Collaborative Management of Risks and Complexity in Banking Systems

Ion IVAN, Cristian CIUREA, Mihai DOINEA, Arthur AVRAMIEA
Department of Economic Informatics and Cybernetics,
Academy of Economic Studies, Bucharest, Romania,
ionivan@ase.ro, cristian.ciurea@ie.ase.ro, mihai.doinea@ie.ase.ro,
arthur.avramiea@gmail.com

This paper describes types of risks encountered in banking systems and ways to prevent and eliminate them. Banking systems are presented in order to have a view on banking activities and processes that generates risks. The risks in banking processes are analyzed and the collaborative character of risk management is highlighted. A way to control the risk in banking systems through information security is described. Risks arise from system complexity, thus evaluation and comparison of different configurations are bases for improvements. The Halstead relative complexity function synthesizes system complexity from the point of view of the size of the variables analyzed and the heterogeneity between the variables. Section four was realized by Catalin SBORA.

Keywords: *Collaborative Management, Risk, Complexity, Banking Systems, Processes, Security*

1 Collaborative banking systems

There are many implementations of collaborative systems in the economy, in different areas of interest and in both environments: real and virtual.

In the real environment, there are many types of collaborative systems, the most important being the collaborative banking systems, collaborative educational systems and collaborative systems in production.

In the virtual environment, the collaborative systems implemented are represented by the virtual campus, the virtual bank, the virtual enterprise for software development and the virtual enterprise for production processes.

There are many aspects that must be taken into consideration when analyzing the differences between collaborative systems implemented in real environments and the ones implemented in virtual environments.

A collaborative system, $\sum$, is defined by the following elements [12]:

$\Sigma = (T, S, R, I, \Omega, X, E, \Gamma, F, \psi, \varphi, \eta)$,

where:

T – the time, represented by the lot of moments in which the system operates;

S – the space, represented by the set of locations where the system operates;

R – the resources, the lot of human, material and energy resources that contribute to activity achievement;

I – the set of values of input variable i;

Ω – the class of temporary evolutions allowed, $\Omega = \{\omega : T -> I\}$, $\omega = \{i(t) / t \in T, i(t) \in I\}$, $\Omega \neq \phi$;

X – the space of states, represented by the set of values of state variable x;

E – the set of values of output variable e;

Γ – the class of possible outputs, $\Gamma = \{\gamma : T -> E\}$, $\gamma = \{e(t) / t \in T, e(t) \in E\}$;

F – the work flows, the set of values of flow variable f;

Ψ – the security component inside the collaborative system;

φ – the transition function of the system, $\varphi : TxTxXx\Omega -> X$, $x(t) = \varphi(t; \tau; x; \omega)$;

η – the output function of the system, $\eta : TxX -> E$, $e(t) = \eta(t; x(t))$.

The banking system is the most significant collaborative system, because it has a large number of components and a large variety of links between them. The banking information system must be collaborative, because it requires the communication, coordination and cooperation of different informatics applications, in order to achieve a common goal.

2 Specific features of banking processes

In a banking system there are many processes which can be analyzed in order to highlight their specific features and their collaborative character. The banking process regarding the acquisition of the electronic payments service by a customer is a collaborative process. Collaborative processes require the existence of such activities that need to be automated to streamline the workflow within an organization [6].

Banking processes involves many and very different types of transactions. In a banking process, there are implied the followings types of transactions:

- transfers between existing accounts;
- opening new accounts;
- realization or liquidation of deposits;
- according loans;
- foreign exchanges;
- payments to state budget;
- payments to customs;
- salaries payments;
- direct payments to suppliers;
- other operations.

These types of operations are executed during the whole working day, but their frequencies are different in every hour of the day. Table 1 shows the hourly frequencies of the operations mentioned above during a whole working day.

Table 1. Frequencies of hourly operations in a banking day

No.	Transaction type	Freq. (08:00-09:00)	Freq. [09:00-10:00)	Freq. [10:00-11:00)	Freq. [11:00-12:00)	Freq. [12:00-13:00)	Freq. [13:00-14:00)	Freq. [14:00-15:00)	Freq. [15:00-16:00)	Freq. [16:00-17:00)
1	transfers between existing accounts	2%	3%	5%	10%	15%	15%	**35%**	10%	5%
2	opening new accounts	5%	**15%**	**15%**	**15%**	10%	**15%**	5%	**15%**	5%
3	realization or liquidation of deposits	10%	10%	10%	10%	**20%**	10%	10%	10%	10%
4	according loans	3%	17%	10%	5%	5%	5%	3%	12%	**40%**
5	foreign exchanges	20%	5%	5%	10%	5%	**23%**	7%	15%	10%
6	payments to state budget	15%	15%	10%	**25%**	5%	7%	5%	13%	5%
7	payments to customs	5%	15%	15%	7%	11%	**20%**	2%	**20%**	5%
8	direct payments to suppliers	20%	10%	15%	13%	19%	3%	**23%**	3%	10%
9	other operations	**20%**	10%	15%	5%	10%	2%	10%	2%	10%

Most risky operations are those with great share, such as transfers between existing accounts, according loans and payments to state budget. As seen in the matrix from Table 1, there are different hours at which these operations achieve their maximum frequencies. The great number of operations and their diversity within a collaborative banking process determine different risks that must be treated accordingly.

For direct payments to suppliers, the risk to debit an account with a value greater than the account balance must be taken into consideration. In this case, the account will remain on unauthorized overdraft.

In the case if an incorrect transaction on a client account is made, meaning that a

payment to another beneficiary than the correct one is made or a wrong amount of money is transferred, then the payment reversal is carried out and a new transaction account is registered.

3 Risks in banking processes

Collaborative processes require the existence of such activities that need to be automated to streamline the workflow within an organization. In collaborative processes within a bank, any change in the workflow must be found in the corresponding rules and procedures.

In [6] is realized a classification of risks encountered in banking processes. Depending on their size, risks are divided into low, moderate and high risk. Within the applications from collaborative banking system, appear:

- *small risks*, technical malfunction of a machine running the banking software system; whereas system was designed to work collaboratively online, any technical failure of the client computers have a limited financial impact and a practically null one in the banking unit;
- *moderate risks*, functional requirements from banking processes are not expressed or explained, which affects the development cycle by replaying design, coding and testing; moderate risks delay the development process: lack of accurate data of credit documents, wrong value records of the payments received/made, incorrect calculation of the credit rates;
- *high risks*, project funding ceases due to changes in legislation or bank's policy: phishing attacks that expose collaborative system's security and gain access to customer accounts.

Depending on the stages of the development cycle of a collaborative banking process, during which risks can occur, several types of risks are identified:

- *user requirements risks*, lack of coverage of all situations of using the banking system, incomplete treatment of security requirements;
- *design risks*, lack of understanding the non-functional cases and constraints related to programming language;
- *implementation risks*, failure to identify significant components, subsystems integration failure, lack of testing use cases;
- *launch risks*, failure of collaborative processes on host machines, negative feedback from users;
- *maintenance and upgrade risks*, the emergence of unsolvable bug, the occurrence of use cases for the implementation of which should be reload the entire development cycle.

These expectations and risk classifications do not avoid unexpected events, but encourage an informed handling of situations. Classifying risks determines first risk identification and then implementation of appropriate methods for treatment in their context.

In [7] and [8] the author is presenting an insight of the today's banking systems and the risks that these systems are exposed to. The banking systems are very complex and the task of controlling the risks is not an easy one, especially because these systems are created by an aggregation of different subsystems. Inside a banking system there are multiple types of risks, but in this section we will refer to the risks of fraud through the computer systems. Having many subsystems involved, there will always be a risk for one of them to create vulnerabilities due to either technical limitations, outside cyber attacks or dishonesty of the inside people.

The banking field is the most exposed to security attacks and the financial losses are significant when security vulnerabilities are found and exploited. The security of banking information systems must be analyzed according to categories of users that accessed them and types of applications integrated in the system. There are some applications of banking information system which can be accessed by internal users (employees) and the others by external users (customers or partners). The access rights and security policies are different, depending on such type

of user access. The internal applications can be accessed by employees without many restrictions, respecting the single-sign-on rules. The external applications, which are accessed by customers, such as internet or mobile banking applications have multiple security restrictions, in order to prevent possible security attacks [13].

Usually, when starting to work with a software system from a bank environment, the user is asked to authenticate before any other operation, in this way the system can adjust the level of permissions and track the operations made by an employee. Authentication is one of the most important security tools, for confirming user's identity.

There are multiple methods for completing the authentication process, but none of them is completely flawless, and we are not talking about flaws in the technical part of the process or encryption algorithms, but more to the situations where the authentication credentials can be stolen by different means (technical or non-technical), and the authentication process and implicitly the security of the system are compromised. So, the strength of an authentication process is actually given by the ability of self-protecting the user.

In collaborative banking information systems, the new security elements that must be taken into consideration in the case of electronic banking applications are not related to users' access. The possible future attacks will be provided by existing users and customers, which will exploit security vulnerabilities of the applications, after they are logged in. These vulnerabilities refer to the possibility to make payments from an unauthorized account or in the name of another user/customer.

4 Collaborative management of risks (by Catalin SBORA)

In [1] is considered that management has been put among the factors determining labor productivity in the academic literature and since its input varies between firms and workplaces, it is likely to have a large effect on economic performance, at least at the low levels of aggregation.

In [2] is described the quality management system that typically improve the documentation of operating procedures, training, and procedures for corrective action.

In [3] is provided a methodology for detecting management fraud in public companies using basic financial data.

In [4] are presented the technical challenges and are illustrated the details about how to enable different management interfaces to be in service-oriented styles. The approach is evaluated and discussed in order to know how to manage middleware systems collaboratively based on management services.

In addition to classical management, the collaborative management comes with some new elements, such as:

- possibility to be applied in distributed environments;
- involvement of multiple managers that are working collaboratively;
- use of a common goal that is followed by all the participants.

When dealing with security risk management one must take into consideration that the risk sources and the factors that can affect the security of the information system are numerous and spread across the entire system, especially when talking about a banking system which has multiple subsystems that need to cooperate. In this case the management of security risks is strongly dependent on the specific of each subsystem, but in the same time it must adhere to a standard procedure, and this thing can be achieved only by having multiple distributed components enrolled in a collaborative process with the goal of providing a unified interface for monitoring and managing the risks across the entire system.

On the other hand when we are referring to risks different than those exposed by information security, like the risks exposed by the fact that functional requirements from banking processes are not expressed or explained, risks exposed by the lack of

coverage for all situations of using the banking system, risks exposed by the failure of identifying significant components, subsystems integration failure, we can say that these risks can be managed only by cooperation and collaboration between the parties involved in the process of development and maintenance for the banking system.

Basically in a banking environment, vulnerabilities can be exploited once, from inside and not necessarily with the acknowledgement of the employees, and once from outside by people that either try to penetrate security systems and gain access to bank's internal systems or simply scamming bank's customers, for getting their credentials. If we think on the public interface of a banking system, we describe three main types of systems:

- wire transfer system;
- ATM system;
- online banking system.

From these three categories, the most exposed to external attacks are the ATM systems, and Online Banking systems, as for the ATM systems, we can say that after almost 50 years of use, they have reached the maturity and their vulnerabilities are well known, and some of these were fixed, others still exists. One of the common and well known vulnerabilities of these systems is the fact that information from the magnetic strip of a card can be copied without owner's knowledge, and used afterwards for cloning the card and use the clone for doing transactions on behalf of the real owner. To copy the information from one's card the thieves are using some third party devices, called skimming devices which are being attached to a legitimate ATM, thereby the users are usually less suspicious. Having only the data on the card is not enough for getting access to the bank account, since the cards are being protected by a 4 to 6 digit PIN number which should be known only by the owner of the card. To get access to this code the thieves are using a video camera that is placed somewhere near the ATM, headed to the keyboard of the machine, so each key that is pressed is recorded on the camera and used later for getting access to the PIN number.

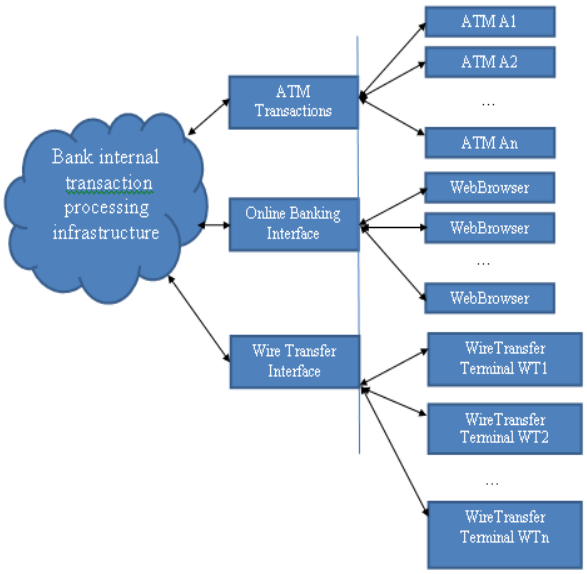

Fig. 1. Bank internal transaction processing infrastructure

To control this kind of threats, banks have started to place the ATMs in locations where they can be watched by authorized personnel, mostly nearby bank offices, reducing the risk for someone to work on the machine and mount the skimming device with the video camera.

For the online banking environment things are more complicated since there is no way the bank could watch all terminals being used for completing transactions, and it comes to the user to make sure that authentication credentials are not compromised. The method by which the users are being identified in such a system, is based on a user and a password, with the password being static or dynamic. At the beginning of the online banking, the way the authentication was made, was through a user and a static password, but shortly this proved to be highly inefficient, since the users were not educated for handling this new technology and they were easy to trick for providing the credentials for their online banking account, providing the thieves with complete access to their bank accounts. Initially when, the users were not really aware of the threats, the easiest way for tricking someone and get access to his account was to launch a

phishing attack, through a simple e-mail. The procedure is rather simple: the thief is sending an e-mail to the account owner, usually in behalf of the bank, and it asks the user to login into his account using a link included in the e-mail. When the user follows the link it will get to a web application that looks identical to the bank's official online banking application, but when the user enters his credentials those will get to the bad guys, instead of getting to the bank system for authentication. Another way for obtaining information about one's authentication credentials is to install different types of viruses, like Spyware and Trojan Horses.

Given these conditions, where the security of the transactions was dependent on users that were more or less educated on how to use this technology and how to keep their credentials safe, the banks had to come with an authentication method that doesn't rely that much on the user's ability of not disclosing his credentials. At this point, most of the European banks are using a method based on a one-time password authentication, where the password is being generated by a hardware device (called password token) that is handed to the user when he is creating the online banking account. In order to be able to access one's account by impersonation, an attacker must physically poses that hardware token, and in the same time to be aware of the owner user name. Although at a first sight this method seems bullet proof, it also has a wick point, and that is generated by the fact that an attacker can run a real-time attack, by sniffing or using a traffic proxy in a classical Man-In-The-Middle Attack. In order to explain this we assume that the attacker has access to change browser settings on a target system through a Trojan Horse or other type of malware, for redirecting the traffic through a proxy.

When the user tries to login on his online banking account the request will get into the proxy application which is actually controlled by the attacker. At this point in order to check the validity of the credentials the proxy will automatically go and try to login on the bank portal, if the credentials are not validated the response is sent back to the proxy, which will forward the response to the user and ask to reenter the credentials. Once the credentials have been validated, the proxy application can return a nice message to the legitimate user, saying that the web site is temporarily unavailable, while in the background the attacker can take over the control and make transactions in behalf of the victim. One might say that this scenario would not be possible because of the fact that SSL (Secure Sockets Layer)/TLS is being used, and the information is being encrypted, but keep in mind that SSL is also vulnerable to MITM attack.

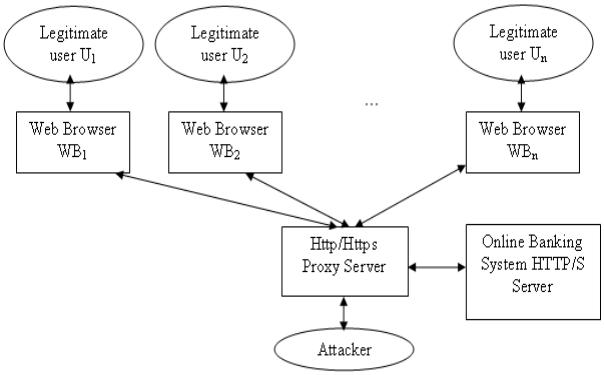

Fig. 2. Attacks against the online banking system

For this kind of architecture, with only one proxy server the attacks are not very hard to detect and stop by the Online Banking System, since the system can have a mechanism that identifies when the server receives too many requests for different users from the same IP address. But if we think to a more complicated architecture with multiple proxy servers distributed in the Internet, the problem becomes hard to approach.

5 Risk control through information security

Risk control is a complex operation that necessitates huge amounts of resources for undertaking activities such as:

- identifying risks is the activity that discovers vulnerabilities and all the sources that can exploit the doors through

which damages could be inflicted into a banking system;
- risks evaluation consists in a set of measurements upon the impact of the damages generated by the identified vulnerabilities that were exploited by outside or inside threats;
- risk control is the stage that based on preliminary measurements can decide which one of the risks need to be treated and which one not and how many resources must be engaged in this fight against threats;
- documenting risks is the final step after a thorough evaluation of a banking system which creates a final ranking and classification.

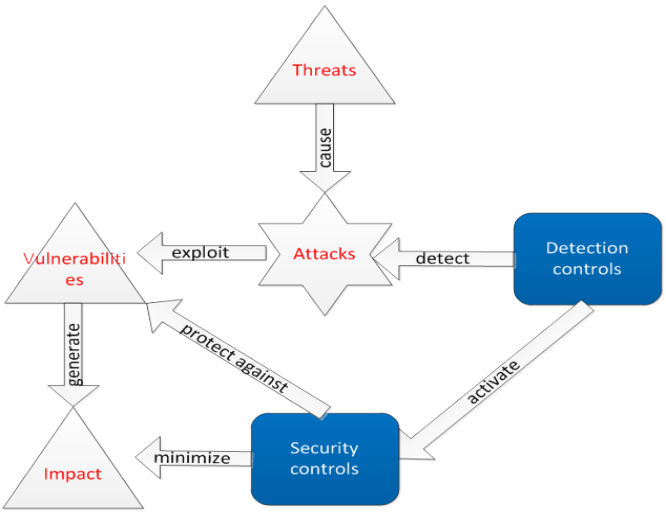

Fig. 3. Correlations diagram

Based on the previous activities presented the diagram [9] from Figure 3 reveals the correlations between threats, attacks, detection and security controls, vulnerabilities and impact.

In the moment when security risks are identified and the steps from Figure 3 are starting to take shape than, based on the correlations in Table 2, [10], which presents the probability that a risk scenario will occur, P, and the impact upon the banking system, I, the level of damage inflicted to banking system can be determined and split in three categories of minimum, medium and critical risks.

Table 2. Risk aggregation

Probability	IR = P x I				
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
	Impact				
	Minimum risk (acceptable)		Medium risk		Critical risk

In order to protect the quality characteristics of a banking system and maintain a certain level of characteristics correlations, [11], the security team has to deal with the process of risk management by taking into account the following aspects:
- security risks will be correlated with the quality characteristics, keeping an eye

upon how much the controls that protects the system against them influence the quality level;
- risks are addressed based on the banking system level at which are identified so they can be prioritized;
- in the risk control activity, a banking system is influenced in an equal manner by inside factors as well as outside threats, case in which the approach should be adequately chosen for each category.

The levels at which a banking system is fragile and what measures can neutralize the correspondent risks effects are:
- online payments system, here an appropriate method of authentication by means of multi factor system is preferable to be implemented in order to secure both the access to personal information and also each transaction made by remote users;
- internal personal, is the level at which a good internal security policy can annihilate almost all the risk aspects that a banking system can deal with by implementing an access policy with roles and privileges and as well a clearance level for each one of its employees;
- outside threats, an ongoing fight against them, being easily out-passed by means of technological and software equipments specially designed to combat the way they attack the system.

In [5] is considered that traditional product process management usually manages some relatively simple process like product document generation, approval and dissemination, and cannot manage complicated product simulation process and correlative dynamic information.

The risk management process implies the following elements:
- a subset of security resources $sr_i = \{sr_{i1}, sr_{i2}, \dots, sr_{in}\}$, n – the total number of different resources;
- a subset of collaborative processes $cp_j = \{cp_{j1}, cp_{j2}, \dots, cp_{jm}\}$, m – the number of existing collaborative processes of which security must be managed;
- a subset of risks associated with a collaborative banking system, $r_k = \{r_{k1}, r_{k2}, \dots, r_{kp}\}$, p – the number of risks identified as a result of security analysis for a collaborative banking system.

Based on the resources from sr_i involved in the process of neutralizing the risks r_k that can affect the collaborative process cp_j, a relation can be established between this elements, described by the *AR* function, which specifies what are the associated risks for a unique pair of security resources and collaborative processes, like follows:

$$AR: SR \times CP \rightarrow R$$

where:

$SR = \{sr_i | i = \overline{1,x}\}$ – the set of security resources;

$CP = \{cp_j | j = \overline{1,y}\}$ –set of collaborative processes;

$R = \{r_k | k = \overline{1,z}\}$ –the set of collaborative risks;

$x = Card(SR), y = Card(CP), z = Card(R).$

In a collaborative banking system, the security component, ψ, is represented by a relation between the set of security resources, *SR*.

The planned risk level associated with a set of resources applied for a set of collaborative processes is defined as PRL_kbeing dependent onr_k. But the actual risk level calculated for a specific moment in time is defined as $ARL_k(t)$.

If the actual risk level for a collaborative banking system, $ARL_k(t)$is determined and compared with the PRL_k, the following situations occur:
- $ARL_k(t) > PRL_k$– the measures taken to counteract the risks are unsatisfactory;
- $ARL_k(t) < PRL_k$ – the actual risk level is lower than the planned one, meaning efficiency of the security resources;
- $ARL_k(t) = PRL_k$ – what comes in the system as defense mechanisms can neutralize exactly the threats identified from outside and inside the system.

Being given the r_k risks associated with the collaborative processes and for a *t* point in time, the costs of the risk management process,$C(RM_k(t))$, are reflected by the following indicator:

$C(RM_k(t)) = C(SR) + C(ARL_k(t) - PRL_k)$
where:
$C(SR)$ – the costs associated with the resources;
$C(ARL_k(t) - PRL_k)$ – the costs associated with effects generated by the measures taken to counteract the risks.

Depending on the result of the expression $ARL_k(t) - PRL_k$ the following situations depicted in Table 3 can occur, describing an undulating effect of the cost function, $C(RM_k(t))$.

Table 3. Risk management costs

$\boldsymbol{C(SR)}$	$\boldsymbol{ARL_k(t) - PRL_k}$	$\boldsymbol{C(RM_k(t))}$
>0	>0	↑
>0	<0	↓
>0	=0	$\boldsymbol{C(SR)}$

The value of the cost function for the risk management process is getting bigger and lower as the costs associated with the effects generated by the security measures are positive or negative. A negative cost is characterized by a situation in which the effects of security resources applied to a set of collaborative processes counteract all risks identified for that system and more. If the actual value is equal to the planned level than no additional costs are recorded, and the final value of the $C(RM_k(t))$ indicator is equal with the costs associated with the security resources used in the process of security management.

6 Collaborative banking systems complexity

A key aspect of collaborative banking systems in relation with security risks is system complexity, which can be studied as a function of the number of components, the links between them, and the types of flows corresponding to each link. The challenges faced in management, the number and type of risks in banking systems are dependent on system complexity. In the following, the Halstead relative complexity function will be used for the study and comparison of different systems' complexity.
The Halstead complexity function for 3 variables is defined as *Halstead:* $\mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* \to [0, \infty)$:
$Halstead(x, y, z) = \log_2 x + \log_2 y + \log_2 z.$
The Halstead relative complexity function is derived from the previous function and is defined as $Hrel: \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^* \to [0,1)$:
$Hrel(x, y, z) = \frac{\log_2 x + \log_2 y + \log_2 z}{(x+y+z)\log_2(x+y+z)}$.

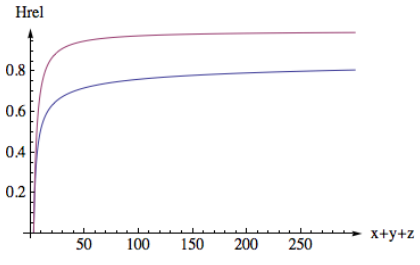

Fig. 4. *Hrel* minimum and maximum as a function of the sum of the variables

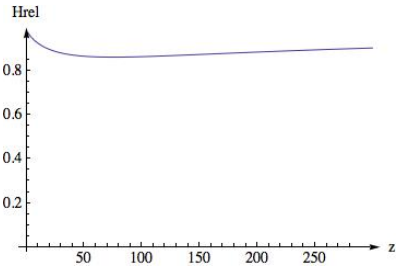

Fig. 5. x=1,y=100; minimum at z=75

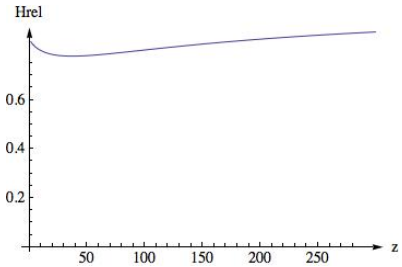

Fig. 6. x=y=50; minimum at z=37

If we keep x+y+z constant, and we vary x,y and z, the minimum point of *Hrel* is at x=y=z. We can see from Figure 4 that the value of the minimum of the function is increasing in relation with the variables' sum. In Figure 7, x+y+z=100, x and y vary between 1 and 98, while z is 100-x-y. The value of the function increases as we move

farther from the center point(x=y=z), and is influenced by the distance from the corners of the triangle (where the value of one variable is maximum, and the two other variables are 1). The function has the maximum value for the points: (98,1,1); (1,98,1); (1,1;98).

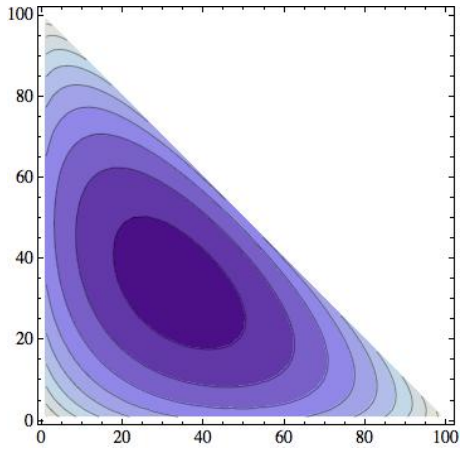

Fig. 7. Hrel values with x+y+z=100, as a function of x and y (lighter color, higher value)

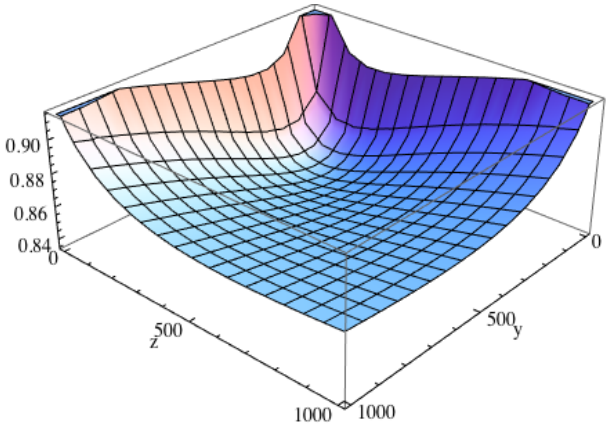

Fig. 8. *Hrel* for x=300;
min: 0.835289, for y=z=203
max: 0.992222, for x=300,y=1,z=1

Let x and y be constant, and z variable. We can see the simultaneous effect of the distance between variables and the sum of the values on the function value in figures 5 and 6. Because the function value is higher when we get close to the points where one variable has a high value, and the other 2 have low values, the minimum is nearer to the variable with the bigger size. The effect of the sum of the variables on the function value is obvious from figure 6: x=y=z=50 is the minimum point for sum=150, but the point that minimizes the function for x=y=50 is z=37. If x is constant and we vary y and z (Figure 8), the lowest point for x=300, is (300,203,203) which minimizes the distance between variables (y=z), and the size of the variables y=z<x.

Given the above properties, we can describe the behavior of the Halstead relative function as being dependent on 2 factors: the size of the variables, and the heterogeneity between the variables. The presence of the second factor (variable heterogeneity), aside with the fact that the codomain is [0,1) are the main aspects that differentiate the relative Halstead complexity function from the Halstead relative complexity function.

For the collaborative banking system Σ, we have S – the space, representing the set of locations; F:S×S→R, the work flows. Let C be the subset of S×S for which work flows are defined. C is the set of connections between the locations in S. Let H be the set of distinct values from F.

Based on the 3 sets, the following variables will be defined: s=|S|, c=|C|,h=|H|. Given the signification of s as number of spaces, c as number of connections between spaces, and h number of different communication types, we have the following inequalities: c≥s-1; h≤c. h is the communication heterogeneity indicator of the system. If we maintain c and s constant, the function is not monotonically increasing for the interval $h \in \mathbb{N}^* \cap [1, \max(s, c)]$ (figures 5 and 6). This can be explained by the fact that a small value of h typically implies that almost all the flow types are present on almost all the edges, which leads to a higher value of complexity. The *Hrel* value decreases as this flow concentration is reduced, and then increases again with as a result of the size of the variables and heterogeneity.

Σ is a collaborative bank system for which the following types of flows are defined:

1 – interbank fund transfers in the same currency
2 – interbank fund transfers in different currencies (Swift)
3 – interbank loans
4 – alternative communication channels (chat, telephony, e-mail)

Complexity will be studied from the point of view of one bank (in this case bank A), which may be present in more than one country, and its relations with other banks. The collaborative bank systems are represented as graphs, with edges representing connections between banks, and the types of flows which are present on a regular basis on that edge. The letters represent banks, and the numbers represent countries. A1 and A2 represent the same bank, from different countries, whereas B1 and C1 are different banks from the same country. Systems 1-4 are different configurations of interbank systems. The flow combinations 1,3,4; 2,3,4; 2,4; and 1,3 in the case of System Σ_1 are considered different.

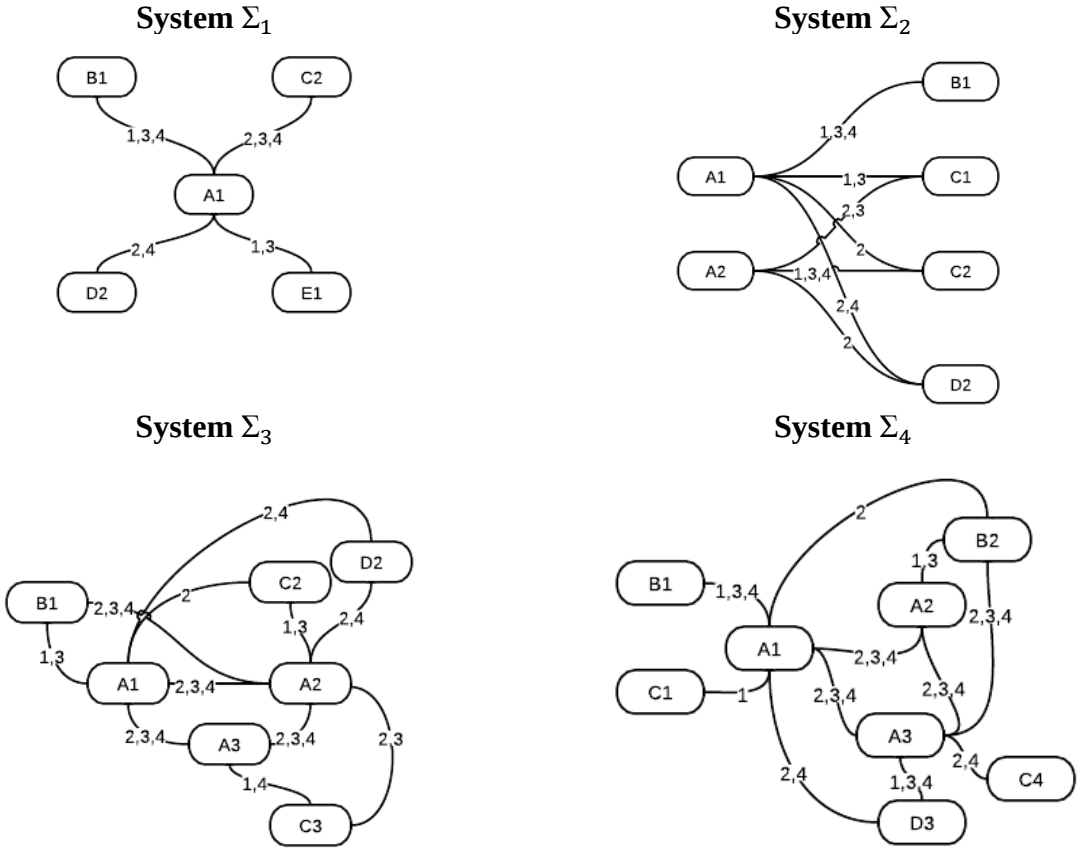

Fig. 9. Collaborative bank systems configurations

System Σ_1: |S|=5, |C|=4, h=4, *Hrel*(s,c,h) = 0.573937; *Halstead*(s,c,h)=24
System Σ_2: |S|=6, |C|=7, h=5, *Hrel*(s,c,h) = 0.623125; *Halstead*(s,c,h)=27.6096
System Σ_3: |S|=7, |C|=11, h=6, *Hrel*(s,c,h)= 0.665354; *Halstead*(s,c,h)= 73.215
System Σ_4: |S|=8, |C|=10, h=6, *Hrel*(s,c,h)= 0.660938; *Halstead*(s,c,h)= 72.7291

Figure 10 is the graphical representation of the *Hrel* function in relation with the 3 variables: s,c and h.

The analysis of the interbank relationships of bank A in the four configurations shows how the value of the Halstead relative complexity function varies with the system characteristics. The value of *Hrel* for the systems Σ_3, Σ_4 is bigger than the value for the systems Σ_1, Σ_2 because of the differences in the metrics of the system characteristics. *Hrel* for Σ_3 is bigger than for Σ_4 as a result of

the difference in the distance between variables: s=7,n=11 versus s=8; n=10; with p=6. For this 2 configurations, a slightly smaller system, with more connections has a bigger value of the *Hrel* function than one in which the number of spaces and the number of connections are closer to each other. A more centralized system has a bigger value for the Halstead relative complexity function than a similar, but decentralized system.

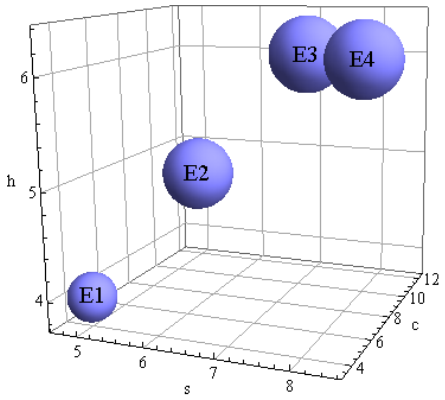

Fig. 10. Halstead relative complexity function values for the 4 systems

The Halstead complexity metric and the Halstead relative complexity metric summarize information about the system characteristics and allow us to compare between different systems configurations. These metrics can be used to analyze complexity at the level of the whole banking system, to study the correlation between complexity and security risks between the components of the banking system, and evaluate potential banking system or components configurations.

7 Conclusions

A risk management process is a complex operation that involves factors, of whose influence is almost always correlated. For this reason multifactor functions can depict the evolution of a set of variables, recording better values of the risk management process of collaborative processes in banking system. The costs associated, on the other hand, have the role to better characterize, and to rank systems between them, giving this perspective.

When talking about internal systems, like bookkeeping system, the greatest risk involves the people working with those systems, thereby it is important to have a tracking system for identifying who is initiating the transactions and the location from where the transactions are being made. Identifying what's actually happening into a system is the key to unlock the risks that can be inflicted upon it, and taking a correct and efficient set of measures to counteract those risks.

References

[1] W. Stanley Siebert and N. Zubanov, "Management Economics in a Large Retail Company," *Management Science*, No. 56, 2010, pp. 1398-1414.

[2] D. I. Levine and M. W. Toffel, "Quality Management and Job Quality: How the ISO 9001 Standard for Quality Management Systems Affects Employees and Employers," *Management Science*, No. 56, 2010, pp. 978-996.

[3] M. Cecchini, H. Aytug, G. J. Koehler and P. Pathak, "Detecting Management Fraud in Public Companies," *Management Science*, No. 56, 2010, pp. 1146-1160.

[4] X. Chen, X. Liu, X. Zhang, Z. Liu and G. Huang, "Service Encapsulation for Middleware Management Interfaces," *2010 Fifth IEEE International Symposium onService Oriented System Engineering (SOSE)*, 4-5 June 2010, pp. 272-279.

[5] L. Xue and L. Tian, "Research on Simulation Process Management for Product Development," *ISECS International Colloquium onComputing, Communication, Control, and Management, 2008, CCCM '08*, vol. 3, 3-4 Aug. 2008, pp. 33-36.

[6] I. Ivan, C. Ciurea, S. Pavel and M. Doinea, "Security of Collaborative Processes in Large Data Sets Applications," *The 5th International Conference on Applied Statistics*, November 19-20, 2010, NIS Publishing

House, Bucharest, Romania, ISSN 2069-2498.
[7] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems First Edition*, Wiley Computer Publishing 2001, pp. 3-32, ISBN 0-471-38922-6.
[8] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems Second Edition*, Wiley Computer Publishing 2008, pp. 313-363, ISBN 987-0-470-06852-6
[9] M. Doinea, *Optimizarea securității aplicațiilor informatice distribuite, PhD Thesis*, Academy of Economic Studies, 181 pg., Bucharest, Romania, 2011.
[10] C. Amancei, *Practical Methods for Information Security Risk Management*, Informatică Economică Journal, Vol. 15, No.1, 2011, pg. 151-159, ISSN 1453-1305.
[11] C. Ciurea, *Metricile sistemelor colaborative, PhD Thesis*, Academy of Economic Studies, Bucharest, Romania, 2011.
[12] C. Ciurea, "Techniques of Building and Validating Metrics for Collaborative Systems Applied in Economy," *Economy Informatics*, Vol. 11, No. 1/2011, INFOREC Publishing House, pp. 80-90, ISSN 1582-7941.
[13] I. Ivan and C. Ciurea, "Security of Collaborative Banking Systems," *Proceedings of the 4th International Conference on Security for Information Technology and Communications, SECITC'11*, November 17-18, 2011, Bucharest, Romania, ISBN 978-606-505-493-6.

Ion IVAN has graduated the Faculty of Economic Computation and Economic Cybernetics in 1970. He holds a PhD diploma in Economics from 1978 and he had gone through all didactic positions since 1970 when he joined the staff of the Bucharest Academy of Economic Studies, teaching assistant in 1970, senior lecturer in 1978, assistant professor in 1991 and full professor in 1993. Currently he is full Professor of Economic Informatics within the Department of Computer Science in Economics at Faculty of Cybernetics, Statistics and Economic Informatics from the Academy of Economic Studies. He is the author of more than 25 books and over 75 journal articles in the field of software quality management, software metrics and informatics audit. His work focuses on the analysis of quality of software applications.

Cristian CIUREA has a background in computer science and is interested in collaborative systems related issues. He has graduated the Faculty of Economic Cybernetics, Statistics and Informatics from the Bucharest Academy of Economic Studies in 2007. He has a master in Informatics Project Management (2010) and a PhD in Economic Informatics (2011) from the Academy of Economic Studies. Other fields of interest include software metrics, data structures, object oriented programming in C++, windows applications programming in C# and mobile devices programming in Java.

Mihai DOINEA has a PhD in the field of Economic Informatics, within Academy of Economic Studies, Bucharest, Romania. His PhD thesis approaches the field of Informatics Security, with clear objectives about finding security optimization methods in distributed applications. His research is also backed up by a master diploma in Informatics Security (2006). He is a lecturer assistant, teaching Data Structures and Advanced Programming Languages at the Academy of Economic Studies. He published more than 30 articles in collaboration or as single author and his research interests

are directed to areas such as security, distributed applications, artificial intelligence and optimization algorithms.

Arthur-Ervin AVRAMIEA has graduated the Faculty of Economic Cybernetics, Statistics and Informatics from the Bucharest Academy of Economic Studies in 2011. He currently works as a software developer for IBM. The present fields of interest are: computational neuroscience, artificial intelligence and parallel programming.