# 22

# Design Criteria to Classified Information Systems Numerically

TEEMUPEKKA VIRTANEN
*Helsinki University of Technology, FInland*
*Telecommunications Software and Multimedia Laboratory*
*P.O. Box 5400, Fin-02015 HUT, Finland*
*teemupekka.virtanen@hut.fi*

Key words: security, classification, evaluation

Abstract: Constant changes in the structure of the organization and the working processes have forces security staff to reclassify and re-evaluate information and information systems too often. In this paper we present one solution to make it possible to use the previous data as much as possible and recalculate the evaluation results automatically.
The solution is based on piercing the processes into parts of the block diagram and then analyzing the classification of the each block. This procedure is continued from top to down until there is no remarkable processes left. After the top-down phase has been reached its end a second phase is started from bottom to top. In this phase the reliability of each block is analyzed and the results of one level is combined. This result is then passed to the upper level and this procedure may continue until the top is reached.
In every level it is possible to have iterative loops if the requirements are not met. It is usually easier to add parallel processes for assurance than improve the reliability of the single component.

## 1. INTRODUCTION

The classification of computer systems have been described in a qualitative way [Tryfonas] that promotes availability because it has attracted the less attention than the other parts of CIA-model triplet (confidentiality and integrity).

There have also been papers that describe availability using the techniques from availability engineering [Lyu]. Many of these assume information systems as a single system or focuses on the reliability of the software [Herrmann], [Leveson], [Kapur]. Information system is, however, an information handling process that may require several attendants and manipulating systems [Kiountouzis]. The information may have a working flow that directs some parts of the information to one department and the rest to another [Smith].

Availability in the information security differs from the reliability in engineering in the sense that in the reliability engineering everything is statistical. In the availability systems are often targets for the attacks and therefore statistical approach is often useless. Information systems may be considered as open systems [Leveson], as they communicate with their environment in a flexible way. This kind of system is often unstable instead of the stable systems where the communication with the world is reduced and formal.

There are however several advantages to use numerical methods. There must be some policies to establish the connection between numbers and the real life but using numbers it is easier to use computers and automatic procedures to handle the information. There are however few methods to describe the other areas than availability with numerical methods [Jønsang].

The delegation and outsourcing have been became popular ways to organize the work of the organization. This requires a proper way to pass the classification of the information and procedures with the delegation. There are often in the each level possibility to organize the work of its own. For the verification there has to be a method to pass the result of the security analyze to the superior level and summarize them.

## 2. NUMERICAL CLASSIFICATION METHOD

### 2.1 Top Down system classification

A classification is a part of business management. In a top level has to be known which processes are the important ones for the organization. In a highest level this may set the standards for the division of the organization saying what is the meaning of the division to the company and what are the remarkable products of the corporate.

In the next level the head of the division has to classify the business processes that are essentials to achieve the goals of the division. This process

may continue until the bottom level is reached or there is another termination rule.

In the classification all the aspects of information has to be notified. In approach like this the availability is a natural aspect but in the same time a higher level has to determine the confidentiality and integrity class of the information it gives to the lower level to be processed.

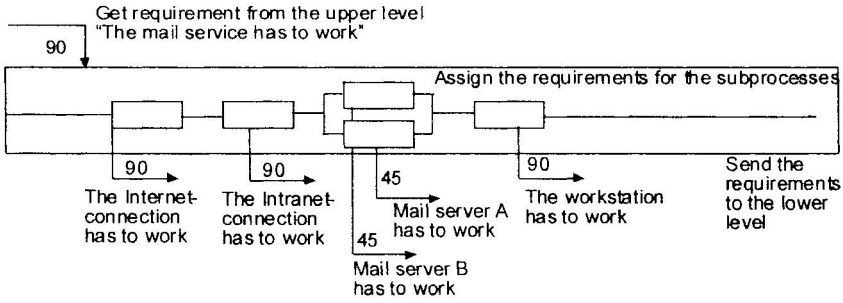


Figure 1. The classification process

The subordinates (lower level) get these classifications as an order. If they like to receive the information they need, there must be proper security methods to handle the information. In the same way a client (upper level) sets the availability standards and requirements for the quality of the information.

## 2.2 Bottom up system evaluation

The requirements are set from top to bottom. The results of the evaluation processes go from bottom to top. In every level the results of its subprocesses are combined and the result is then delivered to the superior level.

In the lowest level the evaluation may check the reliability of certain components or devices. In the upper levels the result of the evaluation is typically information that is summarized from results of the subprocesses and the subresults. This means that the hard work is done in the bottom level. All the evaluation information in the upper level is already numerical and easy to recalculate if needed.

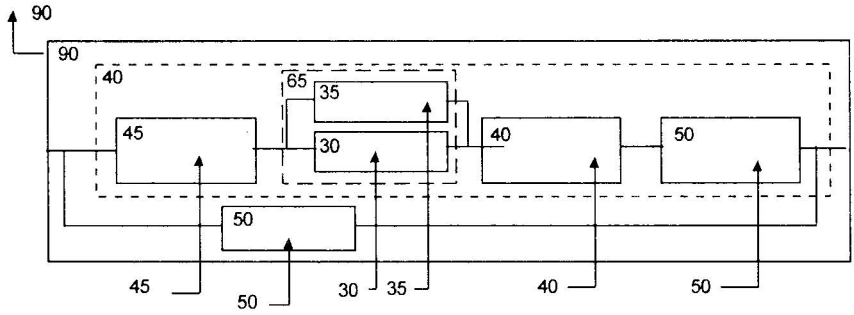


Figure 2. availability evaluation

In every level the results have to be compared with the classification. If the results don't meet the classification, there has to be an attempt to correct situation. This may happen either requesting the lower level to make it's result better or adding redundancy by reorganizing the work flow and adding some parallel subprocesses..

## 3. AVAILABILITY

In this paper availability is the probability that a process will produce its result in the designed time. The scale is 0-100 where 0 means that process will never succeed in time and 100 means totally always. We understand that there are other possible definitions. Especially the delay is also important. We have to assume that a process with high probability have also very short delay those cases it misses the designed time.

The required classes and their limits are defined in the information security policy of the company. One may for example define that there are four classes: top important (100-80), important (80-60), useful (60-40) and no requirements (40-0). In this definition a process that is classified as a top important must succeed to produce it's output in defined time four times out of five. In the policy there might also be defined a lowest level for the classification and evaluation. In the previous example the natural lower limit is 40 because systems below this level are considered useless or at least there are no requirements for systems below that.

In the classification procedure every piece of process gets an availability requirement from its superior process. That is the goal this process has to fulfill. This procedure takes automatically account of the business processes because the requirements come from the top. That means the more important a process is for business the higher requirements should be set for it.

In the next step the process has to be analyzed and divided to the subprocesses. These subprocesses may follow each other when they are said to be in series or they may be alternatives when they are said to be parallel. This analysis produces a block diagram where are the subprocesses and their connections.

Each subprocesses must be classified. Each subprocess in a series must have the same classification and that must be the same as is required for a whole block. If there are subprocesses or blocks in parallel, they must have classification where the original requirement is divided with a number of parallel blocks. In some cases this automatic procedure is not practical. If one of the parallel processes is the most profitable choice and the other are the more expensive backups it is reasonable to set the higher requirements for this alternative than the others.

When each subprocess has the classification, it is passed to the subprocess that means the classification steps one level downwards. This procedure is repeated until the classification of the subprocesses reach the termination level that means the lower processes are not significant.

In the second phase the evaluation is performed from bottom to top. In each level the availability of it's subprocesses are measured using the same scale as in the requirements. In the lowest level this may be the reliability of the processing equipment and in the upper level it is the results of the lower level.

The results are put in the block diagram that describes the process and the evaluation of the process is summarized using the same formulas as in the requirement phase. The result is the evaluated availability of the process and is compared with the requirement. If the result does not meet the requirement, corrective measures have to be started.

There are two ways of improving the availability. One can improve the reliability of the subprocess or add parallel subprocesses. The improving means that a new higher requirement is sent to the lower processes and those have to make their arrangements to meet these new requirements. Adding new parallel subprocesses means that the requirements for each parallel subprocesses will be lower.

It is easy to see that it is overall much more easier to add some additional procedures for the situation the main process is not available. The parallel availability is much more efficient that trying make single process more reliable.

## 4. INTEGRITY

For the integrity the basic procedure is the same as for the availability. Each level gets the requirements from the upper level, analyzes the graph of its own functionality and makes a block diagram of it's subprocesses. An integrity requirement is then assigned to each of these subprocesses and passed to the lower level.

After the termination point has been reached the evaluation starts and produces an integrity level that is passed to the upper level. If the criteria do not meet, the corrective measures will be started.

In this paper the integrity means the quality of the information. The integrity is high if the information was correct in the beginning and the correctness of the information was ensured during the processing so that it is correct in the end of the processing. The integrity decreases always when the original information is changed. If there is proper assurance for the changes to be correct the integrity doesn't decrease.

The classes and their definition are defined in the information security policy of the organization. They might be for example high integrity (100-70), normal integrity (70-40) and no requirements (40-0). There are no clear correspondence between this number and the real life like in the availability case.

In the block diagram subprocesses in series means steps that handles information straightforward and in the parallel subprocesses the information are cross-checked. Thus the serial coupling decreases the integrity and the parallel coupling increases the integrity. The processes that are read-only don't change the integrity of the data.

## 5. CONFIDENTIALITY

For the confidentiality the basic procedure is the same as for the availability and integrity. Each level gets the requirements from the upper level, analyzes the graph of it's own functionality and makes a block diagram of it's subprocesses. A confidentiality requirement is then assigned to each of these subprocesses and passed to the lower level.

After the termination point has been reached the evaluation starts and produces a confidentiality level that is passed to the upper level. If the criteria do not meet, the corrective measures will be started.

In this paper the confidentiality means the secrecy of the information. The requirements for the systems are based on the confidentiality of the information the system processes. The secrecy is based on the fact how much damage it is caused if the information is came public to unauthorized

people. This amount of damage may be based on the loss of money or time to correct the situation with new information.

The classes and their definition are defined in the information security policy of the organization. They might be for example top secret (100-80), secret (80-60), confidential (60-30) and unclassified (30-0).

When the block diagram is made one has to concentrate the information that is required to pass to the subprocess as an input. If the subprocess requires the information it has to be authorized to receive it. This authorization is achieved by setting the confidentiality requirements for the subprocess.

The confidentiality of the information may be decreased by dividing it into pieces. The part of the information is often less confidential as the whole information. There are two ways of decreasing the amount of the information in one single point. One may decrease the amount of the information, for example records in the database, or quality of the information, for example fields in the database.

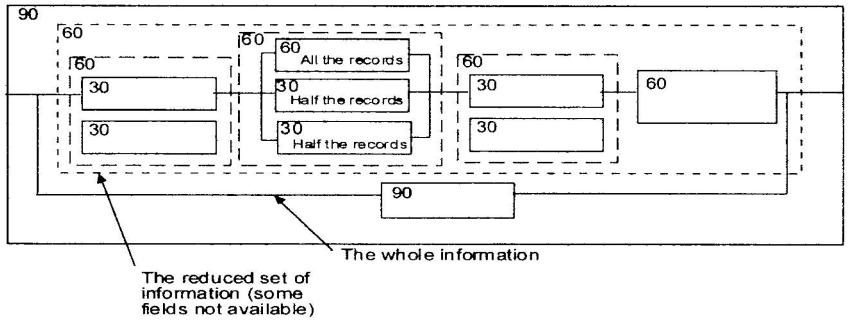


Figure 3. Confidentiality classification

In the block diagram subprocesses following each other means that they use the same information and thus must have a same confidentiality classification. If the information is the same that comes from the upper level, the classification must be the same as the whole process classification. If the information is divided into smaller units then the classification of the subprocesses must correspond the amount of information they receive.

One has to notice that the classification process requires intelligence. This means that somebody has to make the block diagram and set the classification. After this work has been done it is possible to use the information automatically by computers to recalculate the results. It is also

possible to redefine one piece of diagram and recalculate the whole result without any other changes.

## 6. THE ADVANTAGES OF THE NEW METHOD

The new model is designed for the modern business organization. An upper part of the organization may assign goals to its subordinates and delegate the decisions and resources needed to fulfill the goals to the subordinates. This model clarifies the goals of the security function so that it may also be delegated to the subordinate. The lower level may organize it's own processes in a way it can fulfill the requirements.

In this model the classification and evaluation of the security is hided in the black boxes of the subprocesses. The upper level doesn't have to know how the results are achieved. It has to trust the lower level.

When the classification and the requirements are clear it is possible to outsource the parts of the processes. The information and service level between the organizations are clarified and classified.

The new model makes it possible to program all the processes and their relationship into a database and automatically calculate the security level of the organization. When the block diagrams are in the database, all the modifications are local and the whole database can be easily recalculated. The changes are local and they affect only local diagram. The changes of the numerical values are summarized automatic.

The department level it is easy to manage the situation. The requirements are defined in the upper level and the results of the evaluation are collected from the lower level. Both requirements and results are in the common form and there are defined functions to produce them.

## 7. CONCLUSION

The new organization structures causes problems for the classification and evaluation processes because all the changes requires reclassification and re-evaluation. The new method described in this article makes it possible to reorganize the processes with local changes and automatic recalculation.

For the calculation the classification and the evaluation have to be numerized. We present one possible methods for this. This classification and evaluation are carried out in the basically same way. The exact numeral values and their explanations have to be described in the security policy of the corporation.

The delegation and outsourcing of the processes are easy when the interface is clear. The subordinate may arrange its work independently as long as it meets the requirements.

The results of the evaluation may be improved using two methods. Either one has to improve the reliability of the single component (device or subprocess) or one has to decrease the importance of the component by adding a parallel process for assurance. One level may add these parallel processes independently from other parts of the organization.

## 8. REFERENCES

[Herrmann] Herrmann D.S: ”Software Safety and Reliability”, IEEE Computer Society Press, USA 1999, ISBN 0-7695-0299-7

[Jønsang] Jønsang, A., Knapskog, S.J.:”A Metric for trusted systems”, Proceedings of the IFIP SEC 1998, Chapman & Hall, UK I998

[Kapur] Kapur P.K., Garg R.B, Kumar S: “Contributions to Hardware and Software Reliability”, World Scientific Publishing Co. Pte. Ltd, Singapore 1999, ISBN 981-02-3751-0

[Kiountouzis] Kiountouzis, E.A., Kokolakis, S.A.:”An analyst’s view of IS security”, Information Systems Security (IFIP SEC 1996), Chapman & Hall, UK 1996, ISBN 0 412 78120 4 [Tryfonas] Tryfonas T, Gritzalis D, Kokolakis S: “A Qualitative Approach to Information Availability”, Information Security for Global Information Infrastructures (IFIP SEC 2000), Kluwer Academic Publisher, the Netherlands 2000, ISBN 0 7923 7914 4

[Leveson] Leveson N.G: ”Safeware – System Safety and Computers”, Addison-Wesley Publishing Company, USA 1995, ISBN 0-201-11972-2

[Lyu] Lyu M: “Handbook of software reliability engineering”, McGraw-Hill, 1996

[Smith] Smith, E., Eloff, J.H.P: “Modelling risks in health-care institution”, Proceedings of the IFIP SEC 1998, Chapman & Hall, UK 1998