Risk Analysis Terminology for IT-systems: Does it match intuition?

Ida Hogganvik, Ketil Stølen
SINTEF ICT, PO box 124 Blindern, N-0314 Oslo, and
Department of Informatics, University of Oslo, PO box 1080 Blindern, N-0316 Oslo
{iho, kst}@sintef.no

Abstract

Many risk specific concepts like "threat", "consequence" and "risk" belong to the daily language. In a risk analysis one cannot be certain that the participants' interpretation of these terms is in accordance with risk analysis definitions. Risk analyses often use brainstorming techniques to identify risks based on the opinions and judgments of system experts. Such techniques employ risk specific terminology, and to avoid misunderstandings and uncertainty among the participants, it is important that the terminology does not conflict with the daily language understanding of these terms. We have developed a formal, conceptual model of IT-system risk analysis terminology and investigated to what extent this model corresponds to the common, or intuitive, understanding of the concepts. The paper reports on the results from a survey conducted among 57 professionals and students.

Keywords: risk analysis terminology, conceptual model, survey

1. Introduction

In software development it is common to conduct some form of analysis of the product to assess how secure it is. One can assess the system's ability to resist unauthorized access or whether the data is transmitted securely. The participants in a risk analysis face questions like: "What are the system threats and its vulnerabilities? "What are the assets in your system which you want to protect?" "Are there unwanted incidents that can harm your assets?" "What is the frequency of this unwanted incident?" The questions make use of a specialized risk analysis terminology, but many of the terms are also commonly used in the daily language.

Standards for risk analysis of IT-systems [1, 6, 9-11] are often inspired by standards developed for risk analysis in e.g. mechanical engineering or the process industry [7, 8]. Within these domains there is a long tradition for using risk analysis, and its terminology is well established, but is this also the case within IT-systems development?

A previous survey with students showed that there were diverging opinions on how to interpret concepts used in risk analysis [12, 13]. Concrete, tangible concepts like *asset* and *threat* were found easier to understand than more abstract terms like *risk*. The results from this survey made us revise our conceptual model of risk analysis terminology, leading to the version we investigated in this survey (Figure 1). To identify the concepts and relationships that are straightforward and those that are more problematic, we conducted a survey among 57 Norwegian subjects with knowledge of risk analysis terminology representative of normal risk analysis participants. The survey tested how risk analysis terms are interpreted by subjects (both students and professionals) with various competences on risk analysis. We believe that many know these terms from before, but how well does our conceptual model correspond with the subjects' interpretation?

The survey revealed that the subjects' interpretations match our model quite closely, in average the subjects obtained almost 60% correct answers (here *correct* means in accordance with our model). There was a statistical significant difference between software engineering students' score and the professionals', which indicates that people's background affects how well IT-system risk analysis terminology is understood.

The paper is structured as follows: Section 2 provides background information on risk analysis, structured brainstorming and risk analysis terminology. Section 3 describes the survey design, and Section 4 provides the results. In Section 5 we discuss our findings. Section 6 reports the threats to the validity of our results. Finally Section 7 presents the main conclusions.

2. Risk analysis of IT-systems

This section provides an introduction to risk analysis of IT-systems and its terminology.

2.1 Structured brainstorming

Risk management of IT-systems is *the total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect IT system resources* [9].

0-7803-9508-5/05/$20.00 ©2005 IEEE

Risk analysis is part of the management process and often based on *structured brainstorming* techniques (i.e. what [14] calls HazOp-analysis). A structured brainstorming for identification of risks is a methodical "walk-through" of the object of analysis. Experts on different aspects of the system are involved to identify system risks, threats and vulnerabilities, and sometimes suggest possible treatments for the risks. The participants in a brainstorming (in addition to the analysis team) can potentially be anyone associated with the target system. The authors of [14] recommend these roles to be represented: (1) user or intended user of the system assessed, (2) experts on one or more aspects of the system, (3) system designer, (4) analysis leader and (5) analysis secretary. The latter two are part of what we call the analysis team, which is responsible for guiding the analysis. Often the only form of preparation the participants receive is an introduction to brainstorming at the beginning of the session. Experts may in some cases only contribute in the part of the analysis where their expertises are needed. During the brainstorming session, the group of experts assesses system descriptions in a stepwise and structured manner, supported by guidewords that help them identify vulnerabilities and threats associated with risks. The findings are documented by the analysis secretary.

2.2 Risk analysis terminology

The participants in a structured brainstorming need a clear understanding of the terminology used. The individual interpretation of terms like *frequency, probability, vulnerability* and *asset* may differ depending on the participant's background and experience. Several of the concepts are employed in daily language, but not with a unique, context independent interpretation. Normally misunderstandings will be cleared up as the analysis progress, but our goal is to minimize them by using an intuitive language.

We have developed a conceptual model inspired by the model used in an IT-system risk analysis method called CORAS (http://coras.sourceforge.net). CORAS was developed in a 4 year long EU project and gathers well known risk analysis methods into an integrated risk analysis framework based on several international standards [1-6, 9-11]. The terminology definitions are mainly taken from ISO/IEC13335: *Information technology – Guidelines for the management of IT Security* [9] and AS/NZS4360: *Australian / New Zealand Standard for Risk Management* [1]. The model is shown in Figure 1 using class diagram notation from the Unified Modeling Language (UML) [15]. The associations between the elements have cardinalities specifying the number of instances of one element that can be related to one instance of the other (example: "a stakeholder has at least one and maximum an infinite number of assets; and an asset belongs to only one stakeholder"). The black diamond symbolizes aggregation and the white composition. Elements connected with a composition can also be part of other compositions, while aggregated elements only exist within the specific aggregation.

We explain Figure 1 as follows: the IT-system or product evaluated during a risk analysis is called the **target of evaluation** [2]. **Stakeholders** are those people and organizations who may affect, be affected by, or perceive themselves to be affected by, a decision or activity regarding the target system [1]. Different stakeholders often value the system differently; a system user who is dependent on the system may put a high value on it, while other stakeholders may not value it equally high. An **asset** is something to which a stakeholder directly assigns value and, hence, for which the stakeholder requires protection [3]. An asset is uniquely linked to a single stakeholder. The type of assets may differ according to the scope of the analysis. In a security-focused analysis the assets may be less obvious than in a safety-focused analysis. A safety analysis is often concerned about protecting people, the environment or equipment. In a security analysis assets can also be customer information, source code, company brand, critical system services etc. A stakeholder wants to protect his/her assets from being compromised. Target system stakeholders and their assets are normally identified early in process.

Figure 1 includes four important risk analysis concepts related to asset: *vulnerability*, *unwanted incident*, *threat* and *risk*. A **vulnerability** is a weakness of an asset or group of assets which can be exploited by one or more threats [9]. One may understand a vulnerability as something that is "missing", e.g. if a company network lacks a firewall it may be a vulnerability with respect to some assets in the network. An **unwanted incident** [9] is an event that may harm or reduce the value of assets and is something we want to prevent. An unwanted incident is the result of a threat exploiting a vulnerability. If a server in a company network is an asset, then an unwanted incident is unauthorized access to the server by intruders. A **threat** is a potential cause of an unwanted incident [9]. A **risk** the chance of something happening that will have an impact upon objectives (assets)[1]. A risk consists of an unwanted incident, the chance of it happening and its consequence. If we continue the example about the company network, a threat may be a person who knows or discovers the network's vulnerability and wants to exploit it. The company may not recognize the potential risky situation because nobody outside the company is aware of the security hole, but if e.g. an employee is fired one suddenly has a risk of unauthorized network access by

people familiar with the company's infrastructure. The level of risk is measured by a **risk value** [1] (e.g. low, medium, high or other scales) which is based upon the estimated **frequency** for the unwanted incident to happen and its **consequence** in terms of loss of asset value. Consequence is sometimes called *impact* [9]. *Frequency* is the exact number of occurrences within a time period, in addition to frequency there exist two other measures for how often a risk may occur: *likelihood* and *probability*. **Likelihood** is a qualitative description of probability or frequency [1] (e.g. "unlikely", "possible", "certain"), whereas **probability** is a number between 0-1 often represented as percentage (e.g. "a 50% chance for a risk to happen"). According to [9] probability should be used to characterize risk, while [1] suggests likelihood. If a risk is estimated to occur two times a year and the consequence is a loss of 200.000 dollars each time, the risk value could be "high" which means the risk should be treated. A **treatment** (in [9] called *safeguard*) is the selection and implementation of appropriate options for dealing with risk [1]. A treatment can either be directed towards the unwanted incident, the threat or the asset's vulnerability (or a combination of these). The desired effect of a treatment is reducing risk frequency and/or consequence (i.e. risk value) to an acceptable level.

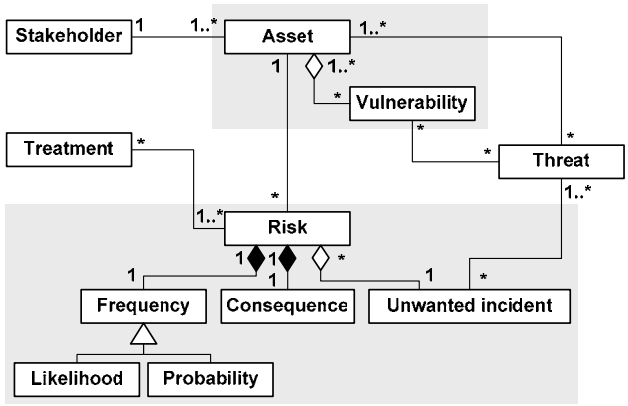

Figure 1 – The conceptual model that was used as basis for the survey

3. Survey design

This section describes the subjects, the material and the analysis model.

3.1 Subjects

We aimed to select subjects representative for participants in a risk analysis. In an IT-system risk analysis the participants have various competence on risk analysis, but they are experts on one or more aspects of the IT-system assessed. Our investigation did not consider a specific system, therefore we included subjects with general experiences from IT-system development. The 57 subjects represent four groups:

- 12 professional researchers, including 2 industrial psychologists, from the Institute for Energy Technology (IFE), who had competence on developing safety critical systems for nuclear power plants (http://www.ife.no)
- 22 professional researchers, including 3 industrial psychologists, from SINTEF ICT (Information and Communication Technology), who had competence on software development, modeling, and usability studies (http://www.sintef.no)
- 14 master students in informatics who were attending a network security course at the University of Oslo (http://www.uio.no)
- 9 master students in informatics who were attending a safety critical software development course at Østfold University College (http://www.hiof.no)

The subjects from SINTEF ICT were paid for the time they spent on the survey, while the students and the IFE professionals received no payment. The students ranged from some experience with risk analysis to none, while the professionals ranged from high competence on risk analysis to only superficial knowledge. The subjects received no training or introduction to our conceptual model in advance.

3.2 Material

The subjects were given a multiple choice questionnaire with 16 questions or statements about risk analysis terminology (see frame below). The material was distributed in English due to several reasons: the CORAS method is documented in English, it is also common for Norwegian companies to use English in reports and presentations, and higher education in software engineering is mainly based on English literature. This means that within software development good skills in English is essential.

The subjects had to judge each answer alternative as either *false, partly false, partly true, true* or *uncertain*. The questionnaire covers risk analysis concepts and their relations; and the subjects were given 20-25 minutes to complete it. Please note that even if the questionnaire occasionally uses the term "security analysis", the risk analysis terminology tested is general and therefore not restricted to security-focused analyses.

1) Which roles could you have in a risk analysis?
2) How well do you know risk analysis terminology?
3) What can be considered as assets in a security analysis?

a. customer register
b. a company brand
c. critical system services
d. human lives
e. equipment
f. source code
g. a company's strategies
h. employees' competence

4) What is true about the relationship between risk and asset?
   a. a risk can harm or reduce the value of the asset
   b. a presumption for a risk to arise is that there are vulnerabilities for someone to exploit
   c. a risk will harm or reduce the value of an asset
   d. one risk may harm more than one asset
5) What is the difference between a risk and an incident scenario for an asset?
   a. an incident scenario is an actual event that can harm the asset but without a frequency or consequence value
   b. a risk for an asset is an unwanted incident assigned a consequence and frequency value
   c. an unwanted incident cannot be part of more than one risk
6) The goal of a treatment can be:
   a. to reduce risk
   b. to remove a threat
   c. to remove a vulnerability
   d. to reduce a threat
   e. to remove a risk
   f. to reduce a vulnerability
   g. to remove an unwanted incident
7) What is true about treatment?
   a. it is usually directed towards a vulnerability
   b. it is usually directed towards a threat
   c. it is usually directed towards an unwanted incident
   d. it is always directed towards a risk
   e. it can be directed towards both a vulnerability and threat
   f. it cannot be directed towards both a vulnerability and an unwanted incident at the same time
   g. it cannot be directed towards both a vulnerability, a threat and an unwanted incident at the same time
8) When will a treatment be considered successful?
   a. if it reduces risk frequency
   b. if it reduces risk consequence
   c. if it makes the risk value acceptable
   d. if it eliminates the risk
   e. if it reduces both frequency and consequence
9) What is the relationship between frequency, likelihood and probability?
   a. the term frequency comprises both likelihood and probability
   b. likelihood is measured qualitatively
   c. probability is measured quantitatively
   d. frequency is measured only quantitatively
   e. likelihood is measured as a value between 0-1
10) What can be used to calculate risk value?
   a. probability and frequency
   b. likelihood and consequence
   c. consequence and frequency
   d. consequence and probability
   e. frequency and likelihood
11) What is a risk composed of?
   a. a consequence, a frequency, a probability and an unwanted incident
   b. a probability, an unwanted incident and a consequence
   c. a consequence and a frequency and an unwanted incident
   d. none of the alternatives above
12) What is the relationship between risk and unwanted incident?
   a. a risk is part of an unwanted incident
   b. a risk initiates the unwanted incident
   c. an unwanted incident is part of a risk
   d. an unwanted incident can be a part of more than one risk
13) When can one consider an unwanted incident a risk?
   a. when it has a consequence, but not necessarily a frequency
   b. when it has a frequency, but not necessarily a consequence
   c. when it has both a frequency and a consequence
14) What is true about vulnerability?
   a. it can be a weakness or lack of the asset itself
   b. it can be a weakness or lack of the asset's surroundings
   c. a threat can exploit vulnerabilities
15) What can be considered a threat?
   a. hardware
   b. people
   c. software
   d. an event (initiated by a person)
16) What is true about threat?
   a. a threat can initiate an unwanted incident
   b. a threat can constitute a risk even if there are no vulnerabilities to exploit
   c. a threat can potentially reduce the value of a n asset
   d. a risk is always associated with a threat
   e. a threat is not necessarily connected to a risk

3.3 Analysis model

The data was analyzed with respect to three aspects: (1) to what extent do the subjects answer correctly without being properly trained? (2) Is there any difference between the students' score and the professionals'? (3) Which concepts and relations are particular difficult or easy to understand? The two categories partly true and true were considered as one positive category, partly false and false constitute one negative category, while uncertain was one category on its own. The reason for combining categories is that one can probably not expect to find one unique definition of a term that everyone agrees to, and as long as the participants in an analysis at least partly agree we consider this a sufficient basis for conducting a successful analysis. The difference between the two groups was investigated using a one tailed t-Test, α=0.05.

4. Results from questionnaire

Table 1 provides the results from the questionnaire showing the number of answers for each alternative regarding question 3-16.

Table 1 – Results

	# false	# partly false	# uncertain	# partly true	# true
3a	2	4	6	12	33
b	14	6	15	8	14
c	1	2	5	8	41
d	10	2	8	6	31
e	1	3	6	14	33
f	2	2	7	16	30
g	10	7	12	11	16
h	10	10	8	13	16
4a	0	0	4	6	47
b	3	8	3	13	30
c	32	8	7	7	3
d	0	1	6	7	43
5a	5	2	12	12	26
b	4	1	11	11	30
c	30	7	15	2	3
6a	1	3	5	7	40
b	8	4	13	7	25
c	2	2	7	7	38
d	5	5	8	11	28
e	6	6	7	11	27
f	2	4	5	12	34
g	15	4	11	4	22
7a	3	4	7	19	22
b	6	8	15	17	8
c	6	4	15	16	13
d	6	6	10	11	22
e	2	7	10	12	25
f	18	8	22	2	5
g	17	6	21	3	8
8a	5	1	4	19	26
b	2	2	5	25	21
c	2	2	6	14	32
d	5	2	2	8	39
e	1	4	4	18	29
9a	10	7	17	7	15
b	4	0	22	10	20
c	2	1	10	9	33
d	7	4	10	12	23
e	12	4	27	4	9
10a	18	4	11	10	13
b	8	4	24	10	11
c	4	4	14	13	22
d	2	4	15	15	21
e	22	2	20	9	4
11a	16	5	14	8	13
b	10	4	17	7	19
c	14	3	15	13	11
d	38	0	7	3	6
12a	25	8	9	7	6
b	23	3	6	9	15
c	5	2	4	19	26
d	3	0	4	7	41
13a	22	4	7	12	10
b	29	11	11	3	1
c	2	1	4	8	40
14a	7	4	9	13	22
b	2	5	9	12	26
c	3	2	2	10	38
15a	6	9	9	7	24
b	2	0	3	9	42
c	2	3	6	7	39
d	5	0	1	5	45
16a	5	3	1	11	35
b	14	9	15	8	9
c	1	1	8	15	30
d	10	3	11	15	15
e	9	4	22	4	15

Mean score for the subjects was: 38.5 (58.6%) correct, 15.5 (23.6%) wrong and 11.7 (17.8%) uncertain answers (Figure 2). With respect to wrong and uncertain answers there is no significant difference between the two groups, but for correct answers the professionals score better (Figure 3, Table 2).

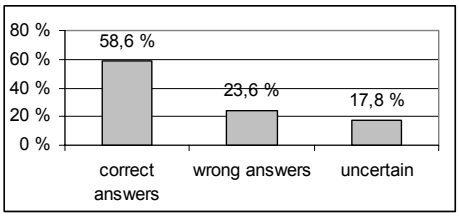

Figure 2 – Mean result

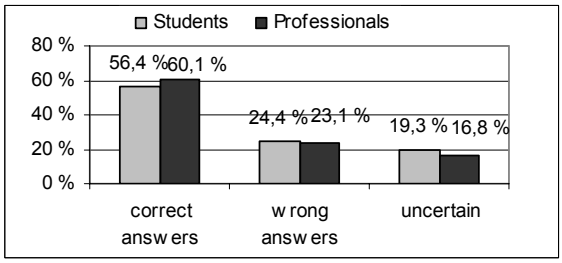

Figure 3 – Students vs. professionals

Table 2 – t-Test

	Students	Professionals
Mean, correct answers	36,2	40,1
t value	-1,89797	
P(T<=t) one-tail	0,032378	
Degrees of freedom	41	

5. Discussion

The underlying assumption for this work is that many potential risk analysis participants know some risk analysis terminology from their daily language, but we do not know whether their interpretation is in accordance

with standard IT risk analysis definitions. The 57 subjects had different backgrounds, but everyone was either studying software engineering or working in an IT-system development environment. Their experience with risk analysis of IT-systems ranged from beginners to experts risk analyst. The results from the questionnaire show that even without being trained in risk analysis, the subjects had a good understanding, or interpretation, of the most important risk analysis terms. In average the subjects obtained 58.6% correct answers, a fairly high number. Some concepts showed more difficult than others (e.g. risk, likelihood) and it would be interesting to see whether similar results are obtained with native English speakers.

We found a difference between the two groups' mean score (p=0.03) in favor of the professionals. This was expected since many of the professionals work with risk analysis-related topics. Rather than the difference between the groups, the main issue in this investigation was the interpretation of the terminology.

In the remaining of this section we discuss the findings related to concepts that were found particular difficult or very intuitive in this order: (1) *asset* and *vulnerability*, (2) *risk, unwanted incident, frequency measures* and *consequence*, (3) *treatment* and (4) *threat*. Questions from the questionnaire are referred to using "Q" + their number, i.e. "Q5" means "question number 5".

5.1 Concerning asset and vulnerability

We asked the subjects what they consider as *assets* in a security analysis (Q3) and the result is shown in Figure 4. Under half of the respondents (39%) think of "company brand" as an asset in a security analysis, even though brand name can be more expensive to repair/replace than "equipment". In fact 35% mean that the company brand is *not* a relevant asset in a security analysis.

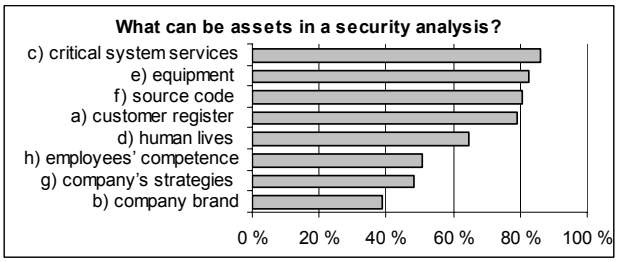

Figure 4 – Assets in a security analysis

We can see from these results that "things" are considered more important than "intangible" assets like company strategies. While security used to focus on protecting physical belongings or valuables, one is now concerned about securing information, reputation, strategies etc. as well. According to these results we can assume it to be challenging to make the participants in an analysis realize what their intangible assets are and also assign them appropriate values. Experience from our industrial field trials supports this assumption; often the participants find identification and valuation of assets particularly hard.

"Employee's competence" was included as an alternative seen from a company's perspective, meaning the risk of loosing core competence. Later we have realized that it is possible to interpret this from an employee's point of view, i.e. the risk of an unwanted incident harming his/her competence, which was not the intention and therefore it will not be discussed.

A *vulnerability* is always associated with an asset. In practice a vulnerability can be either an aspect of the asset itself (a too simple password) or in its "surroundings" (the password stored in clear text). More of the subjects (70%) think of a vulnerability as a weakness in the asset's surroundings rather than a part of the asset itself (64%) (Q14). Both interpretations are covered by our conceptual model, and do not seem to create particular problems. The model also lets one vulnerability yield for more than one asset, which often is the case.

A large group (75%) agrees that there have to be vulnerabilities to exploit before a risk can arise (Q4). In practice this means that it is possible to limit the scope of the analysis to only consider assets that have vulnerabilities.

5.2 Concerning risk, unwanted incident, frequency-measures and consequence

Risk is the most important term in a risk analysis. Nevertheless our studies have shown that it is one of the most difficult terms to fully understand. According to our definition, a risk can be understood as the relation between one unwanted incident and one asset, which means that one risk is only associated with one asset. Unfortunately the results show that 88% believe *one* risk may harm more than one asset (Q4). The rationale for our definition is to cover the cases where an *unwanted incident* harms more than one asset and the consequences or frequencies are different. To specify this case they should be considered as two different risks (Figure 5) which also makes it possible to specify different and more specialized treatment alternatives.

Figure 5 – One unwanted incident: two risks

We do not think the conceptual model should be changed to reflect the subjects' interpretation, but we will have to emphasize the special risk-asset relation when

conducting risk analysis. Nevertheless, 80% agree that an unwanted incident is a part of a risk (Q12) and also that it can be part of more than one risk (65% in Q5 and 87% in Q12). This means that the relationship between risk and unwanted incident seems quite clear. When 46% think a risk can *initiate* an unwanted incident (Q12), we believe this is due to the misunderstanding that a risk is the same as a threat.

More people think a risk *can harm* than *will harm* an asset (93% vs. 18%, Q4) which means that risk is seen as something "potential", i.e. something that may or may not happen and this is in accordance with the definition of the term. In our previous survey [13] we also found that people were reluctant to accept the statement "a risk is something that will reduce the value of an asset" due to the use of "will".

A majority (72%, Q5) believes a risk is an unwanted incident assigned a consequence and a frequency value, a high number that contradicts the result for Q11 where few subjects were able to state what a risk is composed of. This gives us reasons to suspect that the subjects did not truly understand Q5. The fact that the subjects are inconsistent in their answers indicates that risk analysis concepts can be quite confusing.

The terms *frequency, probability* and *likelihood* create a large amount of uncertainty (Q9). Frequency measures were also a problem in our previous survey. This survey shows that likelihood has not a unique interpretation as qualitative, 39% are uncertain whether it is measured qualitatively or quantitatively, and 48% say they are uncertain on whether it is measured as a value between 0-1. Even though the term likelihood is difficult, we need a frequency measure that is not quantitative. In risk analyses of IT-systems, one seldom has the appropriate frequency statistics and one has to rely on expert judgments. The definition of likelihood covers both probability and frequency and in our revised conceptual model likelihood will be used. The term itself will still be subject to further investigations, e.g. will native English speakers find it complicated as well? One of the disadvantages of using qualitative measures is that it makes it more difficult to calculate risk severity using a traditional risk analysis technique like Fault Tree Analysis (FTA) [5] which requires quantitative input.

Risk value is a term that people without risk analysis background will find hard to understand (Q10). Nevertheless many managed to select the correct alternatives for calculating risk value: "consequence & probability" (63%), "consequence & frequency" (61%), but only 39% chose the alternative "consequence & likelihood". We believe that a large group of the subjects guessed, or deduced what a risk value is and chose the statements in Q10 that contained "consequence" plus a frequency measure, i.e. recognized that probability, likelihood, and frequency are the same kind of measure.

Probability is without doubt seen as a quantitative measure (78% agree in this) and most subjects (63%) think frequency is measured only quantitatively (Q9). All alternatives containing likelihood obtained a higher uncertainty rate than the others. It is up to the risk analysis team to decide on which measure to use in an analysis, but probability seems to be the one that is easiest understood.

When it comes to identifying which components a risk consists of, the subjects get quite confused (Q11). The majority (70%) believes it is one of the alternatives presented, but is unable to choose the correct one. As many as 17% do not believe it is any of the alternatives even though they according to the definition are all correct (alternative "a" includes more information than strictly necessary to characterize a risk).

Figure 6 shows that almost everyone (87%) will consider an unwanted incident as a risk if it has both frequency and consequence (Q13). Interestingly, 40% think an unwanted incident with consequence is a risk, while only 7% consider an unwanted incident with frequency a risk (Q13). Again this shows that frequency is a difficult concept and that consequence is more easily associated with risk.

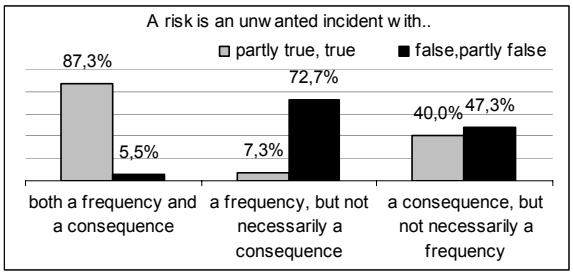

Figure 6 – Unwanted incident and risk

5.3 Concerning treatment

In the questionnaire we asked what the *goal* of a treatment is (Q6) and where one usually applies it (Q7). In Figure 7 we see that it is more common to consider "reduce risk" as the goal than "remove risk". The subjects are reluctant to choose alternatives that include "remove", an option which probably seems more unlikely than "reduce". When it comes to *where* to apply the treatment, our model says that a treatment is directed towards a risk, without specifying exactly how, and a large group of the subjects agrees (60%) A treatment can be applied to anything that contributes to the occurrence of the risk. Most of the subjects believe a treatment is something one applies to a vulnerability (75%), which is similar to the results from our previous survey. It is more unusual to think of treatments directed towards threats (46%) or unwanted incidents (54%). In field trials we have

experienced that the participants are more likely to come up with treatments that help reduce frequency (avoid incidents from happen) than treatments applied to reduce the consequences after incidents have happened.

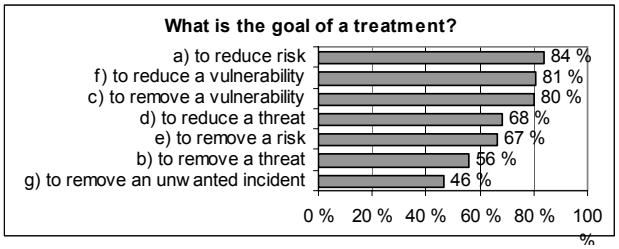

Figure 7 – The goal of a treatment

With respect to whether it is allowed to apply a treatment to more than one entity (e.g. treating both vulnerability and unwanted incident at the same time) the uncertainty rate increases.

We asked when a treatment is to be considered successful (Q8), but have later found the intention behind this question a bit tricky to "get". Nevertheless, the essence of the answers clearly indicates that the subjects believe a successful treatment should reduce frequency and/or consequence. Almost everyone (84%) considers a treatment successful if it *eliminates* a risk, which implies reducing frequency and/or consequence to zero.

5.4 Concerning threat

We distinguish between what a threat *is* and what it can *do*. When we asked what a threat is in Q15, it was most common to consider people (91%) and events initiated by people as threats (89%), then software (81%) and hardware (56%) (Figure 8). This means that an *event* is seen as a threat, even if there is a person behind it. This contradicts our definition where we consider the entity (human or non-human) that *initiates* the event as the real threat. Neither an explosion nor a security breach starts by itself, and the first step to solve the problem is to identify the source or initiator.

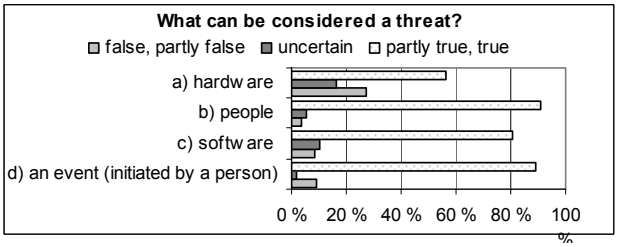

Figure 8 – Potential threats

A surprisingly large group means that hardware cannot be a threat (27%), even though hardware failure most certainly can initiate unwanted incidents that may affect an IT-system.

In [9] a threat is specified to be *human* or *environmental*, while [1] simply speaks of identifying the "cause of event" and [11] categorizes threats as either *accidental* or *intentional*. In field trials we have experienced that the participants are well aware of the latter two, but less aware of non-human threats. To emphasize that a threat can also be non-human we will include *human threat* and *non-human threat* as specializations of threat in our revised model.

The subjects mean that a threat has the ability to exploit vulnerabilities (87%, Q14). The majority (84%, Q16) also thinks that a threat can initiate an unwanted incident and that it can potentially reduce the value of an asset (82%). The subjects seem to be more uncertain whether or not a threat can constitute a risk even if there are no vulnerabilities to exploit (42% agrees and 27% are uncertain). Our model says that there have to be a vulnerability to exploit before one can speak of a risk. We define a risk to be associated with at least one threat, i.e. one initiator, and 56% of the subjects agree. On the other hand, we do not say that a threat has to be associated with a risk, but 24% disagree in this and 40% are uncertain. This relation is obviously quite difficult to comprehend. We believe that if one has identified a risk, meaning identified an unwanted incident with frequency and consequence, then it is likely that one also has identified *what* or *who* initiates the unwanted incident, i.e. the threat. A threat in itself is not associated with a risk unless there is a possibility of it initiating an unwanted incident. Therefore a risk is always related to one or more threats, but a threat is not necessarily related to a risk.

6. Threats to validity

We have developed a conceptual model inspired by the one from CORAS which includes the most important terms from the CORAS risk analysis method. The terms' definitions are taken from the international standards [1-3, 9]. We do not attempt to cover all possible risk analysis terms.

The subjects were not native English speakers and the interpretation of the statements could have been affected by this. The survey should be replicated with native English speakers to compare the results. Questionnaires formulated in natural language will always have room for misinterpretations. We did notice some minor vagueness in the text after the first run, but since the survey was to be replicated we did not change the material. The conclusions drawn from the material has taken into account the potential misleading questions.

Participation was voluntarily and we do not know whether this affected the results. The subjects had various competences in one or more of the following domains (1)

system modeling and design, (2) risk analysis and system development in the safety domain and (3) system development and security. The system modeling and design group had all heard a little about CORAS, but only a few had used it themselves. The professionals from the safety domain all knew something about software development and risk analysis, but less about security-focused risk analysis. The safety students knew some conventional risk analysis, and the security students were unfamiliar with both conventional risk analysis and security-focused risk analysis. A risk analysis team may very well be composed of people with similar knowledge of risk analysis as our subjects.

Even though we used master students attending a security course, it would have strengthened our results further if we had a group of professionals from the security domain like we had from the safety domain.

7. Conclusion

The paper reports on the results from a survey concerning the understanding of risk analysis terminology. The mean score for the group was 58.6% correct answers, which supports our assumption that many of the terms we have in our conceptual model are well understood even by people without training in risk analysis. Being more experienced in risk analysis, the professionals obtained a higher number of correct answers than the students.

7.1 Asset & vulnerability

Assets are something of value to the system stakeholder, but getting the participants to fully understand the notion of *asset* appears challenging. Traditionally assets are considered physical entities, but in IT-systems assets are often intangible objects like information, company reputation/brand etc. These can be both hard to identify and value appropriately. During our field trials we have experienced that the participants find it very hard to value an intangible asset in terms of money.

Assets are subject to weaknesses that make them vulnerable to threats. In our conceptual model a vulnerability is associated with one or more assets, but it is not a part of the asset. In this survey we found that it is most common to think of a vulnerability as something in the asset's surroundings, meaning that our model does not conflict with the subjects' interpretation.

7.2 Risk

We define a risk to consist of an unwanted incident, a frequency and a consequence (Figure 9), and the subjects appear to have a clear understanding of an unwanted incident being a part of risk. On the other hand, it seems more complicated to know when an unwanted incident can be characterized as a risk. It looks like the subjects believe it is sufficient to establish the potential effect of the unwanted incident, but not how often it will occur. When the subjects were to judge whether an unwanted incident is a risk, it appears that a serious consequence is more important than a high frequency. This belief is reflected in the difficulties the subjects experienced with frequency measures, a concept that is less used in the daily language and associated with more uncertainty. In a real system, an unwanted incident that happens every day but with low consequence may over time cost just as much as a rare event with a serious consequence.

It is common to confuse how risk and unwanted incident relate to asset. In our definition an unwanted incident may harm more than one asset, but a risk is only associated with one asset. This enables us to describe an unwanted incident that has different consequence and/or frequency for a set of assets. The challenge is to make the participants understand that a risk is an "abstract" concept, while the unwanted incident is the "real" event.

Most of the subjects seem to have the correct interpretation of risk as something potential, meaning it *can happen*, not that it *will happen*, but still it should be emphasized that the risk is not only the incident (Figure 9).

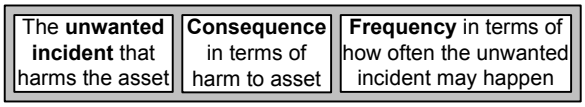

Figure 9 – Risk components

Our previous survey tested the understanding of probability and later included this as a frequency measure because it was a well understood concept. In this survey we also included likelihood, which is a qualitative frequency measure. Likelihood was found to be a difficult and unfamiliar term without a unique interpretation. The problem may be that likelihood often is associated with mathematics and therefore people react to its definition as qualitative. In an analysis one seldom has appropriate quantitative data available, and one needs a qualitative measure similar to likelihood that can be estimated from experience or other relevant information. In lack of a better term, likelihood is included because of its suitable definition. Since it is more general than frequency (and probability) it will replace frequency in the revision of our conceptual model.

7.3 Treatment

Most subjects consider the goal of a treatment to be to *reduce* risk or *reduce/remove* vulnerabilities. The subjects

consider a treatment as successful if it reduces the frequency and consequence of a risk, or if it eliminates risk. More subjects think a treatment is successful if it reduces consequence than if it reduces frequency. In our definition, a treatment is successful if it reduces consequence and/or frequency to an acceptable risk level. On the question of what it is most common to treat, most subjects gave priority to vulnerability and thereafter risk. This does not contradict our model where we define a treatment to be directed towards a risk, without specifying whether this means treating a vulnerability, a threat or an unwanted incident or a combination of these.

7.4 Threat

Human beings are most commonly viewed as threats, followed by *events* even if they are initiated by a person. According to our definition the initiator of the unwanted incident is regarded as the real threat and one needs to emphasize this. Surprisingly many do not consider hardware a threat. The concepts that most think of as threats are those involving humans which means that the term threat is interpreted as one with ability to do something. To emphasize that a threat can be *human* or *non-human*, this specialization will be included in our revised model.

7.5 Revising the conceptual model

The conceptual model of risk analysis terminology used as basis for our survey, intend to incorporate the common risk analysis terms from CORAS and the interpretations of these. The results from the survey show that it successfully reflects the subjects' common understanding of the risk analysis terminology. Still we like to make some minor adjustments based on the findings from this survey. To increase the awareness of non-human threats the model should specify threat as *human threat* and *non-human threat* (Figure 10).

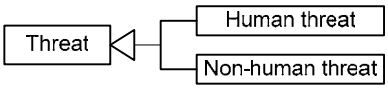

Figure 10 – Specializing threat

The current specialization of frequency into probability and likelihood is not satisfactory. Both frequency and probability are measures that can be covered by likelihood.

7.6 Further work

The findings from this survey will be used in the development of a graphical modeling language for risk scenarios. The abstract syntax of the language will match our final conceptual model. These investigations will contribute to make the language as intuitive and easy to understand as possible. Our further hypothesis is that the relations that were found easy to understand in this survey will also be most suitable and appropriate to model in a simple and straight forward manner, while the difficult concepts will need a more complex representation. This will be investigated in our further work.

Acknowledgements

The research on which this paper reports has partly been funded by the Research Council of Norway project SECURIS (152839/220). The authors thank Monica Kristensen (IFE), Lasse Øverlier (Norwegian Defence Research Establishment) and Jan Heim (SINTEF ICT) for valuable assistance and input. We are also grateful to the subjects for their participation.

References

[1] Australian/New Zealand Standard for Risk Management (AS/NZS 4360), 1999.
[2] British Standard BS4778: Quality vocabulary: Availability, reliability and maintainability terms. Glossary of international terms, 1991.
[3] HB 231:2000 Information security risk management guidelines, 2000.
[4] IEC 812 (IEC60812): Analysis techniques for systems reliability - Procedures for Failure Mode and Effects Analysis (FMEA), 1985.
[5] IEC 1025: Fault Tree Analysis (FTA), 1990.
[6] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems, 1998-2000.
[7] IEC 61511: Functional safety - Safety instrumented systems for the process industry, 2004.
[8] ISO 14121: Safety of machinery - Principles for risk assessment, 1999.
[9] ISO/IEC 13335: Information technology - Guidelines for management of IT Security, 1996-2000.
[10] ISO/IEC 17799: Information technology - Code of practice for information security management, 2000.
[11] ITU-T X.800: Security architecture for open system interconnection for CCITT applications. (Technically aligned with ISO 7498-2), 1991.
[12] I. Hogganvik and K. Stølen, "Empirical Investigations of the CORAS Language for Structured Brainstorming," SINTEF ICT, Technical report STF90 A05041, January 2005.
[13] I. Hogganvik and K. Stølen, "On the Comprehension of Security Risk Scenarios," in Proc. International Workshop on Program Comprehension (IWPC), pp. 115-124, 2005.
[14] F. Redmill, M. Chudleigh, and J. Catmur, *HAZOP and Software HAZOP*: Wiley, 1999.
[15] J. Rumbaugh, I. Jacobson, and G. Booch, *The Unified Modeling Language Reference Manual*: Addison Wesley, 1998.