Risk Management in Projects

Case study: Risk Management in Fennovoima from Security Perspective

Turvallisuusjohdon Koulutusohjelma

Tutkielma

Matti Peltola

Kaukomarkkinat Oy

Helsinki 24.4.2015

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Kyky ymmärtää riskienhallintaa sekä pystyä kommunikoimaan riskienhallinnan merkitys on erityisen tärkeää riskialttiissa ympäristöissä, kuten ydinvoimateollisuus. Siksi riskienhallinnan teoria osana turvallisuusjohtamista on nostettu tämän tutkielman perusteella keskeiseksi menestystekijäksi Fennovoima hankkeessa. Riskienhallinnan ymmärryksen lisäksi kyky ja valmius toimia poikkeustilanteissa oikein ovat erittäin tärkeitä elementtejä turvallisuus näkökulmasta.

Ilman etukäteen tehtävää riskien tunnistamista ja suunnittelua yritys voi päätyä vaikeuksiin projektin aikana. Siksi osana projektia tärkeimmät riskit olisi aina syytä selvitettävä etukäteen ja osa riskeistä tulisi poistaa tai minimoida. Projekteissa yleisimmät riskit liittyvät talousarvioon ja projektin aikatauluun, mutta yhtä hyvin riskit voivat liittyä ympäristöön, tietoverkkoihin, henkilöstöön tai johonkin muuhun kokonaisturvallisuuden osa-alueeseen. Yleisimpiä menetelmiä analysoida projektiin sisältyviä riskejä ovat riskimatriisi, haavoittuvuusanalyysi ja skenaarioanalyysi.

Tämän tutkimuksen tavoitteena on tunnistaa, mitkä tekijät ovat erityisesti otettava huomioon projektien riskienhallinnassa ja mitkä ovat tärkeimmät asiat projektien riskienhallinnassa turvallisuus näkökulmasta. Tutkimuskysymykset ovat: miten roolit ovat jakautuneet turvallisuuden ja riskienhallinnan osalta Fennovoima projektissa? Mitä eri sidosryhmiä on riskienhallinnan otettava huomioon ja mitkä ovat heidän roolinsa osana riskien hallintaa ja turvallisuutta?

Fennovoima Oy:n riskienhallinta on jaettu kolmeen osaan; taloudelliset riskit, tuotantoprosessiin liittyvät riskit ja turvallisuus riskit. Kaikilla kolmella ryhmällä on oma organisaationsa ja jokainen niistä valitsee itsenäisesti riskienhallinta menetelmänsä. Fennovoima projektissa tärkeimmät sidosryhmät turvallisuuden näkökulmasta ovat STUK, työntekijät, johto, viranomaiset ja omistajat. Tärkein sidosryhmä on koko henkilöstö sisältäen erilaiset alaryhmät kuten johto ja turvallisuusorganisaatio. Jatkuva turvallisuuskoulutus ja riskien tunnistamien on yksi tärkeimmistä osa-alueista johon turvallisuus organisaation tulisi keskittyä. Lisäksi tulisi varmistaa organisaation kyky toimia ja reagoida tilanteiden vaatimalla tavalla. Omistajat ja STUK vaativat jatkuvaa ja toimivaa vuorovaikutusta turvallisuusorganisaation kanssa.

Abstract

The ability to reliably determine and understand risk management, and being able to solidly quantify and communicate risk management value is especially important in risky environments such as nuclear power industry. This is why risk management theory as part of security management has been lifted out as key determinant for success in Fennovoima Project. Organizations everywhere speak about managing risks, but very few may have the knowledge and the readiness to eliminate all the risks. Moreover it is important particularly in projects to analyze the risks beforehand because without identifying the risks the company may end up into difficulties during the project. As part of project, risk analyses should be carried out and the most important risks should be always identified and minimized. In projects, the most common risks are related to budget and schedule as well the risks can be related to the environment, IT technology, personnel or some other aspect of the enterprise risk management area. The most common tools for analyzing risk are risk matrix, vulnerability analysis and scenario analysis.

This research aims to identify which factors should be considered in risk management in projects and what are the major characteristics of project risk management in the eyes of the security management. This study raises two categories of questions: What are the roles of the security management and the risk management in the project? What stakeholder groups should be considered in risk management process and what are their roles in risk management and security?

Fennovoima risk management is divided into three parts which are financial risk, process related risks and security risks. All of the groups have their own organization and each of them selects independently methods for securing the critical factors. The main stakeholders from security perspective includes; STUK, personnel and the owners. From the security perspective the whole personnel's continuous security and safety training is one of the key areas to focus and measure. In addition owners and STUK requires well working communication with the security team.

The keywords include: risk management, project risk management, security management

Table of Content

1 Introduction

1.1 Structure of the report

This thesis is structured into four chapters

1. Introduction - this chapter outlines the aims, objectives, reasons and significance of the topic under review.

2. Review of current thinking - the main theories within the topic are identified and critically discussed.

3. Investigation - includes discussion of findings. Interpretations are made from the analysis and discussed in context of the literature review.

4. Conclusions - In the final part the conclusions are presented and research questions are answered. Finally recommendations are made on the bases of this study.

1.2 Reason for this Research

Turvallisuusjohdon Koulutusohjelma (TJK) course material classifies risk management as one of the top topics of the whole course. The sponsoring company for this study is Kaukomarkkinat Oy which is a sales company in industrial project sales in the area of security systems. Additionally future sales potential can be seen in project based risk management due to increasing of complexity of working environment which maybe changed into opportunity to offer expertise and consultancy services in the area of risk management. Compared to systems sales, project security sales may offer higher profit margin and competitive advantage. In the energy market which Fennovoima Oy is operating can been seen an increasing pressure towards cost efficiency and streamlined operations due to the price competition, which have lead to situation where many companies are finding it increasingly difficult to cover all the possible risk management

areas by themselves. Also the technological change and globalism may increase the complexity level in processes which likely appear as new opportunities for sales and service companies in the future.

1.3 Personal Objectives

As the result of this research I expect to gain new evidence based knowledge in the area of risk management and discover possible unexpressed problems which may be used as relationship builders and future growth opportunities. Furthermore the information generated through this study is likely to help me in every day management and decision making in the area of risk management. Through this research I would like to know how Fennovoima Oy's risk management process can be seen within the company.

2 Review of Current Thinking

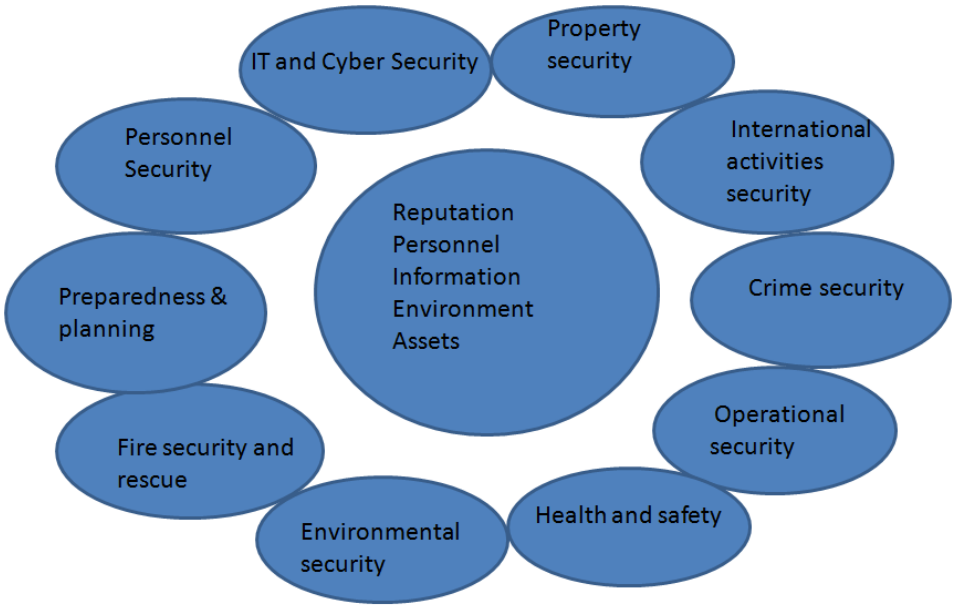
This review of current thinking critically reviews the academic literature in the area of project risk management.

2.1 Principles of Risk Management

Risk management thinking has gained increasing interest in the recent years and a growing number of researchers have emphasized its importance. As the result ISO31000 was published in 2009 as a standard on the implementation of the risks management in order to help organizations increase the likelihood of achieving objectives, improve the identification of opportunities & threats, effectively allocate and use resources for risk treatment. It is stated, that organizations using ISO 31000 can better compare their risk management practices with an internationally recognized benchmark, providing sound principles for effective management and corporate governance (ISO31000, 2009).

Roebuck in 2011 defines risk management as the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities (Roebuck, 2011). According to ISO31000 definition of risk is the 'effect of uncertainty on objectives'. In this definition, uncertainties include events (which may or may not happen) and uncertainties caused by ambiguity or a lack of information. Risk management should include both negative and positive impacts on objectives. According to Bakliwal in 2011 Risk management is simply a practice of systematically selecting cost effective approaches for minimizing the effect of threat realization to the organization. However all risks can never be fully avoided or mitigated simply because of financial and practical limitations. Therefore, all organizations have to accept some level of residual risks (Bakliwal, 2011).

Additionally Taleb, Golstein and Spitsnagel stated in 2009 that instead of trying to anticipate low-probability, high-impact events, risk managers should reduce their vulnerability to them. Furthermore risk management should be about lessening the impact of what is not understood - not a futile attempt to develop sophisticated techniques and stories that perpetuate the illusions of being able to understand and predict the social and economic environment (Taleb;Goldstein;& Spitznagel, 2009). Based on the objectives and tasks of risk management two areas can be identified which are crucial for the design of risk management: strategic risk management and management of operational risks (Sadgrove, 2005). The methods, definitions and goals of risk management vary widely according to whether the risk management method is in the context of project management, security, engineering, industrial processes, financial portfolios, actuarial assessments, or public health and safety (Roebuck, 2011). The relationship between risk management and security management may change from one company to another as this study also justified, however security is increasingly seen as one element of an organization's overall risk management. Overall risk management also includes financial, reputation and legal risks.



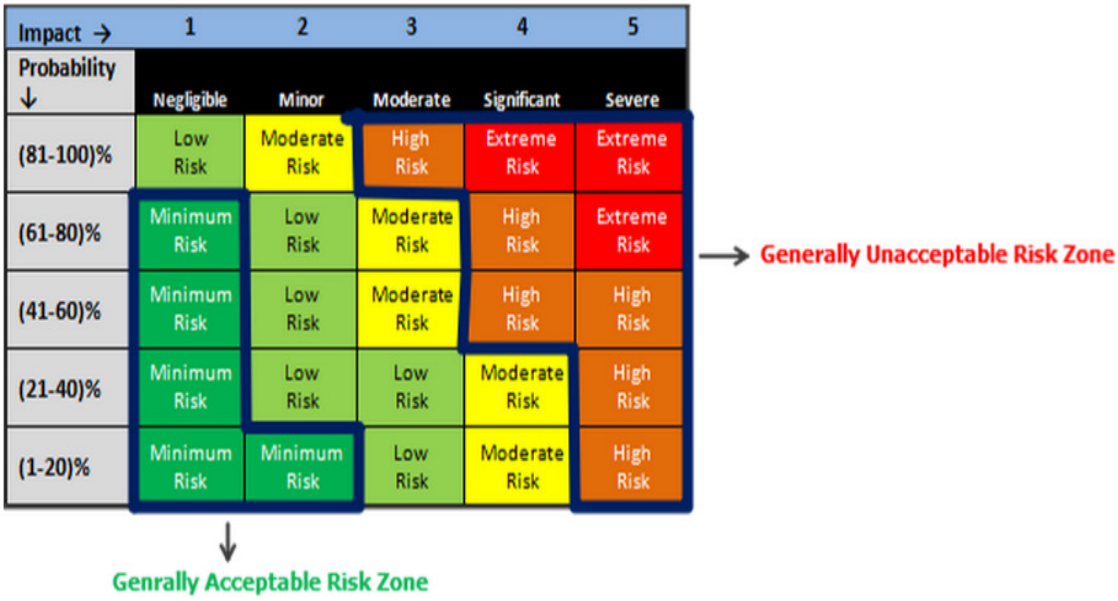
Kuva 1 Security Management Diagram (adapted from TJK13 course material)

In the figure 1 can be seen the diagram which summarizes overall security management tasks which risk management can be seen as one the security

management procedures. In other words management of security risks applies the principles of risk management to the management of security threats.

2.2 Project Risk Management

Anttonen in 2003 and Rissanen 2002 stated that the model of project working has been increasing in the recent years. They also forecast in their studies that project working in generally is going to grow in the future (Anttonen, 2003) (Rissanen, 2002). In order to succeed in project management it is important to analyze risks and manage all risks related to projects. According to them all projects are unique therefore also risks related to projects may be unique this is why management and specialists cannot purely rely on their experience and intuition. In conclusion, it is important particularly in projects to analyze the risks beforehand because without identifying the risks the company may end up into difficulties during the project. As part of project, risk analyses should be carried out and the most important risks should always be identified and eliminated (Pelin, 2002). Even if projects usually include small risks their probability and signification should be minimized to the acceptable level (Silfverberg, 2004). The most common risks in project risk management are usually related to project schedule and budget. The most common tools used in risk analyses are vulnerability analysis and risk matrix (Saarela, 2008). In addition risk scenarios are recognized as powerful tool which help risk professionals to ask the right questions and prepare the management for the unexpected.



Kuva 2 Risk Matrix (Chittoor, 2013)

It is recommended that companies have standard scales on their projects for how risks can be rated. A sample risk matrix is presented in the figure 2, which a scale of 1%-100% will be used for Probability (Chittoor, 2013).

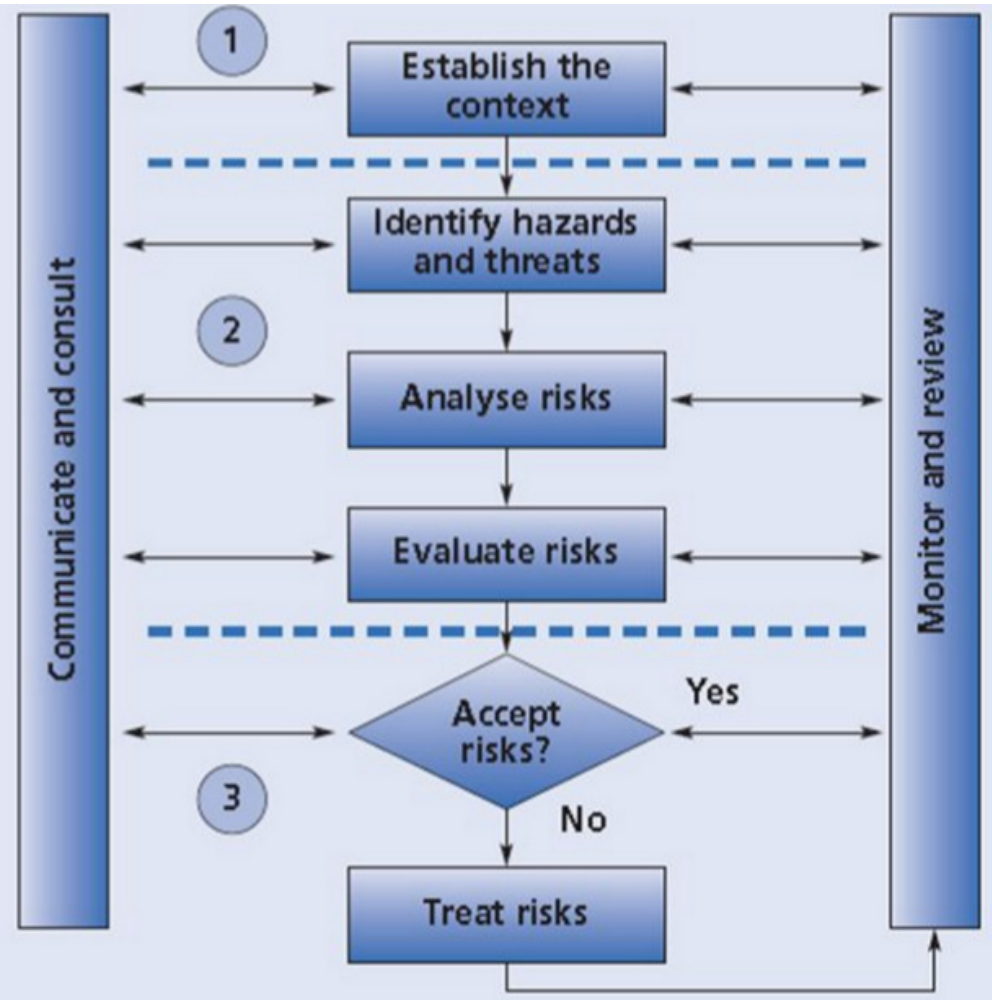
(1-20)% means very low
(21-40)% means low
(41-60)% means medium
(61-80)% means high
(81-100)% means it is a fact

Impact: A scale of 1-5 is normally used for impact ratings where;

1 means negligible
2 means minor
3 means moderate
4 means significant
5 means severe

In generally can be said that good project risk management depends on supporting organizational factors, clear roles and responsibilities, and technical analysis skills. On the other hand Chapman and Ward argued in 2003 that risk management is one of the key tasks for all project managers

in any project. In other words risk applies to any management decision that could have a good or bad outcome (Chapman & Ward, 2003).

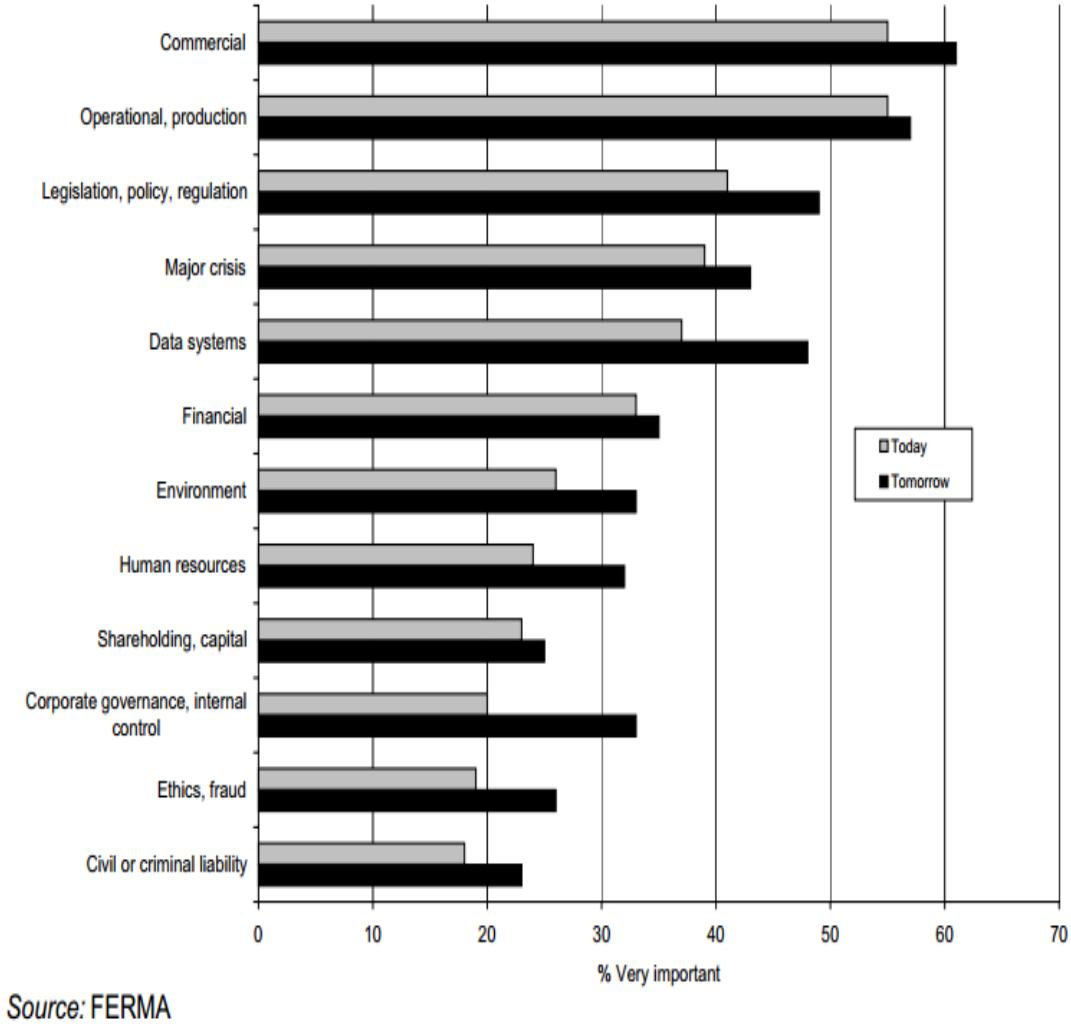


Kuva 3 Process of Risk Assessment (Aggregate Risk Management, 2015)

Project risk management in its entirety, includes the process of several activities which are presented in the figure 3. According to Guide to the Project Management Body of Knowledge the activities of risk management generally includes five different steps which are:

1. Planning risk management
2. Risk identification
3. Performing qualitative risk analysis
4. Planning risk responses
5. Monitoring and controlling risks

(A Guide to the Project Management Body of Knowledge, 2009)



Kuva 4 Risk ranking today and tomorrow

Figure 4 presents risk ranking done by FERMA (Risk Management Associations of Europe) in 2013 which European respondent companies rank the most important risk to their company today and tomorrow. From the figure can be seen that it is estimated that data systems risk ranking is going to increase the most in the future due to the cyber threat.

2.3 Criticism

Taleb, Goldstein and Spitznagel argue in their article in Havard Business Review in 2009 that low-probability, high-impact events are almost impossible to forecast. Moreover the complexity not only increases the incidence of Black Swan events, which failure comes as a surprise with major effect, but in addition to that the complexity makes forecasting even in ordinary events impossible. Taleb et all also criticize in the article that

risks should not be managed by predicting extreme events and studying the past may not help in managing the risk because today's world doesn't resemble the past; both interdependencies and nonlinearities have increased. Finally according to them; risks may not be measured by standard deviation. In other words risk managers should avoid using methods and measures connected to standard deviation, such as regression models, R-squares, and betas because anyone looking for a single number to represent risk is inviting disaster (Taleb, Goldstein, & Spitznagel, The Six Mistakes Executives Make in Risk Management, 2009).

3 Investigation

The aim of the part three is to highlight the key issues related to the Fennovoima Oy and their risk management. In addition, this part answers the first research question; what are the roles of the security management and the risk management in Fennovoima project?

3.1 Fennovoima Oy

Fennovoima Oy is a Finnish consortium of 40 companies that partnered with Rosatom in building the new 1,200 megawatt nuclear plant at Pyhäjoki. Finland set deeper energy ties with Russia after Finnish parliament approved plans for a nuclear plant to be supplied by Russia's state-owned Rosatom despite East-West tensions over the current Ukraine crisis. The project carries a foreign policy risk and some other risks with which are discussed later in this chapter. This makes a successful risk management particularly important for the project. According to this research, risk management in Fennovoima Oy can also be seen as an important part of the company's security management. The nuclear power industry is one of the most comprehensively regulated industries of all. The regulators' demanding risks analyses are numerous and they are not discussed in detailed as part of this study. For example Finnish nuclear power plant requirements obligate that there have to be several defense levels in the case of problems occur in a nuclear power plant. Moreover all of the defense levels must work independently in case any of the defense level falls down. Fennovoima uses three level solutions which include:

1. normal operational system in normal use
2. security systems
3. severe accident security systems

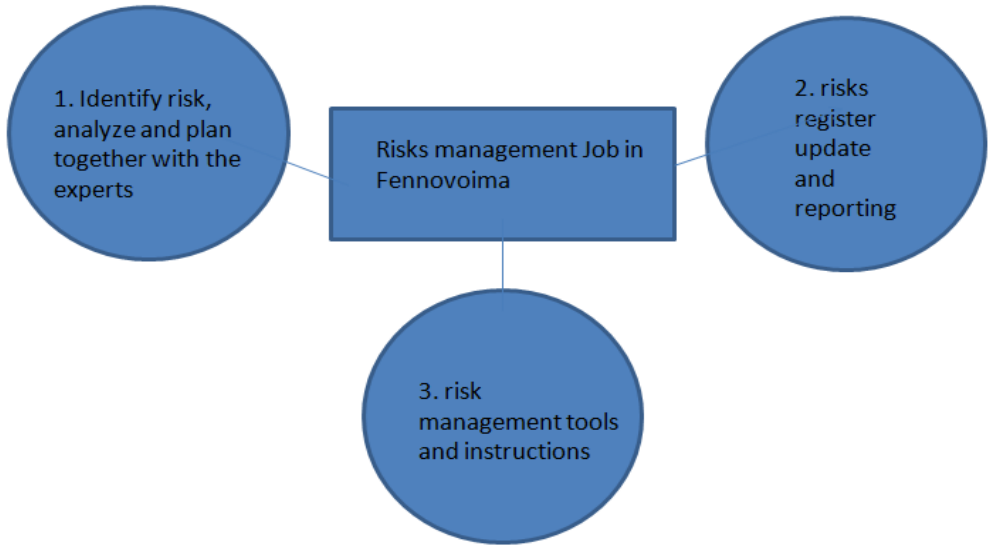
The security operations in Fennovoima are divided into three parts:

1. security of operations
2. information security
3. personnel security

The Fennovoima occupational health and safety policy (OHS policy) defines the principles followed by the management and personnel of Fennovoima to ensure a safe and healthy working environment for themselves and their colleagues. Fennovoima also requires its partners to comply with the principles of this OHS policy when working in Fennovoima premises. Fennovoima's target is zero accidents. Occupational accidents and diseases can be prevented by proactive measures. The commitment of Fennovoima is manifested as taking care of sufficient resources, setting clear and measurable targets and the consistent management of activities. Occupational health and safety activities are systematically managed and developed as part of Fennovoima's integrated management system. In addition to the personnel, Fennovoima provides guidance and training for its partners to obey common safety procedures and guidelines. From the security personnel the main area include: physical security, crime prevention, fire protection and preparedness (Fennovoima.fi/turvallisuus).

3.1.1 Risk management in Fennovoima

In size the risk management and security organization are typical for many industrial organizations in Finland. The organization include specialized such as project risk manager, site security manager, IT security professional, security development manager and security expert. In Fennovoima the risk management is divided into three parts which include; financial risk, process related risks and security risks. All of the three areas have their own organizations' and each of them selects independently methods for securing the critical factors (Lampen, 2015). The security risk management can also be included as part of Fennovoima's overall risk management. Along with the specialists, the employer expects that each employee keeps herself/himself up-to-date on matters regarding corporate security as is required by their own tasks. Finally, the corporate security is based on each employee's attitude, know-how and motivation (Fennovoima.fi/turvallisuus).



Kuva 5 Management tasks in Fennovoima (by author)

The figure 5 summaries Fennovoima Oy's risk management tasks. Risk identification answers the question what risk the company has and analyses are done in order to be able to determine what the risks' impacts are. In the planning stage the firm decides the steps for controlling the risks and determines the critical factors. In the second stage risks are registered systematically and reported usually to company management. In the third step risk management tools and instructions are developed and implemented (Fennovoima.fi/Turvallisuus).

3.1.2 Media Criticism

There have been lots of discussions in the Finnish media for and against Fennovoima project. In March 2015, according to the Finnish media the biggest risks in related to Fennovoima project are:

Profitability of the project (Financial Risk)

Some of the investors that dropped out of the project had concerns about the project's profitability. Even though the profitability may be high the project requires high investment and it takes long to time just to brake-even which increases the financial risks related to the project.

Renewable energy resource (Ethical Risk)

The argument is related to the fact that establishing a new nuclear plant decreases the need to develop renewable energy. It is still unclear now when the plant is in the building stage where to dispose the nuclear waste in the future. There is a big nuclear waste disposal project which is managed by Posiva Oy and Fennovoima is not currently participating to that project.

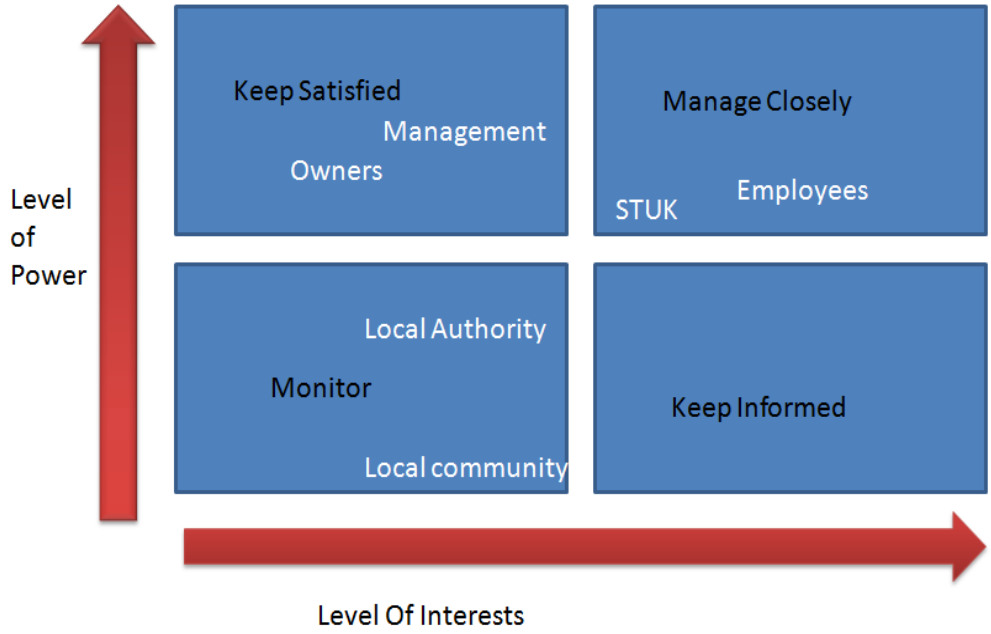
Security of the project (Political risk)

The nuclear fuel for the plant is going to be supplied by TVEL which owned by Rosatom and they are both Russian based companies. In Fennovoima case it is argued that the foreign owner is going to have the full power to control the company which production is going to be a big part of the total energy supply for the whole country. This means that the energy dependency particularly with Russia is going to increase in the future (http://www.fennovoima.fi/ydinvoima/ydinpolttoaine).

The security risks related to the premises are not widely discussed in the media and public briefings from the security organization have not been needed. However the media discussion may provoke some people to try to intrude to the area which makes security management important. (Lampen, 2015)

3.2 Stakeholder Analysis

The second research question is: what stakeholder groups should be considered in risk management process and what are their roles? In order to answer this question stakeholder analysis is presented and later in the conclusion part the findings of the analysis are discussed more detailed



Kuva 6 Fennovoima Stakeholder Analysis (by author)

3.2.1 Owners

One of the major owners of Fennovoima project is Rosatom with 34% share. Rosatom has also background from Russian nuclear weapon industry. According to criticisms in the Finnish media against the Fennovoima project is that Rosatom includes political and ethical risk which may have effect on risk management from the financial perspective. However according to the interview done for this study the background of the company has minor effect on risk management from the security perspective. On the other the legislation and cultural differences between Russian and Finnish nuclear safety - and general safety requirements may cause lots of work which makes the communication between Fennovoima Oy's security organization and the owners important because the owners' interests is to make profit therefore the costs for the security may be cut down without working communication.

3.2.2 Radiation and Nuclear Safety Authority (STUK)

STUK (Säteilyturvakeskus) is the main radiation and nuclear safety authority in Finland. One of STUK's main roles is to set and control of the fulfillment of the safety and security requirements in the nuclear power companies in Finland. STUK's role within nuclear power companies in

Finland and particularly in the safety and security area is very active which means intensive communications between the authority and Fennovoima's risk and security management.

3.2.3 Authorities

Pyhäjoki where the plant is going to be located belongs to Oulu's police district which has hired one fulltime employee for the Fennovoima project. In addition, the local fire & rescue department's role is important from the security perspective. Fennovoima Oy is going to have also they own rescue department later during the project.

3.2.4 Personnel

The fact that the security organization in Fennovoima is not bigger than in companies in generally makes the role of the whole personnel highly important in order to be able to fulfill the high requirements of the nuclear power industry. This makes the good communication between the security organization and all the other personnel vital for the project success.

4 Conclusions

Fennovoima project can be defined as complex and large scale project which makes the project management from security perspective important and unique. Despite the fact that the life cycle for the project is relatively long 64 years the problems related to risk management may be similar to many short terms projects. In other words the company has to start their practices from zero and move fast forward in order to be able to make profit as soon as possible. According to this study the risks management at strategic and operational level is important for the whole project's success.

The stakeholder analyses indicates that the main stakeholders from security perspective include; STUK, personnel and the owners. The owners may not need communication in daily basis such as STUK and personnel require but the owners' role is to make sure that the management has the needed resources for the project. Additionally, the owners and management may have positive influence on the company's security culture development. Nuclear Power industry differs from other industries with higher safety & security regulations and controlling from the regulator (STUK) but in the end the success depends on the company's security and risk management capabilities which makes the company's own personnel the most important stakeholder group in this case. From the security perspective the whole personnel continuous security and safety training is one of the key areas to focus. On the other hand the personnel of the company include subgroups such as management and nuclear security department which may require closer communication. In the end, the management and the whole personnel are needed to prevent accidents and they have to be able to act in the case of emergency. According to this study; the security management may benefit from tripartite dialogue with the management and owners in order to be able to enhance the security policies and security culture within the company. Despite the fact that risk management aims to developed low cost practices

in the complex project like Fennovoima the cost of risk management may rise high which may require supportive argumentation. Today in March 2015 the security policies and design are at their starting therefore it is difficult to analyze the current stage because not much has been done so far. In conclusion, the ultimate question for the success of the security risk management within the company may be related to the security practices and personnel's activity within the company. Additionally the owners and managements supportive roles are vital for the project.

References

A Guide to the Project Management Body of Knowledge. (2009). Project Management Institute.

Aggregate Risk Management. (2015). Retrieved from http://www.aggregate-rm.com/?page_id=16

Anttonen, K. (2003). *Tehosta projektityötä: Johda hanketta 80/20 – periaatteella.* Jyväskylä: Talentum Media Oy.

Bakliwal, V. (2011). *Production and Operation Management.* Pinnacle Technology.

Chapman, C., & Ward, S. (2003). *Project Risk Management: Processes, Techniques and Insights* . Wiley.

Chittoor, A. (2013, 4). *projectmanagers.net*. Retrieved from http://network.projectmanagers.net/profiles/blogs/what-is-a-risk-matrix

Fennovoima.fi/Turvallisuus. (n.d.). Retrieved 4 2015, from http://www.fennovoima.fi/turvallisuus

ISO31000. (2009). Risk Management - Principles and Guidelines.

Lampen, T. (2015, 3 6). Head fo Security in Fennovoima Oy. (M. Peltola, Interviewer)

Pelin, R. (2002). *Projektinhallinnan käsikirja.* Jyväskylä: Projektijohtaminen Oy Risto Pelin.

Rissanen, T. (2002). *Projektilla tulokseen.* Jyväskylä: Kustannusosakeyhtiö Pohjantähti.

Roebuck, K. (2011). *Risk Management Standards.* Emereo Pty Limited.

Saarela, M. (2008). *Riskianalyysi ja riskienhallinta osana onnistunutta hypermediaprojektia.* Retrieved from http://hlab.ee.tut.fi/hmopetus/riskianalyysi-ja-riskienhallinta-osana-onnistunutta-hypermediaprojektia

Sadgrove, K. (2005). *The Complete Guide to Business Risk Management.* Gower Pub Co; 2 edition.

Security Management Diagram. (2013). Turvallisuusjohdon koultusohjelman kurssimateriaali.

Silfverberg, P. (2004). *Ideasta projektiksi Projektisuunnittelun käsikirja.* Helsinki: Finnish Environment Ministry.

Taleb, N. N., Goldstein, D. G., & Spitznagel, M. W. (2009). The Six Mistakes Executives Make in Risk Management. *Harvard Business Review*

Interview

Lampen, T. (2015.03.06). Head fo Security in Fennovoima Oy. (M. Peltola, Interviewer)