Risk assessment in disaster recovery strategies development

A. Galach
Polish-Japanese Institute of Information Technology, Warsaw, Poland

Z. Kotulski
Polish Academy of Sciences, Institute of Fundamental Technological Research, Warsaw, Poland &
Warsaw University of Technology, Faculty of Electronics and Information Technology, Warsaw, Poland

ABSTRACT: The paper describes the model for selecting disaster recovery strategies for information system. The risk assessment covers the threats and vulnerabilities related to the problem of losing the availability of information processes in the particular information system model. The analysis takes under consideration the relationships between the components of information system in order to find the risk of availability lost propagation within the system. That is the basis for finding the candidate disaster recovery strategies, which have to fulfil these basic requirements. Such an approach allows sifting these ones, which are basically not suitable for the security requirements of the information system. The preliminary accepted strategies are to be analyzed regarding to the estimated cost of implementation and maintenance. The next phase covers the detailed analysis of confidentiality and integrity risks in the candidate strategies. The level of risk related to the confidentiality and integrity of information processed in the disaster situation using given strategy is to be estimated.

1 INTRODUCTION

The business continuity management is recognized as the very important success factor for the nowadays organization. The need for planning the business operations in the disaster scenario, when there is a lack of some of basic resources availability, was recognized especially after September 11th, 2001. According the survey conducted in Australia during 1999 and 2000 (HB221 2003) 65% of business organizations and 71% of councils reported, that the acceptable downtime is shorter than 24 hours. That data can be extrapolated on the organization outside Australia as well, remembering, that the survey took place before the WTC disaster, so nowadays the awareness of the business continuity need may be much higher.

The contingency of business processes relies very strongly on the availability of information and the ability to process it. The information system is the bloodline of the nowadays enterprise, therefore the assurance of the system services availability is absolutely critical. The reported case of Omega Engineering (Gaudin 2000), where the disgruntled administrator destroyed the data stored in IT system leading to the $10 million loss and the layoff of 80 workers. It should be noted that these disaster caused the significant problem for the company, its employees and customers. It is hard to imagine what the impact could be caused by similar disaster in the information system supporting utilities or the SCADA system supporting powerplant steering.

The facts described above lead to the conclusion, that nearly every organization shall consider undertaking the activities increasing the abilities to survive the disaster situation. The result of these activities shall include implementation of the strategy allowing to continue business and recover the company from the disaster, as well as the plan describing what to do in the disaster situation to continue the critical processes and recover the company. Generally, the strategy describes the approach of the organization to the business continuity and recovery issue, while the plan precisely describes the activities, which shall be undertaken in the disaster situation. The plan depends very strongly on the strategy, therefore choosing and implementing the proper disaster recovery strategy is a vital part of business continuity management.

2 DISASTER RECOVERY STRATEGY

The aim of the disaster recovery strategy development and implementation is to assure that it will be possible to rebuild the ability of the organization to conduct processes if the disaster happens. Analysing the possible solutions for the disaster recovery strategies (Hiles 2004) the four basic options, presented on the diagram below, exist:

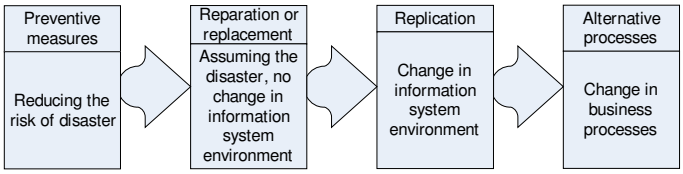

Figure 1. Relations between the approaches to the disaster recovery strategy.

Considering the disaster recovery strategies for information system the additional factor depicting the information protection requirements shall be analyzed. According the ISO/IEC 17799 standard (ISO 17799 2000) the data security consists of three elements: confidentiality, integrity and availability. Basically, the disaster recovery strategy assures the availability of information and the information processing. However, the strategy choice and further implementation shall assure the confidentiality and integrity of the information on the level, which is acceptable from the organization point of view.

3 MODELING THE SYSTEM AVAILABILITY

Further analysis of the disaster recovery strategy selection process requires defining the model of the information system availability, which could allow modelling the strategy. Such a model can be based on a reliability network concept (Dhillon 1999).

In the following part of the paper we will semi-formal define the serial, parallel and independent (being an extension of pure reliability network) elements of the network depicting the information system. Every unit of the network may depict the asset in the information system, as listed in (ISO 13335-3 1998).

Definition 1. Let us take the reliability network R for the given information system I. We say that two units U_1 and U_2 are serial and U_1 is over U_2 when A_2 can be available if A_1 is available where U_1 represents the asset A_1 and U_2 represents the asset A_2.

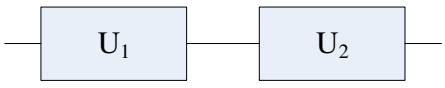

Figure 2. An example of serial units

Definition 2. Let us take the reliability network R for the given information system I. We say that two units U_1 and U_2 are parallel when the A_1 can be used instead of A_2 and vice versa where U_1 represents the asset A_1 and U_2 represents the asset A_2.

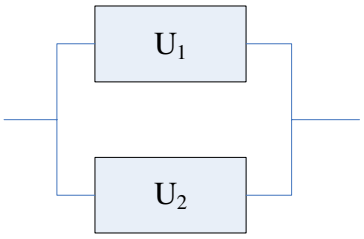

Figure 3. An example of parallel units

Definition 3. Let us take the reliability network R for the given information system I. We say that two units U_1 and U_2 are independent when they are neither serial nor parallel.

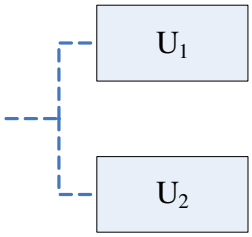

Figure 4. An example of independent units

The next issue would be to analyze the recovery time of the system depicted by the reliability network required in the case failure of the network unit. In the case of serial network $R_s=P(U_1 \ldots U_i \ldots U_n)$ the time for the network recovery $t_R(R_S) \leq \max\ t_R(U_i)$ where $i=1 \ldots n$, if the failure of the particular unit does not cause the failure of other unit.

Definition 4. Let us take the reliability network R for the given information system I. Let the network R consists of two units: U_1 and U_2. Let unit U_1 represent asset A_1 and unit U_2 represent asset A_2. Let U_1 and U_2 be serial and U_1 be over U_2. We say that U_1 propagates failure to U_2 if in a case of failure of A_1, the failure of A_2 occurs.

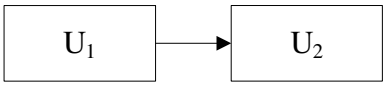

Figure 5. An example of failure propagation

Definition 5. Let us take the reliability network R for the given information system I. Let the network R include the unit U_1 representing asset A_1. We say that unit U_1 is confidentiality oriented if A_1 is either a safeguard protecting a confidentiality of information or includes safeguard protecting a confidentiality of information.

Definition 6. Let us take the reliability network R for the given information system I. Let the network R include the unit U_1 representing asset A_1. We say that unit U_1 is integrity oriented if A_1 is either a safeguard protecting integrity of information or includes safeguard-protecting integrity of information.

Definition 7. Let us take the reliability network R for the given information system I. Let the network R include the unit U_1 representing asset A_1. We say

that unit U_1 is information unit if A_1 is an information or set of data.

Definition 8. Let us take the reliability network R for the given information system I. Let the network R include the unit U_1 representing asset A_1. We say that unit U_1 is information processing unit if A_1 process the information.

Definition 9. Let us take the reliability network R for the given information system I. Let the network R include the unit U_1 representing asset A_1. We say that unit U_1 is supporting unit if A_1 is neither information nor set of data nor process the information.

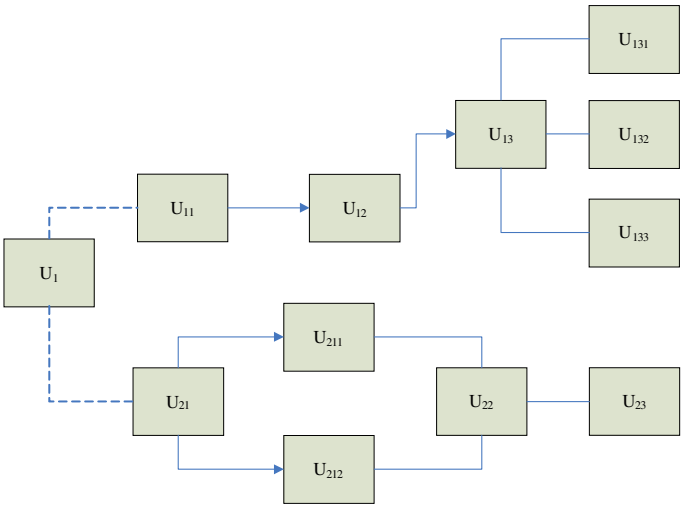

Figure 6. An example of more complex reliability network

4 MODELING THE DISASTER RECOVERY STRATEGY

The disaster recovery strategy describes the approach of the organization toward the recovery of the critical information processing in the disaster situation. The possible solutions within a disaster recovery strategy are described in chapter 2 of this paper. Here we consider how the model described in the previous chapter could be used to represent the disaster recovery strategy. If the strategy bases on the replication the reliability network could directly represent that as the parallel units.

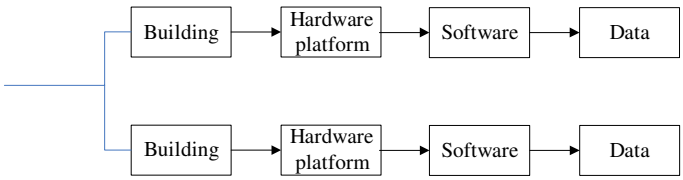

Figure 7. An example of replication strategy description

The replication, although the safest from the availability point of view, could lead to some risks, including:

- The situation, when the back-up infrastructure is not able to take over the tasks of the basic infrastructure
- The problem with data replication, leading to the lack of consistency, which makes the integrity loss
- The problem with confidentiality protection – the data shall be protected according the confidentiality requirements in the basic system as well as in the back-up system
- Another problem with confidentiality protection – the data has to be replicated, that makes the requirement of protecting the confidentiality of the data between the basic and backup infrastructure

If the replication strategy is taken under consideration the switching time between the basic system and the backup system shall be analyzed. It is also worth to note, that in our discussion we consider backup centre as dedicated to take over the tasks of basic infrastructure in a case of disaster. It not necessary has to be true: you can imagine the situation when the backup centre is in practice used in non-disaster situation for supporting some processes and, in a case of disaster, these processes are either suspended (and backup is used to support most important processes) or continued (and backup is used to support both groups of processes). That can have a significant impact on the performance of the whole system, however, that case will not be further analyzed in that paper.

Reparation or replacement as the disaster recovery strategy does not have a direct impact on the reliability network presenting the system. However, the following issues shall be analyzed

- The time required for the reparation or replacement
- The risk related to the reparation or replacement, describing the unsuccessful activity or the situation when the activity is not possible
- The risk related to the loss of confidentiality or integrity of information. That can be caused by various factors, including lack of competences, untrusted staff, etc.

Analyzing the reparation or replacement strategy from the availability point of view the time required for the reparation or replacement shall be considered.

Another strategy bases on the possibility of performing some business processes in other way. In fact, that means, that in the disaster situation another resources can be used to enable process performance. This strategy can be depicted as switching from one reliability network to the other reliability network, while some elements of both networks are common. Let us call the reliability network depicting the resources used in the non-disaster situation as the basic network and the resources used in the disaster situation as the alternative network.

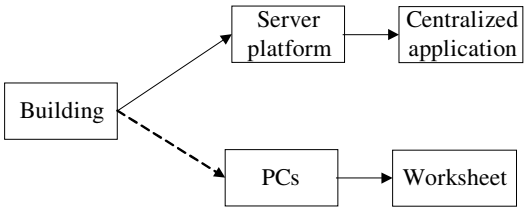

Figure 8. An example of basic and alternative network

This strategy can lead to some risks, including the following:

- The switching time between the basic infrastructure and alternative one can be not acceptable from the organization's point of view
- The alternative resources may not be able to take over the tasks of basic one in the disaster situation at all
- The data has to be replicated to the alternative resources, that can make additional problems with integrity, especially because the other platform is used
- As the provisional resources are used, the confidentiality safeguards may be much weaker than in case of basic resources - in fact the confidentiality protection may be not relevant to the requirements of the organization
- Some integrity assuring mechanisms present in the basic resources may be not present in the alternative ones (an example could be the relational database system, where the integrity is assured by built in mechanisms, which can be replaced in the disaster situation by worksheet personal application where the integrity assurance mechanisms are hardly comparable

The last approach to the disaster recovery strategy presented in the chapter 2 is using the preventive measures. They reduce the probability of the disaster, however considering them the following issues shall be analyzed:

- The impact of these measures on the system performance (it may appear, that, although the measures reduce the disaster probability, they have the negative impact on the system performance, and therefore are not acceptable from the availability point of view)
- The impact of these measures on the confidentiality and integrity of information – if this impact is negative and the level of confidentiality and/or integrity protection is below the acceptable one either another measure shall be considered or the additional one improving the confidentiality and/or integrity shall be implemented.

The issues initially described above include the problems related to the availability of the system services and information, confidentiality and integrity of data resources. However, the disaster recovery strategy selection shall take under consideration the cost of strategy implementation and maintenance. This could include:

- Solution analysis
- Implementation analysis
- Integration with the existing infrastructure
- Environment assurance
- Preparing business contingency plans basing on the selected strategy
- Training
- Data synchronization
- Technical components maintenance
- Monitoring and change management
- Upgrading

5 FINDING THE OPTIMAL DISASTER RECOVERY STRATEGY

The proposed method of finding the disaster recovery strategy for the given information system uses two stages of risk assessment process and the calculation of the cost of implementation and maintenance for the strategy. The strategy selection process can be therefore described in the following steps:

- Risk assessment stage 1 – stress on availability
- Cost assessment
- Risk assessment stage 2 – stress on confidentiality and integrity

Let us assume the information system I which is described by reliability network R. Due to the tasks performed by the system I it is assumed that maximal tolerable downtime for the system I is T.

Definition 10. Let us take the reliability network R for the given information system I. Let the network R include the unit U_1 representing asset A_1 which can be either repaired or replaced. The t_1 is the reparation time for unit U_1 if A_1 can be either repaired or replaced within a time not greater than t_1.

Definition 11. Let us take the reliability network R for the given information system I. Let the network R include the parallel units U_1 and U_2 representing assets A_1 and A_2. The $t_{1\to2}$ is the switching time if the A_2 can fully take over the tasks of A_1 in the time not exceeding $t_{1\to2}$.

Definition 12. Let us take the reliability network R for the given information system I. Let the network R include the unit U_1 representing the asset A_1. The p_1 is the downtime probability for the U_1 if the probability that A_1 is not working is p_1.

The aim is to find the availability requirements for the system I. In order to analyze such requirements we make the following assumptions:

- The reparation or replacement capabilities for any two assets are independent, what means that resources for reparation or replacement are not limited
- In the case of failure propagation, the time t_p between the failure of asset A_1 propagating the failure to asset A_2 and the failure of asset A_2 is such that $t_p \to 0$.

Now the availability for various information systems is analyzed.

Case 1. Pure serial network

The case which is analyzed at first is the situation when the network R representing the system I is the serial one. There are neither parallel units nor independent units in the network. We also assume there is no failure propagation in the network R. For every unit U in the network R the risk function F(p,t) is defined, where p is the downtime probability for unit U and t is the reparation time. If $F(p,t)>F_R$ where F_R is the acceptable availability loss risk level, than the disaster recovery strategy shall cover reducing the risk of availability loss of unit U or define the way of conducting processes such, that unit U is not required. Summing up, in a pure serial network the result of availability analysis in risk assessment stage 1 is the list of units for which the availability loss risk level is above the acceptable level.

Case 2. Serial network with failure propagation

This case covers the situation when at least one asset propagates the failure to at least one other asset. This can be described using the reliability network R. Let the unit U_m propagates the failure to units U_{sk} where $k\in\{1,..,n\}$. Let p_m is the downtime probability for the unit U_m, t_m is the reparation time for unit U_m, t_{sk} is the reparation time for unit U_{sk}. As in Case 1, the risk function F(p,t) is defined for every unit U, that is $F_m(p_m,t_m)$ for unit U_m and $F_{sk}(p_m,t_{sk})$ for unit U_{sk}. If

$$\max\{F_m(p_m,t_m), \max_{k=1}^{n}[F_{sk}(p_m,t_{sk})]\}>F_R,$$

where F_R is the acceptable availability loss risk level, than the disaster recovery strategy shall cover reducing the risk of availability loss of unit U_m or define the way of conducting processes such, that unit U_m is not required.

Some remarks regarding the reliability network with failure propagation shall be described here. The analysis presented above allows finding out if the given unit propagating the failure shall be covered by the disaster recovery strategy. Such an approach forces to review all units on which the failure is propagated; however that could be optimized in real life implementation. The another point is the fact that the formula presented above is the recursive one, which allows to find the units which must be covered by disaster recovery strategy, which are both the propagating ones and on which the failure is propagated.

The approach described above assumed it is sure that the failure of U_m causes the immediate failure of U_{sk}. However, such a situation does not have to happen. The value $p_{m,sk}$ can be defined as the probability of situation that unit U_m fails and unit U_{sk} fails as well. The condition $p_{m,sk}\le p_m$ is obvious. The formula presented above shall be changed to the form:

$$\max\{F_m(p_m,t_m), \max_{k=1}^{n}[F_{sk}(p_{m,sk},t_{sk})]\}>F_R.$$

Case 3. Parallel units

The parallel network case could be the most interesting one because it describes the situation of assets replication, which is quite often used as a basis for the disaster recovery strategy. The analysis shall cover the following issues:

- The time necessary for switching between the units (when the unit takes over the tasks of failed parallel one)
- The time required to process the information if one of the parallel units is failed
- The risk of failure of some or all parallel units (worst scenario)

Let the reliability network R represent an information system I. There are two parallel units U_1 and U_2 in the network. The unit U_2 is able to take over the tasks of U_1 within the switching time $t_{1\to2}$. If p_1 is the downtime probability for U_1, than the availability requirements are satisfied if $F_1(p_1,t_{1\to2})\le F_R$ where F_1 is the risk function for unit U_1 and F_R is an acceptable availability risk level. In other situation the disaster recovery strategy shall cover units U_1 and U_2. That condition may be extended to more complicated system, where the number of parallel units is present. Let the parallel units $U_1,\ldots,U_n$ be the components of reliability network R. The downtime probability $p_{1,\ldots,k}$ is the probability that units $U_1,\ldots,U_k$ fail, while within the switching time $t_{1,\ldots,k\to k+1,\ldots,n}$ the assets $A_{k+1,\ldots,n}$ represented by units $U_{k+1,\ldots,n}$ take over the tasks of the assets $A_{1,\ldots,k}$ represented by units $U_{1,\ldots,k}$. The availability requirements are satisfied if

$$\max_{i=1}^{k}[F_i(p_{1,\ldots,k},t_{1,\ldots,k\to k+1,\ldots,n})]\le F_R,$$

where F_i is the risk function for the unit U_i.

The analysis presented above does not take under consideration the performance of the assets. It is assumed that the taking over the tasks in a case of failure of an asset does not have a negative impact on information processing. Such a situation may appear if there is a backup asset "waiting" for a failure of a basic asset. This is presented on the following picture – in normal circumstances unit U_1 works while unit U_2 is a backup one "waiting" for a failure of U_1.

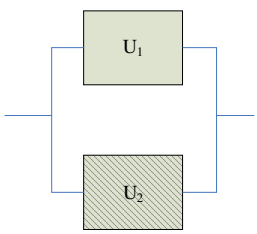

Figure 9. Basic and backup unit configuration

However, there could be a situation when the asset, in addition to its task, takes over the task of the failed asset. According to (PAS56 2003) such a situation can be described by

- Active/active model – there are some production sites (assets), each of the production site can be a backup for other production site
- Alternate site model – there is a backup site (asset) that periodically functions a primary site

Let the parallel information processing units $U_1,\ldots,U_n$ be the components of reliability network R. Let $t_{1,..,n}$ be the time required to perform given operation having assets represented by units $U_{1,\ldots,n}$, and $-\Delta t_{1,\ldots,k\Rightarrow k+1,\ldots,n}$ describe the negative impact on time required to perform given operation if assets represented by units $U_{k+1},\ldots,U_n$ takes over the tasks of the assets represented by units $U_1,\ldots,U_k$.

Analyzing the time requirements the backlog phenomenon shall be considered (HB221 2003). As the switching time $t_{1,..,k\rightarrow k+1,..,n} > 0$ there are some operations which should be performed within that switching time but have not been performed. These operations shall be performed after switching, which could cause an additional delay $-\Delta t^B_{1,\ldots,k\Rightarrow k+1,\ldots,n}$. If, due to the requirements analysis, given operation shall be performed within the maximal time T the following condition shall be satisfied:

$$T > t_{1,..,n} - \Delta t_{1,\ldots,k\Rightarrow k+1,\ldots,n} - \Delta t^B_{1,\ldots,k\Rightarrow k+1,\ldots,n} - t_{1,..,k\rightarrow k+1,..,n}$$

Case 4. Independent units

The reliability network containing the independent units can be transformed into the reliability networks without the independent units. Such networks can be analyzed according the availability requirements using the cases described above.

The risk function being the basis for availability requirements fulfilment evaluation can be tailored depending on the asset type and risk assessment methodology used. Generally that function shall fulfil two basic requirements:

- The value of function increases while the time being the argument of the function increases. That means that risk of losses caused by the lack of availability increases
- The value of function increases while the probability being the argument of the function increases. That means that the value of risk increases

The time of unavailability is proportional to the loss caused by unavailability; the proportion is typical for the given assets and that shall also be depicted in the risk function. The function can be used while the continuous values for probability and time are used, that is $p\in\langle 0,1\rangle$, $t\in R$, but also if the risk assessment is performed using the failure modes (Dhillon 1999), when the probability and time are discrete, that is $p\in P$, $t\in T$ and P, T are the sets containing the finite number of discrete values. The risk function can, in such a case, be based on models proposed in standards, like (ISO 13335-3 1998) or (AS/NZS 4360 2004). However, the models presented in standards use probability of the loss (or frequency of the loss) and the value of loss, so the relation between the downtime and the value of loss shall be found.

The discussion above covers the analysis of availability requirements – the aim was to find the components of the information systems, which availability is not high enough so they shall be covered by a disaster recovery strategy. The disaster recovery strategy could be depicted using the reliability networks.

Case 1. The reliability network preserves the structure.

This is the situation when the number of assets and the relations between assets are the same as before the disaster recovery strategy was implemented. However, the availability risk for the assets is reduced. It can be reached by decreasing the reparation time or replacing the assets by more reliable ones.

Definition 13. Let $F_1(p,t)$ be the risk function for the asset A_1 and $F_2(p,t)$ be the risk function for the asset A_2. Asset A_1 is more reliable than asset A_2 if $F_1(p,t)<F_2(p,t)$.

Case 2. The reliability network is changed.

This is the situation when either the assets are duplicated or some additional assets (eg. safeguards) are implemented.

Case 3. There is a reliability network in normal situation and another reliability network for the disaster situation.

This is the situation when some processes are performed alternatively in the disaster situation. The basic and alternative reliability networks describe the information system and the change during the disaster.

The preliminary set of disaster recovery strategies includes the reliability networks, which are the candidates for the network describing the final disaster recovery strategy. The networks shall fulfil the following requirements:

- The availability loss risks shall be smaller or equal to acceptable availability loss risk
- The time required for performing the given operation using an information system shall be smaller than maximal acceptable time
- The confidentiality protection shall be sustained
- The integrity protection shall be sustained

The first requirement is to be fulfilled by transforming the network R_1 to network R_2 changing the structure of the network or assets such that the availability risk is decreased to or below the acceptable risk level. The second requirement deals with the performance issue. The problem was already analyzed for the parallel units. The negative impact may

happen also when the assets are exchanged (more reliable assets are used) or if the safeguards are implemented. Let A_1' be the asset replacing the asset A_1, U_1' be the unit representing the asset A_1' and U_1 be the unit representing the asset A_1. Let U_1' and U_1 be information processing unit. Let T be the maximal time for performing the given operation by assets A_1' or A_1. If t_1' is the time required for performing the given operation by asset A_1' it is obvious that $T>t_1$' It may be also a situation when the asset has an impact on performance of another asset.

Definition 14. Let us take the reliability network R_1 for the given information system I_1 and the reliability network R_2 for the given information system I_2. Let the network R_1 contain unit U_1 being an information-processing unit and do not contain unit U_2. Let the network R_2 contain units U_1 and U_2. Let unit U_1 represent asset A_1 and unit U_2 represent asset A_2. We say that U_2 is an inhibitor for U_1 if the time required for performing the given operation for the asset A_1 in information system I_1 is $t_{1,\,in}$ information system I_2 is t_2 and $t_1<t_2$.

If the reliability network is changed – new units are added or the units are exchanged it shall be analyzed if any new unit U_1 is an inhibitor for any information processing unit U_2 and when it is it shall be assured that $t_2<T$, where T is maximal time acceptable for performing given operation and t_2 is the time required for performing given operation by the asset represented by the unit U_2.

The preliminary disaster recovery strategy selection shall take under consideration also the some issues related to confidentiality and integrity.

Definition 15. Let us take the reliability network R_1 for the given information system I_1 and the reliability network R_1' for the information system I_1'. The information system I_1' emerged as the result of implementation of given disaster recovery strategy into the information system I_1. Let the network R_1 contain unit U_1 and the network R_1' contain units U_1'. Let unit U_1 represent asset A_1 and unit U_1' represent asset A_1'. The asset A_1' emerged as a result of implementing disaster recovery strategy on asset A_1. We say that U_1' is the transformation of U_1 by the given disaster recovery strategy.

Let unit U_1 in the given reliability network R is the confidentiality oriented. R' is the reliability network depicting the information system after the disaster recovery strategy implementation. Unit U_1' being the transformation of U_1 in R' shall be confidentiality oriented as well. That assures that assets in the transformed information systems still protect the confidentiality of information. It may happen the replication approach is used. Unit U_1 is transformed to the number of units $U_1^{(1)}\ldots U_1^{(n)}$. Every unit $U_1^{(i)}$ where $i\in\{1,\ldots,n\}$ shall be the confidentiality oriented unit. The same approach shall be used in the case of integrity protection. The problem how strong the confidentiality and integrity is protected is analyzed more precisely in the second phase of risk assessment.

The next phase of the selection process covers the analysis of the cost requirements. As described in chapter 4 the cost of disaster recovery strategy covers both the implementation as well as further maintenance. The following conditions have to be fulfilled:

$$B > C_A + C_I + C_O$$

$$B_A > C_M + C_{OM}$$

where

- B – budget dedicated for disaster recovery strategy implementation
- C_A – cost of analytical work
- C_I – cost of technical implementation
- C_O – cost of organizational implementation
- B_A – annual budget for the strategy maintenance
- C_M – annual cost for the technical maintenance
- C_O – annual cost for the organizational maintenance

The cost of the disaster recovery strategy is proportional to the assured level of availability. It may appear that the strategies fulfilling the availability requirements are too expensive – that forces the return to the previous analysis phase with the relaxed requirements for the availability. That approach is based on a modified waterfall model (Krutz et al. 2001).

The third phase of the selection process deals with the specific requirements of the information system – the confidentiality and integrity protection.

Let us take the reliability network R representing the given information system I. Let U_I be the information unit in the network R. We define the confidentiality risk function $F_{CI}(R)$ for the given information unit U_I. The function $F_{CI}(R)$ shall possess the following capabilities:

- It shall be considered the threat related to any unit in network R if it has an impact on the confidentiality of information represented by U_I
- It shall be considered the confidentiality safeguard capabilities of any unit in network R if it reduces the probability of exploiting the threat related, directly or indirectly, to unit U_I
- If the unit U_I is replicated it shall be considered the impact of replication on the information confidentiality
- The relation between various threats and relation between various safeguard shall be considered

The first point can be analyzed using recursive approach. The list of threats is created for given unit (initially U_I) and all units being over that unit.

The next point is to analyze the confidentiality protection. In order to find the level of protection only the confidentiality-oriented units are to be taken under consideration. The recursive approach has to

be used again. However, the units, which are not confidentiality oriented, may be dropped. The following formula for estimating probability of exploiting given threat T having impact on the unit U_I is suggested:

$$E_T(U_I) = \max_{i=1}^{n}[E_T(U_i)]$$

$$E_T(U_i) = \min\{\varepsilon_T(U_i), \max_{j=1}^{m}[E_T(U_j)]\}$$

where:

$E_T(U_I)$ – probability of loosing confidentiality of information asset represented by U_I as a result of occurring threat T

$E_T(U_i)$ – probability, that neither U_i nor any unit being over U_i does not protect against threat T

$\varepsilon_T(U_i)$ – probability, that unit U_i does not protect against threat T

If the information asset U_I is replicated some confidentiality problems related to the synchronization process may appear. Depending on reliability network model they may be addressed in the analysis already described above, but may also require additional attention.

There may be more complicated relations between threats or relations between safeguards. Such relations may be depicted using tools like fault trees analysis (Fullwood et. al 1988) or the model presented in OORAM - Object-Oriented Risk Assessment Model (Galach 2002).

The similar approach as presented above may be used for integrity risk assessment. After the confidentiality and integrity risk assessment the value of confidentiality risk function $F_{CI}(R)$ and integrity risk function $F_{II}(R)$ is known. They shall fulfil the following requirements

$F_{CI}(R)<R_{CI}$
$F_{II}(R)<R_{II}$

where R_{CI} is an acceptable confidentiality risk level for the given information, while R_{II} is an acceptable integrity risk level for the given information.

6 SELECTING THE STRATEGY FOR THE SCADA SYSTEM

The SCADA systems play a significant role as a lifeline infrastructure steering component. The availability requirements for such a system are obviously very high. The integrity assurance is required in order to allow the proper work of the system. The confidentiality of the information is still required as well. According to (Stamp et al 2003) the cyber attack is the serious threat for the SCADA system. Beside the implemented safeguards the disaster recovery strategy shall be implemented in order to assure the sustain work of the system. The approach presented in this paper allows finding the disaster recovery strategy for such a system. Some features make selecting of the strategy easier, e.g.:

- Reliability network allows to model the complex relation within the SCADA system as well as the interfaces to the non-IT components
- Defining availability requirements separately for the information assets allows to model different requirements for various information starting from the real time processing up to the archive
- Confidentiality and integrity risk assessment covers only the elements which have the real impact on the information protection – this can be very useful in the case of SCADA being on the border between the IT and automation.

The reliability network schema for the real SCADA system may be very complex, however, the presented approach can improve the disaster recovery strategy selection process.

REFERENCES

AS/NZS 4360 2004. Risk management. Sydney: Standards Australia International

Dhillon, B.S.1999. Design reliability. Boca Raton: CRC Press

Fullwood, R. & Hall, R. 1988. Probability risk assessment in the nuclear powed industry. Oxford: Pergamon.

Galach, A. 2002. Object-oriented risk assessment model. *Information Systems Solutions Europe 2002*

Gaudin, S. 2000. Case study of insider sabotage: the Tim Lloyd/Omega case. *Computer Security Journal* vol XVI number 3:1-9

HB221 2003. Business continuity management. Sydney: Standards Australia International

Hiles, A.. 2004. Business continuity: best practices. Brookfield:Rothstein

ISO 13335-3 1998 Information technology – guidelines for the management of IT security. Part 3: Techniques for the management of IT security.

ISO 17799 2000. Information technology – code of practice for information security management.

Krutz, R. L. & Russell, D.V. 2001. The CISSP prep guide. New York:John Wiley & Sons

PAS56 2003. Guide to business continuity management.

Stamp et al. 2003. Sustainable security for infrastructure SCADA. Albuquerque:Sandia National Laboratories