A Review of Research on Risk Analysis Methods for IT Systems

Conference Paper · April 2013

DOI: 10.1145/2460999.2461013

CITATIONS
20

READS
1,045

3 authors, including:

Sardar Muhammad Sulaman
Lund University
18 PUBLICATIONS **112** CITATIONS
SEE PROFILE

Martin Höst
Lund University
108 PUBLICATIONS **9,337** CITATIONS
SEE PROFILE

A Review of Research on Risk Analysis Methods for IT Systems

Sardar Muhammad Sulaman, Kim Weyns, and Martin Höst
Department of Computer Science, Lund University, Sweden.
(sardar, kim.weyns, martin.host)@cs.lth.se

ABSTRACT

Context: At the same time as our dependence on IT systems increases, the number of reports of problems caused by failures of critical IT systems has also increased. This means that there is a need for risk analysis in the development of this kind of systems. Risk analysis of technical systems has a long history in mechanical and electrical engineering.

Objective: Even if a number of methods for risk analysis of technical systems exist, the failure behaviour of information systems is typically very different from mechanical systems. Therefore, risk analysis of IT systems requires different risk analysis techniques, or at least adaptations of traditional approaches. This means that there is a need to understand what types of methods are available for IT systems and what research that has been conducted on these methods.

Method: In this paper we present a systematic mapping study on risk analysis for information systems. 1086 unique papers were identified in a database search and 57 papers were identified as relevant for this study. These papers were classified based on 5 different criteria.

Results: This classification, for example, shows that most of the discussed risk analysis methods are qualitative and not quantitative and that most of the risk analysis methods that are presented in these papers are developed for IT systems in general and not for specific types of IT system, like e-government systems.

Conclusions: The results show that many new risk analysis methods have been proposed in the last decade but even more that there is a need for more empirical evaluations of the different risk analysis methods. Many papers were identified that propose new risk analysis methods, but few papers discuss a systematic evaluation of these methods or a comparison of different methods based on empirical data.

Keywords

Risk Analysis, IT systems, Mapping study

1. INTRODUCTION

IT systems have become an essential part of our modern society. This evolution has not only created new opportunities, but also new threats to our society. The presence of IT systems everywhere has made us dependent on IT systems for our daily life. This is the case both for individuals and organisations, both private as well as public organisations. However, at the same time as the usage of, and dependence on, IT systems increases, the number of reports of problems caused by failures of critical IT systems has also increased [18].

One of the common aspects of these failures is the faith in systems that are not sufficiently dependable. The core of the problem is not that these systems suddenly become unreliable, but that we have become critically dependent on a wide variety of systems without analysing whether they are dependable enough and what the consequences could be of a possible failure [18]. To prevent critical systems from causing problems for the organisations dependent on them, risk analysis is a necessary activity.

Risk analysis of technical systems has a long history in mechanical and electrical engineering where many well-established methods exist. The failure behaviour of IT systems is typically different from mechanical systems and, at the same time, the complexity can be significantly higher. The high rate at which new IT systems are being developed and updated for many critical applications usually means there is not enough historical data available for a strictly statistical analysis of the reliability of each system and its components, as is sometimes the case in risk analysis of mechanical systems.

For all these reasons, risk analysis of IT systems requires different risk analysis techniques or at least adaptations of these traditional risk analysis approaches. In this article we present a systematic overview of previously published research on risk analysis for IT systems.

Risk analysis can be performed during the development of the system, at deployment of the system or at any time afterwards. In the ideal situation, the risk analysis should be re-evaluated each time major changes occur in the system or in the environment in which the system is used.

In this article we present an overview of operational risk analysis methods for IT systems. This includes many dif-

ferent types of systems and methods, but does not include project risk analysis methods, used to analyses the project management risks in software development projects.

Section 2 presents related work in the field of risk analysis and systematic literature reviews. Section 3 discusses the methodology used in this study in detail. Next, Section 5 contains the results of this mapping study and presents the categorization of the identified articles based on different attributes of the research and the risk analysis methods presented in each article. Finally, Section 6 summarizes and analyses the results of this classification.

2. RELATED WORK

Many different national and international high-level frameworks exist for information technology risk management and assessment. Such frameworks have for example been published by the International Organization for Standardization (ISO), such as ISO/IEC 27005 [7] and ISO/IEC 27002 [6], by national governmental organisations, such as the National Institute of Standards and Technology (NIST) [21] or the British Central Communication and Telecommunication Agency (CCTA) [5], by non-governmental organisations such as Club de la Sécurité de l'Information Français (CLUSIF) [16] or by research institutes such as the Carnegie Mellon Software Engineering Institute (SEI) [1]. A detailed comparison of some of these frameworks can for example be found in [3] and [22].

There also exist a number of low-level risk analysis methods for technical systems in general or for IT-systems in particular. Some of the most well-known methods are Fault Tree Analysis (FTA) [4], Failure Mode and Effect Analysis (FMEA) [15] and Hazard and operability study (HAZOP) [19]. Some of the frameworks mentioned above specifically recommend one or more of these risk analysis methods.

The goal of the study presented in this article is to identify research articles that describe or evaluate new or established risk analysis methods for IT systems, which includes both high- and low-level methods. To identify and categorize these research articles this study uses the methodology of mapping studies [11], which is a variation of systematic literature reviews [12].

Systematic literature reviews and mapping studies have been conducted in different studies [10] in widely different areas such as cost estimation (e.g. [8]), open source software (e.g. [20]), and testing (e.g. [2]). Two systematic reviews, [14] and [9], have focused on project risk assessment in software development projects. However, to the best of our knowledge, no reviews have looked specifically at operational risk analysis methods for IT systems.

3. METHODOLOGY

This article presents a study of available risk analysis, assessment, and management methods for IT systems. The review presented here is a systematic mapping study, conducted based on the guidelines presented in [12]. This article presents, in addition to the overview of the identified risk analysis methods, a categorization of the identified methods.

A review protocol was developed in the initial phase of the review. It contains research background, research questions, search strategy, study selection criteria and procedures, validity assessment, data extraction instructions, and data synthesis strategies.

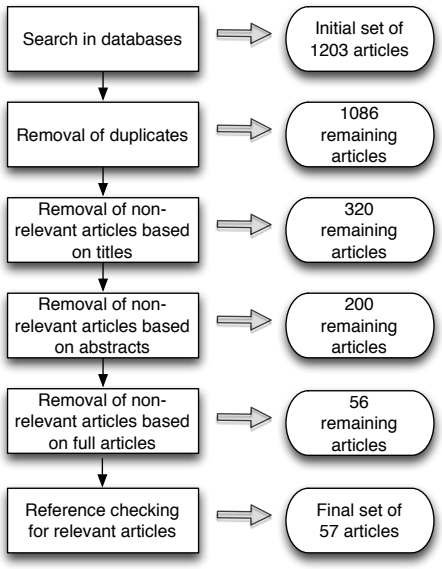

Figure 1: Identification and selection of articles.

This research is conducted as a planned study and was carried out in the following steps:

1. Defining the research questions.
2. Selection of sources to be searched for relevant articles.
3. Defining the search query and performing the search on the selected sources, resulting in 1203 articles.
4. Removing 117 duplicate articles by using EndNote reference manager and by manual search.
5. Defining the inclusion and exclusion criteria and initial selection based on titles and keywords according to the defined criteria, leaving 320 articles for the next steps of the study.
6. Second round of selection by reading abstracts according to the same criteria and first classification of the articles, leaving 200 articles for the next steps of the study.
7. Final selection of articles based on careful reading of the full text of each articles, resulting in a final list of 57 relevant articles for this study.
8. Analysis of the results of the classification of the final list of articles.

During each step special measures were taken to improve the validity of the research. Each step is described in more detail in the following subsections.

The steps involved in the identification and selection of articles are summarized in Figure 1.

3.1 Research questions

The objective of this article is, as described above, to present an overview of risk analysis methods for IT systems, by summarizing and synthesizing the results from research that has already been carried out on available risk analysis methods for IT systems. This general goal has been broken down to the following main research questions:

1. What risk analysis methods and approaches are reported in the research literature for IT-systems?
2. To what extent are the identified methods used in practice?
3. Is there empirical research published where the identified methods are evaluated/compared/etc.? If there is, which research methodologies are used?
4. Which phases of the risk management process have been the focus of the identified research articles?
5. What type of risk analysis methods are presented in the published research, qualitative or quantitative?

This research can be categorized as a systematic mapping study that is carried out in the same way as a systematic review. It focuses on the main research that has been conducted in the area of risk analysis for IT systems, and it is done by adopting a systematic approach to identify relevant research and classify the identified research articles according to predefined categories.

3.2 Search strategy

Searched resources

The following databases were searched (through Engineering Village[1]) for relevant research:

- INSPEC: This database is provided by Elsevier Engineering Information Inc. and the Institute of Electrical Engineers (IEE). It includes articles from 1969 to present.
- COMPENDEX: This database is provided by Elsevier Engineering Information Inc. It includes papers from 1969 to present.

The above mentioned databases provide a broad coverage of the area of interest, i.e. "Risk analysis methods for IT systems", and they include articles from the main conferences, journals, and publishers (IEEE, ACM, Springer, etc.).

Search query

After a number of iterations, the following search query was considered a good compromise between finding as many of the relevant articles as possible, and returning a manageable number of results:

```
({risk analysis} OR
 {risk analyses} OR
 {risk identification} OR
 {RA})
AND (
 method* OR
 technique* OR
 approach*)
AND (
 {computer system} OR
 {information system} OR
 {IT system} OR
 {network system} OR
 {web?based system} OR
 {computer systems} OR
 {information systems} OR
 {IT systems} OR
 {network systems} OR
 {web?based systems})
NOT
( oil OR gas OR flood OR
 agricultur* OR chemi*))
```

The search string has four main parts separated by AND and NOT clauses.

The first part of the search string excludes articles that are not about 'risk analysis' or 'risk identification'.

The second part of the search string excludes articles that do not discuss one or more specific methods for risk analysis, or a synonym to 'method'. The '*'-character is a wildcard representing any string of characters, which allows different grammatical numbers of the term to be identified, e.g. both 'method' and 'methods'.

The third part of the search string excludes articles that are not in the field of information technology or computer science. The '?'-character is a wildcard representing one character, included because we want to identify both '-' and ' '.

The last part of the search string explicitly excludes articles about oil, gas, agriculture or chemistry. These research fields traditionally have a strong safety focus and contain many papers about risk analysis. They are, however, not domains in which IT systems are considered as the most critical components, and this part of the search string was included to prevent irrelevant papers from these domains from dominating the returned results.

3.3 Inclusion and exclusion criteria

When articles were identified with the search string from the databases, it was necessary to manually remove non-relevant articles from the selection. This was done first based on the title and keywords, then based on the abstract, and finally based on the full text. The inclusion and exclusion criteria were defined during the design of the review protocol. The manual selection of articles was carried out based on the following criteria:

- Articles not about methods for risk analysis or risk

[1] http://www.engineeringvillage2.org

management of computer system were excluded from the selection.

- Articles about the risk analysis of system development projects were excluded from the selection. That is, articles about risk management of *project risks* were excluded. The focus in this article is on risks for the organisation depending on the operation of IT systems, i.e. operational risk, not about the project risks associated with developing the systems.

- Articles specifically about the risk analysis of computer networks were excluded from the selection because the focus in this study is on risk analysis for complete IT systems not just the network component of the system. The excluded articles present risk analysis of network components such as, firewalls, intrusion detection systems, routers and implementation of security policies to cope with unauthorized access of data or resources, e.g., [17].

- Articles about the risk analysis of space systems, nuclear power plants, embedded medical devices, and military systems were also excluded from the selection. These domains have a long history of risk analysis methods, but these methods are often very time-consuming and mostly suited for embedded systems that are analysed in great detail. This study, however, focuses on risk analysis for large IT systems that are applicable to a wide range of systems in many types of organisations. An example of excluded article is [13].

Each of these criteria was necessary to limit the scope of this study. It would be impossible to cover risk analysis for all types of risk associated with all categories of IT systems in one review like this, because of the large number of relevant articles.

3.4 Selection of relevant articles

The above mentioned search query was carried out on 23 May 2012 and retrieved 1203 articles, and it has been decided to continue systematic review with these records. After this, the title, keywords, abstract and author names were downloaded for the initial selection of relevant articles. Then the EndNote (Reference manager) was used for the removal of duplicate articles. It found (automatically) 91 duplicate articles that have been removed from the initial list. After this, 26 duplicate articles were found by manual search and removed from the initial list as well.

In each step of the selection process (based first on the title and keywords, then on the abstract and then on the full text) these criteria were used by the first author of this article to manually remove non-relevant articles from the initial selection. This resulted, in each step, in three groups of articles:

- **Relevant:** Articles that clearly fulfil the criteria established above.

- **Not relevant:** Articles that are out of the scope of this study.

- **Possibly relevant:** Articles for which there was not enough information to establish whether they are relevant for this study. This list was rechecked by the co-authors for the selection. The remaining Articles (from selection based on title and keywords, and abstracts) were then added to the relevant articles for further selection in the next step.

After removing irrelevant articles based on the title and keywords, a first effort to remove non-relevant articles was carried out by the first author of this article. This selection resulted in a list containing 229 relevant and 48 possibly relevant articles. To check the reliability of this first step, the second author of this article cross checked 100 randomly chosen articles from the initial list and found disagreement on 3 relevant articles not added and 6 non-relevant articles added. To increase the reliability of the selection, it was therefore decided to repeat the initial selection process based on this information and to only exclude those articles that were not relevant in light of this. The selection process was by this conducted once again and resulted in 70 more articles from the initial list to the main selected list. After this, the possibly relevant articles list was checked and 21 out of 48 articles were selected and added in the main list for the next step of review. After doing the initial selection process again the resulted selection list came up with a total of 320 relevant articles.

The second selection was conducted based on the abstracts, the first author read the abstracts and found 183 relevant articles out of a total of 320. The second author again rechecked this selection and he found 17 more relevant articles. After adding these 17 articles the second selection list came up with a total of 200 relevant articles for the next step of review.

In the third step of the selection process, the full text of the relevant articles needed to be downloaded. The full text for all articles was not always available for all articles and 57 articles were removed from the selection because the articles were not written in English (most often in Chinese) or because the full text could not be downloaded (mostly older articles).

After this, the first author carefully read the full text of all downloaded articles and selected 77 relevant articles. The second author of this article cross-checked the excluded articles from the final list suggested adding two more relevant articles in the final list, which resulted in 79 relevant articles. Then, he cross checked the finally selected articles by reading the full text and removed 23 irrelevant articles. After removing the irrelevant articles the list contained 56 relevant articles. There was a disagreement for the selection of [article 24], the third author carefully read it, and after discussion all authors agreed to select it for the review.

Finally, the reference lists of the most relevant articles were inspected for further relevant articles that were not included in the selection. Initially 5 articles were selected from reference inspection, after reading the full text of selected articles only one article identified as relevant for this study. This article was from a source that was not included in the searched resources. After adding this article the final list contains the

57 articles listed in the appendix of this article.

3.5 Data extraction and synthesis

In the final steps of the selection, i.e. the selection based on the full text of the articles, the articles were classified based in the following classes:

Class A Articles describing or evaluating existing risk analysis methodologies.

Class B Articles presenting improvements or changes to existing risk analysis methodologies.

Class C Articles presenting new methods for risk analysis of IT systems.

Further, a number of relevant attributes were also extracted from each of the articles with respect to the research questions discussed in Section 3.1. The results of this data extraction and classification are discussed in Section 5.

4. VALIDITY ASSESSMENT

The main objective of this research is to summarize the available research in the field of risk analysis for IT systems. An important threat to the validity of this study is that it cannot be guaranteed that all possible relevant articles in this field have been included in the study. First of all, only research published in English was included for practical reasons. Secondly, some lesser known journals or conferences are not available in the searched databases, and were therefore not searched in this study. Also, articles for which the full text was not available were excluded from this study. This mostly affects older articles. Thirdly, it is likely that some relevant articles were rejected by the search string, since it is impossible to define a search string that finds absolutely all relevant articles without returning an unmanagable number of false positives. Finally, it is of course also possible that relevant articles were incorrectly rejected during the manual selection process from over one thousand articles to the final selection of 57 articles.

To increase the validity of this study, the reference list of the most relevant articles from the final selected list were examined for missing important articles. This validity check resulted in only one new article being added to the selection of articles. This article had not been found in the automatic search because it was from a source not included in the searched databases.

In order to reduce the risk of incorrect rejection of an article during the selection process, the co-authors of this article cross-checked the selection in each step. Whenever there was doubt about whether to include an article or not, the article was retained for the next step of the selection process. After initial selection process based on the title and keywords, the second author of this article cross checked 100 randomly selected articles from the initial list, and suggested a few additions and removals of articles. Instead of just adding and removing these articles, it was decided to repeat the selection process and to keep any articles selected in either case.

After the second selection process based on abstracts, the second author of this article re-checked the complete selection and found 17 more relevant articles that had possibly been rejected incorrectly, and in this way made sure that also articles where we were in doubt were included.

After the third selection process that was conducted after reading the full text of articles, the second author of this article cross checked the excluded articles from the final list and suggested the adding of two more relevant articles to the final list. Then he cross checked the finally selected articles by reading their full text and found 23 non-relevant articles according to the defined research questions.

That is, whenever there was a doubt in selection of an article it was retained for the next step, were more information was available to decide the relevance of an article with more accuracy. Whenever one author was not sure about the classification of an article, the co-authors reviewed the article and decision about the classification was based on the agreement by all authors.

By taking the above mentioned measures for the validity of this study we are more confident that most of the relevant articles for this study have been identified and included in the final list of articles.

5. RESULTS

This section presents an analysis of the data extracted from the selected articles.

5.1 Year of publication

In Figure 2, the publication year for the selected articles is displayed. It can be observed that the oldest selected article is from the year 1980, and the most recent from 2012. About half of the articles were published in the last 5 years before the publication of this study. That is, this indicates that the number of publications in the area has increased the later years, at least if we were able to find as many of the older articles as the newer articles.

5.2 Risk analysis method classification

Table 1 shows the classification of the selected articles into classes A, B, and C, see Section 3.5. Class A, about existing risk analysis methods, includes 18 articles. Articles in this class describe general risk analysis concepts and its importance for dependable IT systems. This class also contains some articles about the comparison of different risk analysis methods. Class B includes 5 articles that present improvements in existing risk analysis methods.

The majority of the articles are in class C. It includes 34 articles that are about presenting new frameworks, methods and models for risk analysis.

5.3 Types of systems

Table 2 shows the types of system that the selected articles focus on. The majority of the selected articles, 49 articles out of 57, are about risk analysis of IT systems in general. This means that the paper does not specificy which type of systems the research is about, and thereby it can be assumed

Table 1: Classification of articles

Classification	articles	#
Class A	2, 4, 5, 7, 8, 10, 12, 14, 18, 21, 22, 26, 32, 38, 41, 45, 52, 56	18
Class B	34, 42, 43, 44, 47	5
Class C	1, 3, 6, 9, 11, 13, 15, 16, 17, 19, 20, 23, 24, 25, 27, 28, 29, 30, 31, 33, 35, 36, 37, 39, 40, 46, 48, 49, 50, 51, 53, 54, 55, 57	34

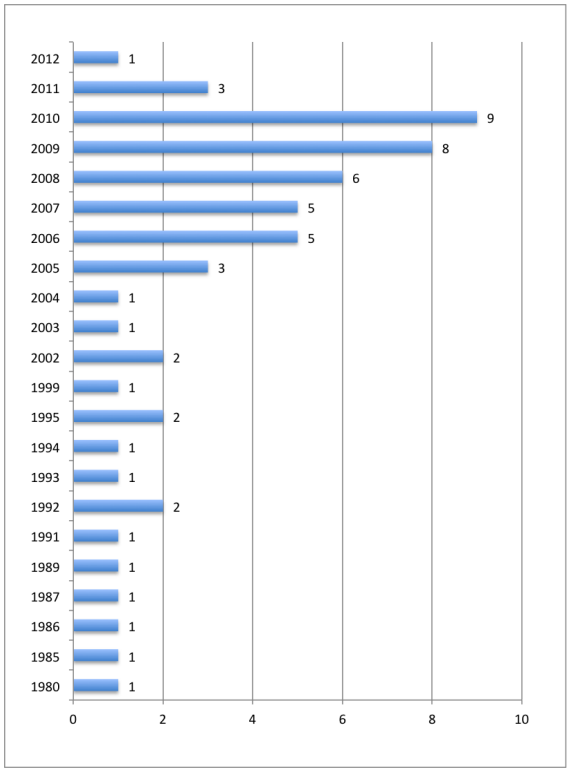

Figure 2: Histogram of publication year for the identified articles

that the intention is that the research results should be generally valid. However, 2 articles are specifically about risk analysis for e-commerce systems, 3 are about hospital systems, 1 is specifically about web service systems, 1 is about cloud computing and 1 is about e-government systems. It should be noted that articles about space technology and military systems were specifically excluded before the classification.

5.4 Analytical or empirical research

In Table 3, the research methodologies that were used in the selected articles are categorized as either completely *analytical* (not containing any research based on the application of a risk analysis method on an actual system) or *empirical* (containing an explicit description of an application of at least one risk analysis method, either in a real-life setting or in a controlled experiment). 36 articles were identified as analytical and 21 as empirical research. These 21 articles all presented case studies on risk analysis methods, no surveys or experiments were identified.

5.5 Area of risk management

Risk management is a process that consists of several activities: risk identification, risk analysis, risk assessment, risk prioritization, and risk mitigation. It is a process that tries to find a balance between loss prevention and cost associated with countermeasures. It usually starts with the *risk identification* activity to determine a list of possible risks. Next, *risk analysis* is applied to combine the probability and the expected consequences associated with each risk. Sometimes the term 'risk analysis' is also used to include the risk identification step. Then, in *risk prioritization*, all the identified risks are prioritized based on the results of the risk analysis. Finally, *risk mitigation*, deals with implementing appropriate measures and controls to reduce the probability or the consequences of the identified risks, based on the results of the prioritisation. *Risk assessment*, on the other hand, usually deals with the analysis of a system with existing security measures and anticipates the weaknesses present in assessed system. However, these definitions are not generally accepted and sometimes each of these terms are used to describe a process that includes several of the other activities.

Although our search for articles specifically searched for articles about risk analysis or risk identification, the final list of selected articles contain some articles that mainly focus on risk management as a whole and some articles that focus only on one or more of the different sub-activities. Table 4 shows the focus of the selected articles within the field of risk management. It can be noticed that the majority of selected articles, 28 articles out of 57, are in fact about risk analysis. Further, it can be seen that 1 article is specifically

Table 2: Focused systems in selected articles

Type of System	articles	#
IT systems in general	1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 26, 27, 28, 29, 30, 31, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 52, 53, 54, 55, 56	49
Hospital systems	2, 32, 57	3
E-Commerce	25, 50	2
Cloud computing	16	1
E-government	51	1
Web-service systems	21	1

Table 3: Type of research presented in selected articles

Research type	Selected articles	#
Analytical	1, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 14, 18, 19, 20, 22, 23, 24, 25, 27, 29, 30, 31, 33, 37, 38, 40, 42, 43, 44, 45, 47, 48, 49, 50, 53	36
Empirical -Case study	2, 7, 15, 16, 17, 21, 26, 28, 32, 34, 35, 36, 39, 41, 46, 51, 52, 54, 55, 56, 57	21

about risk identification, 15 are about risk assessment, 1 is about risk prioritization, 2 are about risk mitigation and 20 are about risk management as a whole.

5.6 Qualitative and Quantitative risk analysis

Table 5 classifies the risk analysis methods in the selected articles as quantitative or qualitative. Quantitative methods express the probability and consequences of the identified risk as a numerical result. This makes it possible to calculate the relationship between loss prevention and cost associated with proposed countermeasures. Often it is difficult to use quantitative risk analysis because it is hard to estimate the exact probability and loss associated with each risk. Qualitative methods, on the other hand, use descriptive values such as 'high', 'medium' or 'very low' to express the probability and consequences of each risk. Both types of risk analysis methods are widely used for different types of systems, and in some cases they can be used together. Except for qualitative, quantitative and combined risk analysis methods, this study also identified semi-quantitative methods. This is an intermediary risk analysis technique that classifies the probability and consequences by using quantitative categories such as 'financial loss between 10.000 USD and 100.000 USD' or 'less than once per 100 years'. It does not require the exact estimates needed for a quantitative risk analysis, but offers a more consistent approach than qualitative risk analysis. Not all of the selected articles contain enough information to determine whether a qualitative or quantitative approach was used, and for some articles the question is not applicable. Of the 38 articles that could be classified according to this criterion, 23 articles use a quantitative approach, 7 a qualitative approach, 6 contain a combined (quantitative and qualitative) risk analysis approach, and 2 are about semi-quantitative risk analysis methods.

6. DISCUSSION

First of all it can be observed that many of the identified articles have been published during the last few years before this study (2006-2011). This may mean that the amount of research has increased. As also discussed above, there may be other reasons, such as that the databases are more complete for later years. However, an increased dependence on information in the society, e.g. when critical processes to an increased extent are supported by IT-systems, may also mean that there is an increased interest in risk management of IT-systems.

In order to investigate the relationship between different investigated factors different pairs of variables were investigated.

It was found that risk management papers are to a larger extent non-empirical than papers in the other categories, see Table 6. This may be because this topic requires more research effort to be studied empirically since it is process covering a rather long time-span.

Risk analysis methods for a specific type of systems are all found in empirical papers, except for the papers about e-commerce systems. This probably indicates that most risk analysis methods are developed with general IT systems in mind. Only when they are applied in practice they are adapted for specific classes of systems.

It was also found that qualitative risk analysis methods are more likely to be investigated in empirical papers than quantitative analysis methods, see Table 7. This may be because quantitative methods are not as easy in practice as it might seem, because a lot of specific data is needed. When a risk analysis method is used in practice, it is often easier to classify a risk's probability and consequence into some categories than to assign an exact numerical value. This however limits the analysis that can be done later. A lot of information is lost when categories are used in stead of a quantitative best estimate, possible combined with an explicit uncertainty range on the estimate.

It can be noticed from the previous section that the majority of the identified articles present either qualitative or quantitative risk analysis and only two articles (3, 16) use

Table 4: Focused risk management part in the selected articles

Risk management part	Selected articles	#
Risk analysis	1, 2, 3, 4, 5, 8, 11, 13, 14, 15, 19, 20, 21, 23, 24, 25, 26, 27, 29, 32, 34, 35, 40, 42, 47, 50, 56, 57	28
Risk identification	32	1
Risk assessment	5, 7, 9, 16, 31, 33, 36, 37, 39, 44, 45, 46, 52, 53, 55	15
Risk prioritization	16	1
Risk mitigation	12, 52	2
Risk management	4, 9, 10, 16, 17, 18, 19, 20, 21, 22, 27, 29, 30, 32, 35, 38, 43, 47, 48, 49	20

Table 5: Type of risk analysis method (quantitative or qualitative)

Risk analysis type	Selected articles	#
Qualitative	2, 12, 13, 14, 21, 34, 57	7
Quantitative	4, 5, 15, 19, 23, 24, 25, 26, 28, 31, 33, 36, 37, 39, 40, 41, 44, 49, 52, 53, 54, 55, 56	23
Combined approach	9, 10, 18, 42, 45, 46	6
Semi-Quantitative	3, 16	2

Table 6: Paper area vs. empirical or not

Paper area	No	Yes
BCP	0	1
General	1	1
Risk Analysis	12	6
Risk Analysis and Assessment	1	0
Risk Analysis and Management	7	2
Risk Assessment	6	7
Risk Assessment and management	1	0
Risk Assessment and mitigation	0	1
Risk Assessment, prioritization, and management	0	1
Risk Identification, analysis, and management	0	1
Risk management	7	1
Risk Mitigation	1	0
SUM	36	21

Table 7: Risk analysis approach vs. empirical or not

Approach	No	Yes
Combined approach	5	1
General	14	5
Qualitative	3	4
Quantitative	13	10
Semi-quantitative	1	1
SUM	36	21

a semi-quantitative risk analysis method. Based on this, it could be argued that there is a need for more research on techniques and methods that combine the advantages of both quantitative and qualitative methods.

Two identified articles (9, 10) present research on the well-known risk analysis method CORAS, that performs model-based risk analysis by using UML, and one article (54) that proposes a new risk analysis method using fault-tree analysis. This review also has identified some other specific risk analysis methods named in a few articles such as LAVA, LRAM , CRAMM, OCTAVE, Mehari and Magerit (20, 34, 45, 47).

This review has identified five articles (2, 42, 43, 44, 47) that describe, analyse and compare existing well-known risk analysis methods. But from these articles it is not possible to decide that a particular method is better than other.

7. CONCLUSIONS

Based on this mapping study of risk analysis methods for IT-systems discussed in the research literature, it can be concluded that most articles focus on new methods, and new frameworks and models for risk analysis. Only few papers focus on already available, and thereby maybe already known, methods. Further, it can be concluded that most research concerns general risk analysis methods, and not methods specific to certain types of IT systems.

The fact that only few articles focused on already available methods also means that it is not possible to say from the identified articles to what extent different methods are used in practice. For the same reason, it has not been possible to find many articles comparing available risk analysis methods, even if we argue that there is a need for this kind of research.

It can also be concluded that a majority of the identified articles present research that is non-empirical (36 articles), and fewer articles (21 articles) present case studies. None

of the identified articles present research conducted as surveys or controlled experiments. Concerning what type of risk analysis methods that are presented in the published research, it can be concluded that most identified research concerns quantitative risk analysis methods.

Based on these findings a number of areas for further research can be identified. First of all it can be concluded that there is a need to conduct research where already available methods are investigated. This can for example be carried out as studies where different types of methods are compared in controlled experiments. We believe that methods for risk analysis are quite possible to investigate in controlled experiments [23], since they are possible to isolate from the whole management process to investigate them in a 'laboratory' setting. Having said that, we also believe that there is a need to further investigate the whole risk management process in longer case studies, where actual cases of risk management are investigated in practice.

ACKNOWLEDGEMENT

This work was funded by the Swedish Civil Contingencies Agency under a grant for PRIVAD, Programme for Risk and Vulnerability Analysis Development.

LIST OF SELECTED ARTICLES

(1) Beachboard, J., Cole, A., Mellor, M., Hernandez, S., Aytes, K., Massad, N., Improving information security risk analysis practices for small-and medium-sized enterprises: a research agenda, Journal of Issues in Informing Science and Information Technology Journal, vol. 5, pp. 73-85, 2008.

(2) Bennett, S.P., An application of qualitative risk analysis to computer security for the commercial sector, In proceedings of Eighth Annual Computer Security Applications Conference (Cat. No.92TH0470-5), pp. 64-73, 1992.

(3) Birch, D.G.W., McEvoy, N.A., Risk analysis for information systems, Journal of Information Technology, vol. 7, issue 1, pp. 44-53, March 1992.

(4) Bojanc, R., Jerman-Blazic, B., An economic modelling approach to information security risk management, International Journal of Information Management, vol. 28, issue 5, pp. 413-22, 2008.

(5) Breier, J., Risk analysis supported by information security metrics, In proceedings of 12:th International Conference Computer Systems and Technologies, pp. 393-398, 2011.

(6) Chivers, H., Information modeling for automated risk analysis, In proceedings of 10:th International Conference Communications and Multimedia Security (CMS), pp. 228-239, 2006.

(7) Coles-Kemp, L., Triangulating the views of human and non-human stakeholders in information system security risk assessment, In proceedings of the 2007 International Conference on Security & Management, SAM 2007, pp. 172-178, 2007.

(8) De Koning, W.F., A methodology for the design of security plans, Computers & Security, vol. 14, issue 7, pp. 633-643, 1995.

(9) Djordjevic, I., Suitability of risk analysis methods for security assessment of large scale distributed computer systems, In proceedings of the 6:th Conference of International Association of Probabilistic Safety Assessment and Management, 23-28 June, San Juan, Puerto Rico, USA, 2002.

(10) Djordjevic, I., Model based risk management of security critical systems, In proceedings of the 3:rd International Conference on Computer Simulation in Risk Analysis and Hazard Mitigation, pp. 253-264, 2002.

(11) Eloff, J.H.P., Labuschagne, L., Badenhorst, K.P., Comparative framework for risk analysis methods, Computers & Security, vol. 12, issue 6, pp. 597-603, 1993.

(12) Eom, Jung-Ho, Qualitative method-based the effective risk mitigation method in the risk management, In proceedings of the International Conference on Computational Science and its Applications (ICCSA), pp. 239-248, 2006.

(13) Eom, Jung-Ho, Risk assessment method based on business process-oriented asset evaluation for information system security, In proceedings of the International Conference on Computational Science (ICCS), pp. 1024-1031, 2007.

(14) Eom, Jung-Ho, Qualitative initial risk analysis for selecting risk analysis approach suitable for IT security policy, In proceedings of the International Conference on Information Theory and Information Security, pp. 669-673, 2010.

(15) Feng, Nan, A probabilistic estimation model for information systems security risk analysis, In proceedings of the International Conference on Management and Service Science (MASS), p. 4, 2009.

(16) FitŮ, J.O., MacŠas, M., Guitart, J., Toward business-driven risk management for Cloud computing, In proceedings of the 6:th International Conference on Network and Service Management (CNSM 2010), pp. 238-241, 2010.

(17) Ghernouti-Helie, S., Reasonable security by effective risk management practices: From theory to practice, In proceedings of the 12:th International Conference on Proceedings of the 2009 12th International Conference on Network-Based Information Systems (NBiS 2009), p 226-33, 2009.

(18) Grob, H. L., Conceptual modeling of information systems for integrated IT-risk and security management, In proceedings of the 2008 International Conference on Security and Management (SAM), pp. 178-184, 2008.

(19) Guarro, S.B., Principles and procedures of the LRAM approach to information systems risk analysis and management, Computers & Security, vol. 6, issue 6, pp. 493-504, 1987.

(20) Guarro, S.B., Risk analysis and risk management models for information systems security applications, Reliability Engineering & System Safety, vol. 25, issue 2, pp. 109-130, 1989.

(21) GutiŐrrez, C., Rosado, G. D., FernĞndez-Medina, E., The practical application of a process for eliciting and designing security in web service systems, Information and Software Technology, vol. 51, issue 12, pp. 1712-1738, 2009.

(22) Hamdi, M., Boudriga, N., Computer and network security risk management: Theory, challenges, and countermeasures, International Journal of Communication Systems, vol. 18, issue 8, pp. 763-793, 2005.

(23) Hu, Zhi-Hua, Knowledge-based framework for real-time risk assessment of information security inspired by danger model, In proceedings of the International Symposium on Intelligent Information Technology, pp. 1053-1056, 2008.

(24) In, H.P., A security risk analysis model for information systems, Systems Modeling and Simulation: Theory and Applications, In procedings of the Third Asian Simulation Conference, AsiaSim 2004, Revised Selected Papers (Lecture Notes in Computer Science Vol.3398), pp. 505-513, 2005.

(25) Jung, C., Han, I., Suh, B., Risk analysis for electronic commerce using case-based reasoning, International Journal of Intelligent Systems in Accounting, Finance and Management, vol. 8, issue 1, pp. 61-73, 1999.

(26) Kaegi, M., Information systems' risk analysis by agent-based modelling of business processes, In proceedings of the European Safety and Reliability Conference (ESREL) - Safety and Reliability for Managing Risk, 2006.

(27) Kailay, M. P.; Jarratt, P., RAMeX: a prototype expert system for computer security risk analysis and management, Computers & Security, vol. 14, issue 5, pp. 449-463, 1995.

(28) Kim, Young-Gab, Quantitative risk analysis and evaluation in information systems: A case study, In proceedings of the 7:th International Conference on Computational Science (ICCS), pp. 1040-1047, 2007.

(29) La Corte, A., A Process Approach to Manage the Security of the Communication Systems with Risk Analysis Based on Epidemiological Model, In proceedings of the 5:th International Conference on Systems and Networks Communications (ICSNC), pp. 166-171, 2010.

(30) Li Helgesson, Y.Y., Managing risks on critical IT systems in public service organizations, In proceedings of the 2009 International Conference on Computational Science and Engineering (CSE), pp. 470-475, 2009.

(31) Li, He-Tian, Security risk evaluation for it systems based on the Markov chain, Journal of the China Railway Society, vol. 29, issue 2, pp. 50-53, 2007.

(32) Lindholm, C, Pedersen Notander, J., Höst, M. Software Risk Analysis in Medical Device Development, In proceedings of the 37:th EUROMICRO Conference on Software Engineering and Advanced Applications, pp. 362-365, 2011.

(33) Lu, Simei, Security risk assessment model based on AHP/D-S evidence theory, In proceedings of 2009 International Forum on Information Technology and Applications (IFITA), pp. 530-534, 2009.

(34) Maglogiannis, I., Zafiropoulos, E., Platis, A., Lambrinoudakis, C., Risk analysis of a patient monitoring system using Bayesian Network modeling, Journal of Biomedical Informatics, vol. 39, issue 6, pp. 637-647, 2006.

(35) McGaughey Jr. R.E., Snyder, C.A., Carr, H.H., Implementing information technology for competitive advantage: risk management issues, Information & management, vol. 26, issue 5, pp. 273-280, 1994.

(36) Mock, R., Risk analysis of information systems by event process chains, International Journal of Critical Infrastructures, vol. 1, issue 2-3, pp. 247-257, 2005.

(37) Mosleh, A., Bayesian probabilistic risk analysis for computer systems, Performance Evaluation Review, vol. 13, issue 1, pp. 5-12, 1985.

(38) Nassar, P.B, Risk management and security in service-based architectures, In proceedings of the International Conference on Advances in Computational Tools for Engineering Applications (ACTEA), pp. 214-218, 2009.

(39) Patel S.C., Graham J.H., Ralston P.A.S., Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements, International Journal of Information Management, vol. 28, issue 6, pp. 483-491, 2008.

(40) Pirzadeh, L., A Cause and Effect Approach towards Risk Analysis, In proceedings of the 3:rd International Workshop on Security Measurements and Metrics (Metrisec), pp. 80-83, 2012.

(41) Post, G. V., Diltz, J. D., A stochastic dominance approach to risk analysis of computer systems, Management Information Systems Quarterly, vol. 10, issue 4, pp. 363-374, 1986.

(42) Rainer, R. K., Snyder, C. A., Carr, H. H., Risk analysis for information technology, Journal of Management Information Systems, vol. 8, issue 1, pp. 129-147, 1991.

(43) Sarkheyli, A., Improving the current risk analysis techniques by study of their process and using the human body's immune system, In proceedings of the 5:th International Symposium on Telecommunications (IST), pp. 651-656, 2010.

(44) Satoh, N., Kumamoto, H., Kino, Y., Norihisa, K., Viewpoint of ISO GMITS and PRA in information assessment, In proceedings of the 8:th conference on Applied Computer Science, pp. 253-258, 2008.

(45) Smith, S.T., LAVA, Proceeding of 12:th National Computer Security Conference, Baltimore, MD, USA, 1989.

(46) Sun, L., Srivastava, R. P., Mock, T. J., An information systems security risk assessment model under the Dempster-Shafer theory of belief functions, Journal of Management Information Systems, vol. 22, issue 4, pp. 109-142, 2006.

(47) Syalim, A., Comparison of risk analysis methods: Mehari, Magerit, NIST800-30 and Microsoft's security management guide, In proceedings of the International Conference on Availability, Reliability and Security (ARES), pp. 726-731, 2009.

(48) Trcek, D., Security metrics foundations for computer security, Computer Journal, vol. 53, issue 7, pp 1106-1112, 2010.

(49) Trcek, D., System dynamics based risk management for distributed information systems, In proceedings of the 4:th International Conference on Systems (ICONS), pp. 74-79, 2009.

(50) Warren, M., Hutchinson, W., A security risk management approach for e-commerce, Information Management & Computer Security, vol. 11, issue 5, pp. 238-242, 2003.

(51) Wei, G., Research on E-government Information Security Risk Assessment - Based on Fuzzy AHP and Artificial Neural Network Model, In proceedings of the 1:st International Conference on Networking and Distributed Computing (ICNDC 2010), pp 218-221, 2010.

(52) Wijnia, Y., Assessing business continuity risks in IT, In proceedings of the IEEE International Conference on Systems, Man and Cybernetics, pp. 3547-3553, 2008.

(53) Winkelvos, Timo, A property based security risk analysis through weighted simulation, In proceedings of the Information Security for South Africa (ISSA), 2011.

(54) Xiao, H., The research of information security risk assessment method based on fault tree, In proceeding of the 6:th International Conference on Networked Computing and Advanced Information Management (NCM), pp. 370-375, 2010.

(55) Xinlan, Z., Information security risk assessment methodology research: Group decision making and analytic hierarchy process, In proceedings of the 2:nd WRI World Congress on Software Engineering, pp. 157-160, 2010.

(56) Yan, H., Power information systems security: Modeling and quantitative evaluation, In proceedings of the IEEE Power Engineering Society General Meeting, pp. 905-910, 2004.

(57) Zain, N. M., Fuzzy based threat analysis in total hospital information system, Advances in Computer Science and Information Technology, In Joint Proceedings AST/UCMA/ISA/ACN 2010 Conferences, pp. 1-14, 2010.

8. REFERENCES

[1] C. Alberts and A. Dorofee. *Managing Information Security Risks: The Octave Approach*. SEI Series in Software Engineering. Addison-Wesley, 2003.

[2] E. Engström and P. Runeson. Software Product Line Testing - A Systematic Mapping Study. *Information and Software Technology*, 53:2–13, 2011.

[3] ENISA ad hoc working group on risk assessment and risk management. Inventory of risk assessment and risk management methods, 2006.

[4] C. A. Ericson. Fault Tree Analysis – A History. In *Proceedings of The 17th International System Safety Conference*, 1999.

[5] Great Britain. Treasury. Central Computer and Telecommunications Agency. *Prince User's Guide to CRAMM*. Programme and Project Management Library. H.M. Stationery Office, 1993.

[6] International Organization for Standardization. ISO/IEC 27002:2005 – Information technology – Security techniques – Code of practice for information security management, 2005.

[7] International Organization for Standardization. ISO/IEC 27005:2011 – Information technology – Security techniques – Information security risk management, 2011.

[8] M. Jørgensen. A Review of Studies on Expert Estimation of Software Development Effort. *Journal of Systems and Software*, 70(1-2):37–60, 2004.

[9] M. Khan, S. Khan, and M. Sadiq. Systematic review of software risk assessment and estimation models. *International Journal of Engineering and Advanced Technology*, 1:298.

[10] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman. Systematic Literature Reviews in Software Engineering – A Systematic Literature Review. *Information and Software Technology*, 51(1):7–15, 2009.

[11] B. Kitchenham, D. Budgen, and O. P. Brereton. Using Mapping Studies as the Basis for Further Research – A Participant-Observer Case Study. *Information and Software Technology*, 53:638–651, June 2011.

[12] B. Kitchenham and S. Charters. Guidelines for performing systematic literature reviews in software engineering. *Technical Report Keele University and University of Durham*, 2.3, 2007.

[13] B. Li, M. Li, K. Chen, and C. Smidts. Integrating Software into PRA: A Software-Related Failure Mode Taxonomy. *Risk Analysis*, 26(4):997–1012, 2006.

[14] D. Liu, Q. Wang, and J. Xiao. The role of software process simulation modeling in software risk management: A systematic review. In *3rd International Symposium on Empirical Software Engineering and Measurement (ESEM)*, pages 302–311. IEEE, 2009.

[15] R. McDermott, R. Mikulak, and M. Beauregard. *The Basics of FMEA, 2nd Edition*. Taylor & Francis, 1996.

[16] Methods working group, Club de la Sécurité de l'Information Français. Mehari 2010 – evaluation guide for security services, 2010.

[17] L. Mixia, Y. Dongmei, Z. Qiuyu, and Z. Honglei. Network Security Risk Assessment and Situation

Analysis. In *Proceedings of the 2007 IEEE International Workshop onAnti-counterfeiting, Security, Identification*, pages 448 –452, april 2007.

[18] P. G. Neumann. Risks of Untrustworthiness. In *Proceedings of the 22:nd Annual Computer Security Applications Conference*, pages 321–328. IEEE Computer Society, 2006.

[19] F. Redmill, M. Chudleigh, and J. Catmur. *System Safety : HAZOP and Software HAZOP*. John Wiley & Sons, 1999.

[20] K.-J. Stol and M. A. Babar. Reporting Empirical Research in Open Source Software: The State of Practice. In *Proceedings of the International Conference on Open Source Systems, OSS 2009*, pages 156–169, 2009.

[21] G. Stoneburner, A. Goguen, and A. Feringa. *Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology, Special Publication 800-30. U.S. Government Printing Office, 2002.

[22] A. Syalim, Y. Hori, and K. Sakurai. Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. In *ARES*, pages 726–731. IEEE Computer Society, 2009.

[23] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén. *Experimentation in software engineering: an introduction*. Kluwer Academic Publishers, Norwell, MA, USA, 2000.