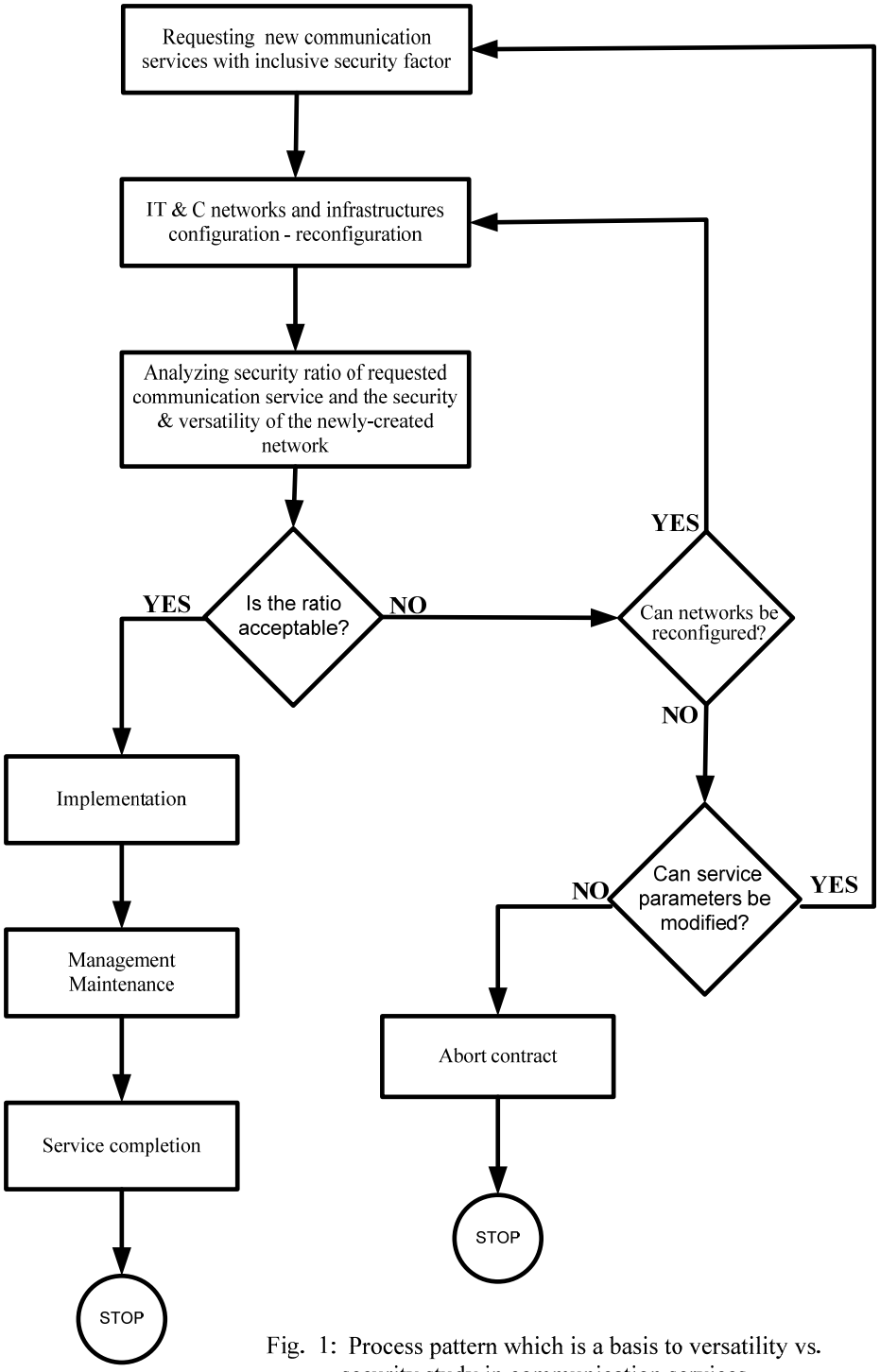

Fig. 1: Process pattern which is a basis to versatility vs. security study in communication services

Decision optimization (decision equation) practically refers to solving the three-dimensional pattern comprising the estimated **financial costs** of the service, the **security parameters** required by the beneficiary and the operator's **network infrastructure** (fig. 2).

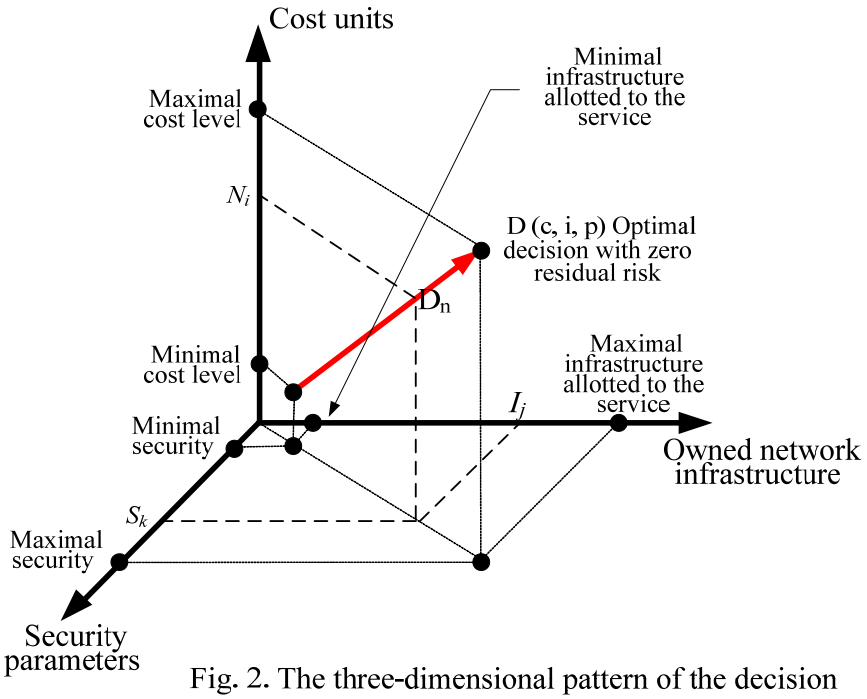

Fig. 2. The three-dimensional pattern of the decision

$$D(c,i,p) = C + I + P \tag{1}$$

where

- ***C*** = "cost units" represent all the estimated costs to provide the communication service;
- ***P*** = "security parameters" is a descriptive vector quantifying the security level and functions required by beneficiary;
- ***I*** = "network infrastructure" is a vector which quantifies either the equipment granted through reconfiguration in order to provide the communication service, or it quantifies the length of network routes, or the transmission way (RR, cable).

While studying network and communication service security, the assessment is performed by means of:

a) network breakdown analysis (from the viewpoint of causes, ways of appearing and development, ways of restoring);

b) assessing equipment behaviour during exploitation and during paroxysmic phenomena in relation to the share that these equipment items hold within the network structure;

c) establishing calculation methods and methodology in security decision prognosis and communication network service implicitly.

d) establishing data selection, filtering and processing in regard with analisys of component factors of network security and the afferent communication services.

Being conceptually defined on and circumscribing the application field of communication services, communication network and systems security represents **their capability of working without mulfunction, entirely safely, at preset parameters and within a certain time frame under well-defined exploitation conditions.**

Nevertheless, being a parameter with own time dynamics, its quantification leads to other two variables that are necessary in estimating communication networks security:

i. the network's (its components) likelihood of accomplishing their functions and maintaining technical parameters during the existence or running the prescribed communication services;

ii. the security and residual risks associated to the mulfunction likelihood be established in correlation with the five factors of communication network/ service security.

3. An abstract way of security moulding

In order to evaluate security performance instruments by means of which quantity expression should lead to as real and accurate as possible an approximation are necessary. The more accurate this evaluation, the more likely security risk-taking value is to become the basis of performant decision-making management.

But such management, applied to a communication network, with or without express specification of service types provided, is defined by another parameter called 'reliability level'[3]..

In other words, the reliability level (according to the definition given by ITU-T, Rec. X660, X400 and others), is achieved "by correlating two entities, one

entrusting the other with confidential data". The former entity acts on the assumption that the latter will "behave" according to an anticipated pattern.

The consquence of decreasing the reliability level is the **prejudice made by affecting the trust in communication services and their associated security factors**. It is possible that trust (reliability) and its level may apply to a single function (e.g. the availability of round-the-clock voice service), or to a complex of functions (e.g. availability and condidentiality of data service).

The **reliability level** is the criterion a security structure decision-maker will have to use in their analysis and whose relevance must be assessed in the long run. It is strongly correlated to the risk coefficient and the risk-taking level (fig.3).

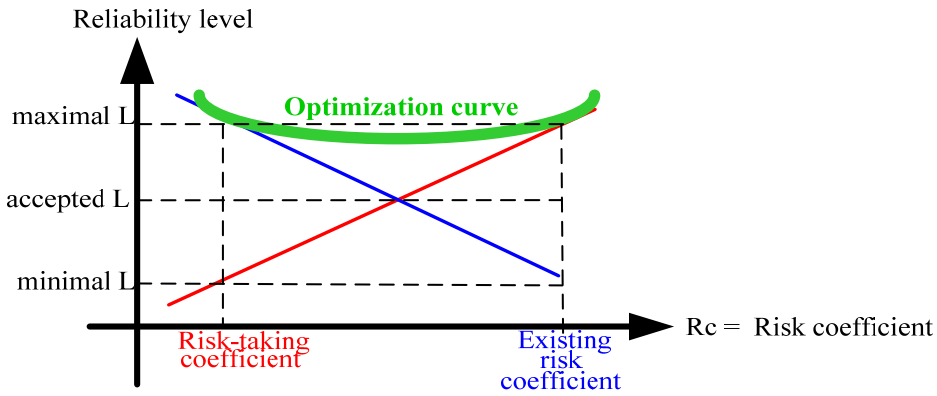

Fig. 3: Reliability level, risk-taking and its coefficient

The possibility or likelihood of affecting trust in the network (in its security) is an extremely important factor, through which the communication operator can be massively harmed. The reliability coefficient must point aut how this parameter can be affected and whether the security indicators are affected (or not).

For instance, a communication network/ service security analysis, depending on associated versatility, can be performed either globally, or at the level of the provided service, using modelling by means of system theory (fig. 4).

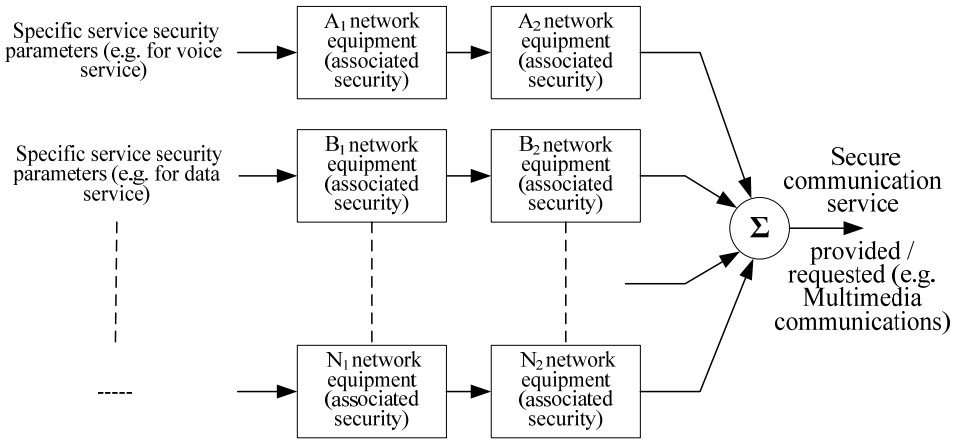

Fig. 4: Versatility analysis of a communication service/ network related to security functions

To exemplify, during a data transmission between two or more network users, the required service can be made up of:

1) user authentification, in which case equipment B_1 will be an access interface with authentification/ password;

2) data confidentiality, in which case network equipment B_2 will be coding/ encryption equipment;

3) availability-mobility, in which case equipment B_3 (not included in fig. 4) is radio-relay, wireless.

In security moulding, of course, all types of stress (static, quasi-permanent, dynamic, fluctuating, perturbation) are to be taken into account. In such a model, when analyzing security of component equipment of the network/ service we can notice that the process quantification assessment is very laborious due to the simultaneous analysis of a $\boldsymbol{p}$ number of random processes composing the exit vector's matrix.

When using the methods in security calculation and analysis, limiting situations in functioning were avoided, preferring the mulfunction situation only, which led to operating – within performance – two dimensions: function at preset parameters or mulfunction (breakdown).

In the case we have selected – a case where there is not a restoring option – it results, from the beginning, that availability function (seen as a service security factor) cannot be taken into account. To consider this function would presuppose the existence of redundant equipment (or certain infrastructures) so as service availability be continually provided throughout the length of the request.

As an illustration, the following functional requirements associated to a communication service are considered:

1. A voice communication service having the following security functions:
   - authentification;
   - confidentiality;
   - non-repudiation.

Such a service can be shaped considering both the security functions and the infrastructure elements of the network as functional blocks in various configurations.

If all components security is known, the problem that poses is that of determining service security through a structural model analysis.

This represents an equivalent logical scheme through which can be described – by means of specific descriptors – the system function from the security viewpoint.

Knowing and analyzing these parameters will lead to the opportunity of optimizing decision patterns.

We must mention that functional blocks appearing in such modelling (patterns) have to be completely independent from the equipment security point of view.

Thus, when making the analysis scheme, it is necessary to carefully study each block functioning, i.e. their impact of partial or total mulfunction on the system/ service in its whole. Based on this information tables of function combinations will be made next, these tables being of help in decision optimization, establishing residual risks and acceptabitity limits.

If functional analysis uses blocks among which there are correlative functions different from zero, the results can be wrong.

Let $X_n(t)$ be a proper work security function of block n, and $X_m(t)$ the proper work security function of block m. A functional analysis can be obtained

$$\forall (m,n) \in S_k \rightarrow C_{m,n}(\tau) = \int_{l_1}^{l_2} X_m(t+\tau) \cdot X_n(t)\, dt \tag{2}$$

where:

- S_k = (1, 2, ..., m, n) is the considered system (network, communication service) having (1, 2, ..., m, n) functional blocks;
- l_1, l_2 are the values of time intervals;
- $T \in (t, t + \tau)$ the time frame (interval) during which the communication service and its associated security function must work;
- $C_{m,n}(\tau)$ = the correlative function between blocks m and n.

Within a functional scheme, the interconnection ways of functional blocks can start with a simple, serial, cascade tie (fig. 5.),

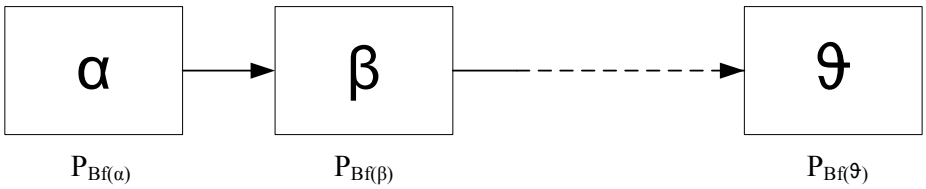

Fig. 5: Serial cascade of functional blocks to be found in a communication service

or other interconnection types that can be further analyzed (fig. 6.).

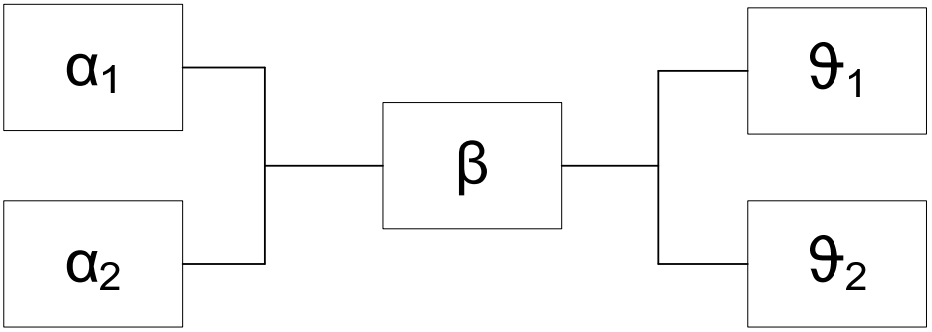

Fig. 6: Examples of functional blocks interconnections within a communication service

For easier use of symbols, we have used part of the already known ones in the respective field of versatility.

$P_{Bf(\alpha)} = R(t) = p_\alpha$ proper work likelihood of block α.

$P_{Bf(\alpha)} = F(t) = q_\alpha$ likelihood of interrupting work or of working out of the preset limits.

To analyze proper work security we can use the language of probability theory. The work interval up to service interruption (breakdown)[1] can be estimated as proper function (work) likelihood. It is obvious that in the pattern illustrated in fig. 5 the secure communication service will be applicable if each of the functional blocks ***α, β, ... γ,*** accomplishes its own security function, in which case the proper work likelihood of the whole chain will be:

[1] I hereby remind that service interruption should not be interpreted as effective occurrence. From the security viewpoint, the deviation from preset functional limits is also considered interruption.

$$R(0,t) = \prod_{i=1}^{k} \left(R_i(0,t) \right) \tag{3}$$

It consequently results that the likelihood of parameter deviation (considered mulfunction and/ or interruption) of the service will be:

$$F(0,t) = 1 - \prod_{i=1}^{k} R_i(0,t) = 1 - \prod_{i=1}^{k} \left(1 - F_i(0,t) \right) \tag{4}$$

For a certain time frame τ associated to a secure communication service starting at moment t, the mulfunction likelihood due to a composing block can be approximated by means of the following equation:

$$F(t, t+\tau) = F(t+\tau) - F(t) \tag{5}$$

As we considered from the very beginning, the communication service is – according to the selected choice – a secure one both with geographic and time availability functions. In other words, a broadcast is not supposed to break down within a preset time frame. Service interruption can be taken for, let's say, 'the death' of an equipment item having a broken component.

But work and interruption depend on the service proper function (work) within interval ***(0, t)***. Hence:

$$F(t, t+\tau) = \frac{F(t+\tau) - F(t)}{R(t)} \tag{6}$$

and

$$R(t, t+\tau) = \frac{R(t+\tau)}{R(t)} \tag{7}$$

If for evaluation purpose the service behaviour at a certain moment is wanted (estimating, for instance, that a vital piece of information will be broadcast at a certain moment) the (system) behaviour can be studied by limit conversion:

$$C(t) = \lim_{\tau \to 0} \frac{F(t+\sigma) - F(t)}{\tau} \tag{8}$$

But since service behaviour is evaluated with a completion likelihood within time interval τ, ***C(t)*** **will be the likelihood density** representing the ratio limit between the overall insecurity likelihood within interval ***(t, t + τ)*** and the size of this interval when it tends to zero. To put it in another way, ***C(t)*** **will be the work time allowance** until insecuring and thus service interruption (or mulfunction), its significance being that of **overall likelihood of security damaging at about moment *t***.

To fiind aut the vulnerabilities at about a given moment ***t*** during a service that belongs to a communication service in working condition up to moment ***t***, we are to define another descriptor pointing to service (network) behaviour from the security point of view. This latter descriptor, called **security damage rate**, is a conditioned probability and it can be defined as security damage likelihood at about a moment ***t***, being nevertheless conditioned by ensuring security up to that moment. It results:

$$Y(t) = \lim_{\tau \to 0} \frac{F(t+\tau) - F(t)}{R(t) \cdot \tau} \tag{9}$$

where ***Y(t)*** = service security damage rate.

From the previous expressions it results that:

$$Y(t) = -\frac{1}{R(t)} \cdot \frac{dR(t)}{dt} \tag{10}$$

The above expression leads to the expression of service/ network timely secure work providing that $\boldsymbol{R_{(0)} = 1}$:

$$R(t) = \frac{1}{e^{\int_0^t Y(\theta) d\theta}} \tag{11}$$

and

$$F(t) = 1 - R(t) \tag{12}$$

Other factors able to characterize a communication service/ network security may be:

- secure work time mean;

- square deviation mean;
- secure work time dispersion.

Secure work time **mean** will be given by the expression:

$$m_{tbf} = \int_0^{\infty} R(t)dt \tag{13}$$

which results from:

$$m_{tbf} = \int_0^{\infty} C(t)dt \text{ pentru } t \in (0,\infty) \tag{14}$$

The **square deviation mean** will be given by:

$$\alpha_{mp} = \int_0^{\infty} \left(t - m_{tbf}\right)^2 dt \tag{15}$$

and the secure work time **dispersion** will be:

$$\alpha_{mp} = \sqrt{\alpha_{mp}} \tag{16}$$

The square deviation mean and secure work time dispersion can point to the way the defining parameters of a communication service or network are timely secure.

If security monitoring process is properly controlled, the descriptor values α_{mp} and σ will be low related to the imposed requirements. The increase of these descriptors, **determined through statistical audit assessment** of network situations is an indicator in the security residual risk evaluation.

Another descriptor, which is almost time-independent, is the **granted security interval** t_s, given by the equation:

$$F(t_s) = s \tag{17}$$

In other words, if s does not exceed a certain preset value, the situations during work of a communication network/ service are not able to affect security.

4. Conclusion

The model (pattern) presented above is only a small part of the great number of opportunities that can be (mathematically) approached in order to assess (predict/ forecast) a communication service or network security when this

is imposed by the service request dynamics. It can be completed or added to other evaluation patterns or options, thus contributing to the spiral of knowing the security engineering field.

Through its content the paper is trying to draw attention to two aspects:
1) the opportunity of calculating a global security coefficient for a communication service with preset initial parameters and
2) the existence of multiple (abstract) approaches on security decision-making.

In time maybe, a unitary theory on approaches of calculating an overall security coefficient, circumscribed to the requested service will be established.

R E F E R E N C E S

[1]. *Dr. Kamilo Feher*: Sisteme şi tehnici de prelucrare a semnalelor, vol. 1, Editura Tehnică, Bucureşti 1993
[2]. *Ghe. Ilie, ş.a.,* „Securitatea Informațiilor”, Editura Militară, Bucureşti, 1996
[3]. ISO/IEC TR 15947:2002, Information technology – Security techniques – IT intrusion detection framework
[4]. ISO/IEC 18028 (all parts), IT security techniques – IT network security
[5]. ISO/IEC 18043, IT security techniques – Guidelines for the Selection, Deployment and Operations for Intrusion Detection Systems (IDS) (document type subject to NP approval on SC27 N4029 by 2004-09-24)
[6]. ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards
[7]. ISO/CEI 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model, Part 2: Security Architecture
[8]. ISO/IEC TR 13335-3, Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security
[9]. National Computer Security Center: "Trusted Network. Interpretation", NCSC-TG-005, NCSC, 31 July 2007.
[10]. National Computer Security Center: "Glossary of Computer Security Terms", NCSC-TG-004, NCSC, 21 October 2006.
[11]. National Computer Security Center: "A Guide to Understanding AUDIT, In Trusted Systems", NCSC-TG-001, Version-2, 1 June 2006
[12]. *R.J. Sutton*: “Secure Communications. Aplications & Management”, Editor David Hutchinson, Lancaster University
[13]. *R. Anderson*: „Security Engineering. A Guide to Building Dependable Disdtributed Systems”, John Wiley & Sons, Inc., New York, 2001
[14]. *Ş.–V. Nicolaescu ş.a.* „Reţele radio de acces de bandă largă”, Editura AGIR, Bucureşti, 2005
[15]. *Ş.–V. Nicolaescu ş.a.*.: „Securitatea în reţelele Wi-Fi”, Editura AGIR, Bucureşti, 2008
[16]. TCSEC, Trusted Computer Systems Evaluation Criteria, US DoD 5200.28-STD, December 1985
[17]. *T.I. Băjenescu*: „Comunicații de bandă largă. Aspecte tehnice, economice, politice şi sociale”, Editura Matrix Rom, Bucureşti, 2004
[18]. *T.I. Băjenescu*: Rețele Inteligente, Bucureşti, Editura Tehnică, 2001
[19]. *T.I. Băjenescu*: „Fiabilitatea sistemelor tehnice”, Editura Matrix Rom, Bucureşti, 2003
[20]. *T.I. Băjenescu*: Managementul rețelelor moderne de telecomunicații, Bucureşti, Editura Teora, 1998
[21]. *V.–V.Patriciu ş.a*: “Securitatea Informatică în Unix şi Internet”, Editura Tehnică, 2001.