Comparison of Risk Analysis Methodologies

Risk Analysis for Better Design and Decision Making

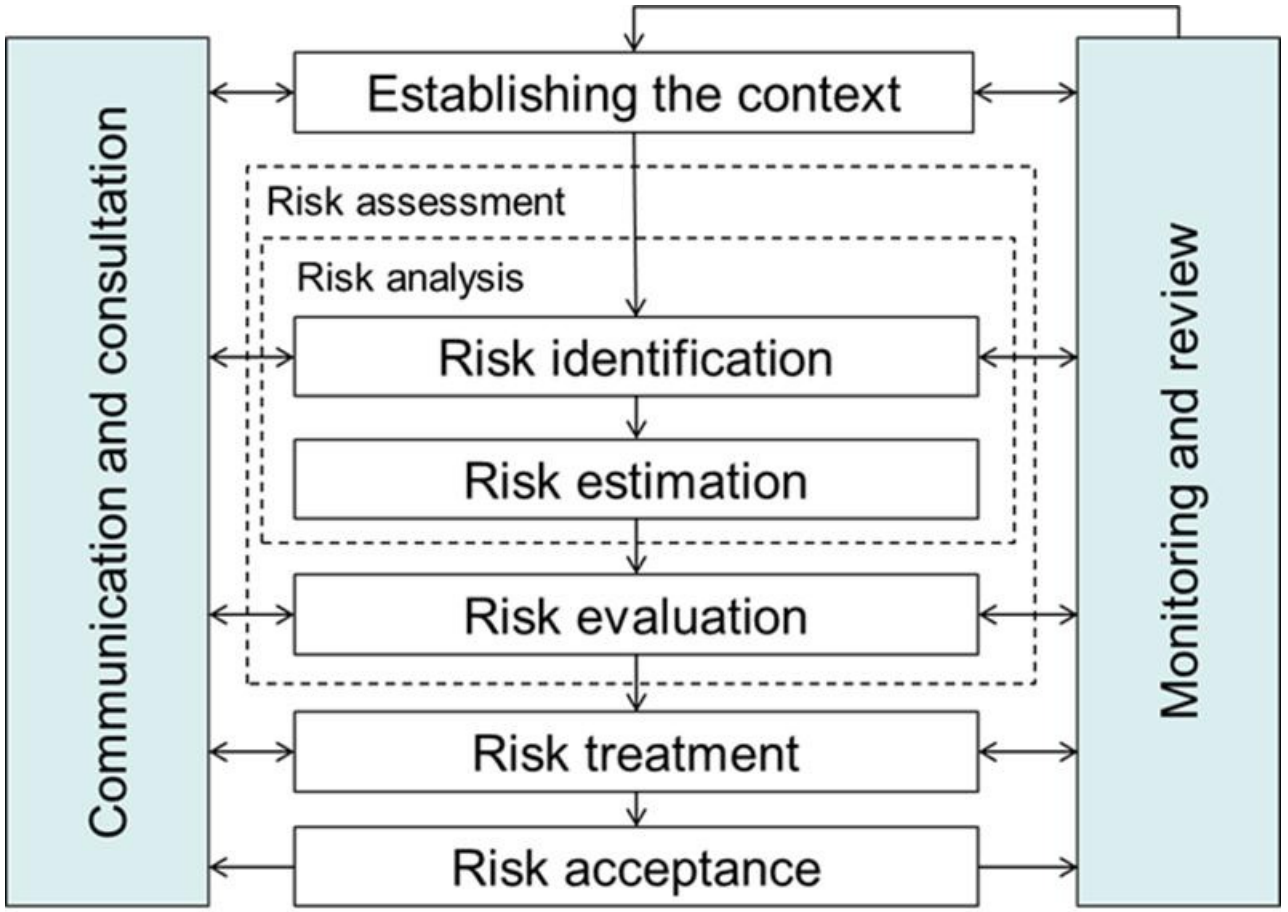
Svana Helen Björnsdóttir

STAMP Workshop MIT, March 23-26, 2015

Purpose of Research

- To study risk analysis methodologies in different fields and examine their effectiveness, compare them, and to seek a general risk analysis methodology that can be used in many different disciplines for integrating security into systems design.
- Investigate whether the new STAMP causality model can be used as a basis for a general risk analysis methodology.

A Typical Risk Management Process



Based on ISO 31000

Aim of Research

- To evaluate and compare different methodologies for risk analysis as an important phase for embedding safety, security and reliability into system design.
- To examine the effectiveness of risk analysis in various businesses and operations from a holistic system-based approach in order to find absolute methodology for different tasks.

Research Questions

1. What are the similarities and what are the differences in the methodologies used in the case studies conducted?
2. To what extent is it possible to formulate a general risk analysis methodology that can be used in many different disciplines?
3. Can a system based risk analysis model be made and successfully applied?

Hypothesis

It is possible to formulate

a general risk analysis methodology that can, to a certain extent, be used in many different disciplines.

Research Methodology

- Both quantitative and qualitative research methods
- In order to approach the first research question six case studies have been performed in different fields:
  1. Pension Fund
  2. Electrical Grid
  3. Power Company
  4. Prosthetics Manufacturer
  5. Blood Bank
  6. Software Company

Pension Fund

- All employees and self-employed persons in Iceland must be members of an approved pension fund.
- The minimum contribution to the pension fund is 12% of total earnings. Employer pays 8% and employee pays 4%.
- In 2013 the assets of the Icelandic pension funds were approximately 150% of GDP in Iceland.
- The main risk Pension Funds are facing is not being able to pay their future pension obligations.

Electrical Grid

- The Electrical Grid´s role is to operate the electricity transmission system and administer its system operations.
- The E-Grid operates under a concession arrangement. All the company's activities are subject to regulation by the National Energy Authority, which determines the revenue framework on which the energy tariff is based.
- The risk E-Grid faces is not being able to deliver electricity to users.

Electrical Grid

Iceland Electrical Grid ©Landsnet

Power Company

- The Power Company operates 15 power stations.
- Emphasis is placed on a holistic vision, where prudence, reliability and harmony of the operations with the environment and society are the guiding principles.
- One of the largest producers of renewable energy in Europe.
- Case Study: Latest Hydropower Station, 2014.
- Risk of life losses during project.

Prosthetics Manufacturer

- Company has wide-ranging expertise in the development, production, and sale of non-invasive orthopedics.
- “Smart” knee – adapts automatically to individual moving styles and improves its response over time.
- Must be fast enough to respond to all life’s little hurdles.
- One of the risk is life threatening situations for users in case of failure.
- Risk analysis is vital for product development.

Blood Bank

- The Blood Bank is an independent business unit of a University Hospital.
- Its services are designed to ensure an adequate amount of blood products at any time and meet the requirements of security and safety.
- The Blood Bank performs testing and monitoring to ensure consistency between the components administered and blood recipients.
- Research for diseases of immunological origin.
- Risk of blood infection and wrong blood transfusion.

Software Company

- The Software Company develops software solutions, provides IT consulting and hosts sensitive information systems for customers.
- Two types of software solutions, to manage risk and to assess quality of health services.
- Much emphasis is put on R&D and collaborative innovation with universities and partners.
- Customers world wide.
- Risk of software bugs and service failures.

Written Contracts

- Separate meetings with all parties.
- Written contracts made.
- Compliance with requirements of ISO/IEC 27001.
- Questionnaire with 49 questions for gathering basic information (quantitative).

Questionnaire

RESULTS AND ANSWERS FROM QUESTIONNAIRE - BASIC INFORMATION	
Q#	QUESTIONS
	Date of answers returned
1.	GENERAL
1.1.	Name of the person
1.2.	Name of company
1.3.	Year founded
1.4.	Listed
1.5.	Business category (ÍSAT 95)
1.6.	Number of employees
1.7.1.	Turnover 2012 - m.kr.
1.7.2.	Turnover 2013 - m.kr.
1.8.1.	Number of branches/offices in Iceland
1.8.2.	Number of branches/offices abroad
1.9.	Export - international business
2.	COMPLIANCE
2.1.	Most relevant laws and regulations
3.	INSURANCE
3.1.	Need for insurance
3.2.	Types of insurance
3.3.	Risk not covered by insurance

Questionnaire

4.	SAFETY AND SEQURITY
4.1.1.	Security / quality policy
4.1.2.	Documented policies, doc. ref.
4.1.3.	Ref. to law/regulation in policy documents
4.2.1.	Other policy documents
4.2.2.	Relevant law and regulations
4.3.	DOCUMENTED PROCEDURES AND PROCESSES
4.3.1.	Risk analysis
4.3.2.	Risk assessment
4.3.3.	Risk management
4.3.4.	Internal control
4.3.5.	Audits (internal - external?)
4.3.6.	Review
5.	CERTIFICATION
5.1.	All business certified
5.1.1.	If yes - by an accredited certification body
5.1.1.1.	If yes - name of certification body
5.1.2.	Parts of business certified
5.1.2.1	If yes - which parts
5.1.2.2	If yes - which certification body (accredited)

Questionnaire

6.	METHODOLOGY OF RISK ANALYSIS
6.1.	Formal methodology used
6.2.	Use of special software solution for Risk analysis
6.3.	Standards, regulations and requrements used
6.4.	Tangible assets registered
6.5.	Intangible assets registered
6.6.	Threats idnetified
6.7.	Consequence of risk assessed
6.8.	Probability of risk assessed
6.9.	Risk assessed or calculated
6.10.	Residual risk assessed
6.11.	Risk criteria set
7.	RISK TREATMENT
7.1.	Risk Info used for improvements - somone resp.
7.2.	Systematic Risk mitigation with controls
7.3.	Risk calculation after selcting controls - effectiveness of controls assessed
7.4.	Asessment on effectiveness and usefulness of risk analysis i.t.o. Cost
7.5.	Result of risk assessment documented
7.6.	Result of risk assessment used to learn from it

Interviews

- All participants formally interviewed.
- Interviews recorded and meeting minutes written afterwards to ensure traceability.
- Many documents have been received, including policy documents, quality manuals, written processes and procedures, results from risk assessments, annual reports, etc.

Results – In General

- Very different businesses – great diversity in business operation.
- Good knowledge of all relevant laws and regulation – also in different countries when matters.
- Genuine interest in risk analysis and risk management confirmed in all cases – as a way to better performance.

Results – Risk Management

- Use of ISO management standards – together with other relevant standards.
- Management system is in place at all participants – some better functioning than others and some also more mature than others.
- All except one are certified.
- Reporting of hazards, incidents and non-conformities is important for seeking root cause.

Results – Risk Management

- Written processes and procedures for risk management.
- Although use of standards and certification provides support in business, this also becomes burden.
- Governmental authorities lack knowledge and understanding.
- More difficult to keep focus.

Results – Risk Analysis

- Formal methodology for risk analysis is used in most cases. Not always written and not being followed very exactly.
- Tactics based bottom-up approach.
- Little awareness of residual risk.
- Expectation of active risk analysis to achieve better business results and more favorable business environment.

Results – Risk Analysis

- Good knowledge of risk treatment and selecting controls to mitigate risk.
- Little awareness of risk criteria.
- Lack of help and support, both from internal and external sources.

Back to Hypothesis

- The hypothesis: It's possible to develop one general methodology for risk analysis that can be applied in every field.
- Many similarities despite different businesses and great diversity in business operation.
- Standards do not provide much help in risk analysis methodologies – therefore company own approach.

Conclusion

- Tactics-based bottom-up approach used for risk analysis and risk management in all cases except one.
- Focus on avoiding threats and preventing failure.
- Reverse the process – start at the highest level.
- Apply STPA and STPA-Sec.