Comparison of Risk Analysis Methodologies in an Electrical Grid

Svana Helen Björnsdóttir

STAMP Workshop in Amsterdam

October 4-6, 2015

Disclaimer

This study is conducted as a part of Björnsdóttir's PhD research at Reykjavik University.

The content of this study and presentation does not reflect the official opinion of Reykjavik University, Stiki ehf. or Landsnet hf.

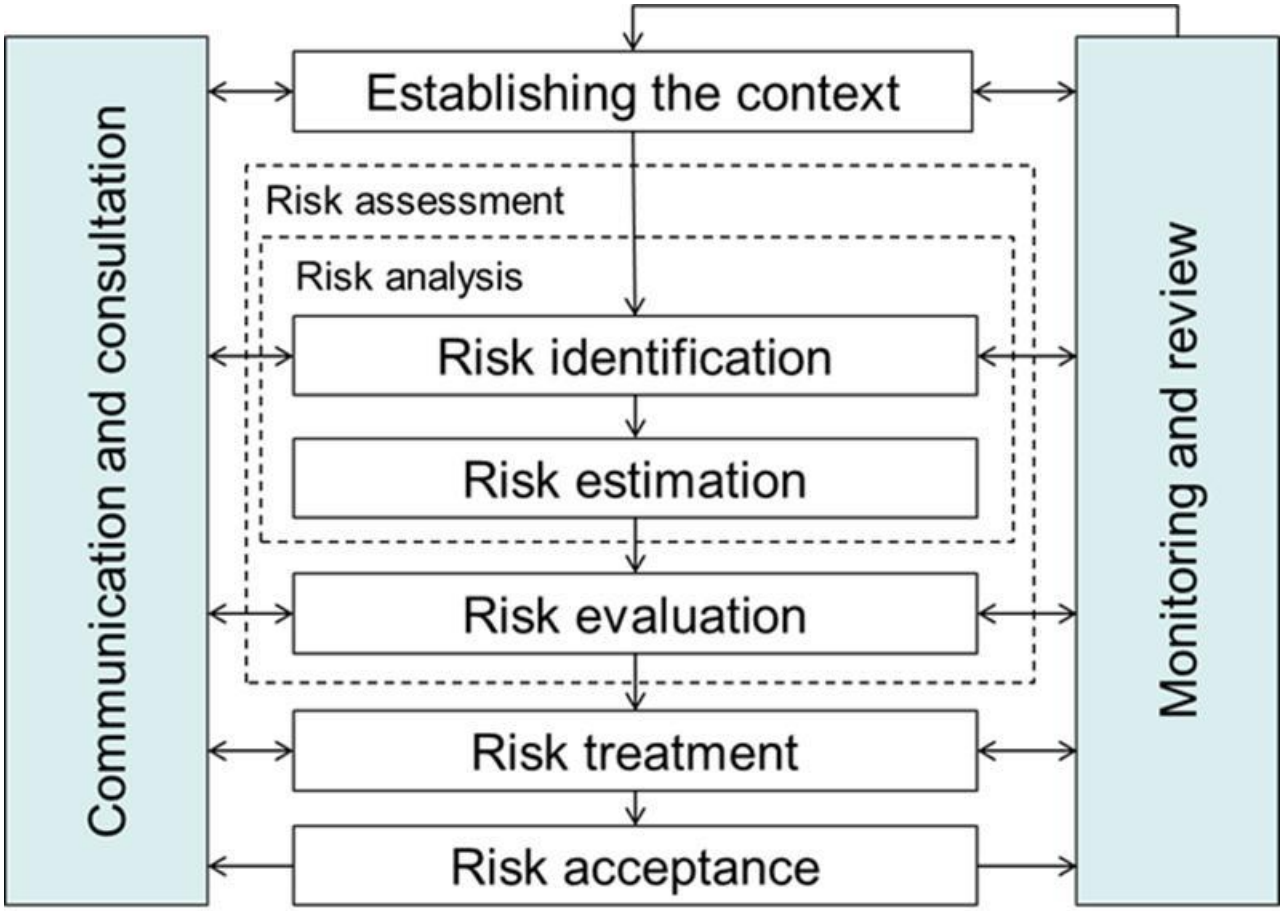
Responsibility for the information, results and views expressed in this presentation lies entirely with the author.

INTRODUCTION

Aim of Study

- Seek a generic risk analysis methodology that can be used in different disciplines
  - Examine currently used risk analysis methodologies
  - Compare different industries (six case studies)
  - Use STAMP/STPA to investigate whether this new causality model can be used as a basis for a generic risk analysis methodology

A Typical Risk Management Process



Based on ISO 31000

Research Questions

Main research question:

What is a generic risk analysis methodology that can be applied in different disciplines?

Research sub-questions:

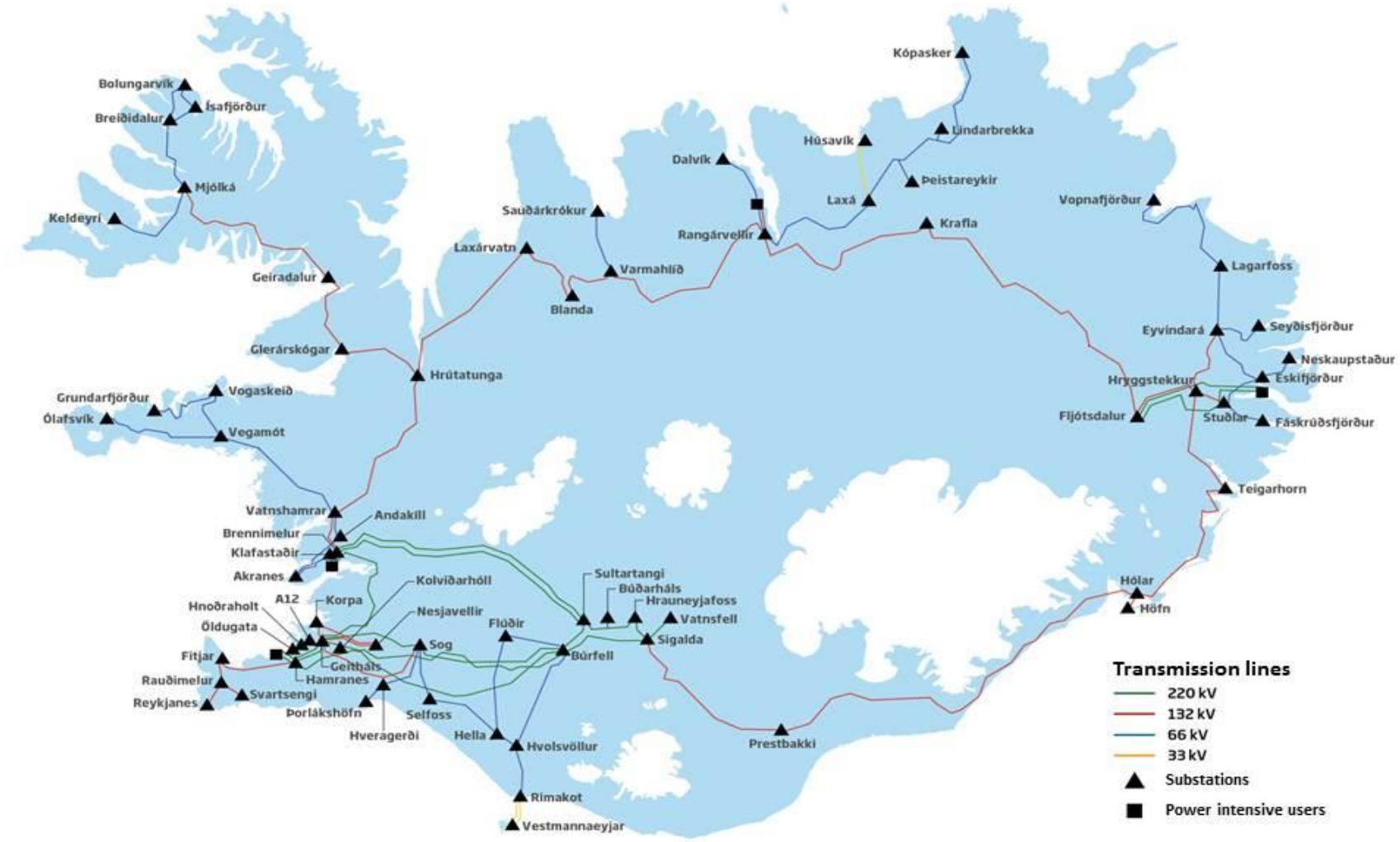
- What is a risk analysis methodology?
- What are the commonalities of risk analysis methodologies in different disciplines?
- What are the requirements for a generic risk analysis methodology?
- Can STAMP/STPA fulfill these requirements?

ICELAND ELECTRICAL GRID - LANDSNET

Iceland Electrical Grid

- Operate and administer the electricity transmission system
- Concession arrangement
- All activities are subject to regulation by the National Energy Authority (NEA)
- NEA determines the revenue framework
- Main Risk: Not able to deliver electricity

Electrical Grid



Iceland Electrical Grid ©Landsnet

Current Risk Analysis

- Company own approach
- Written risk assessment procedure
- Bottom-up approach within each department
- Departments identify same risk factors in different ways
- Focus on avoiding threats and preventing failure

APPLICATION OF STAMP/STPA

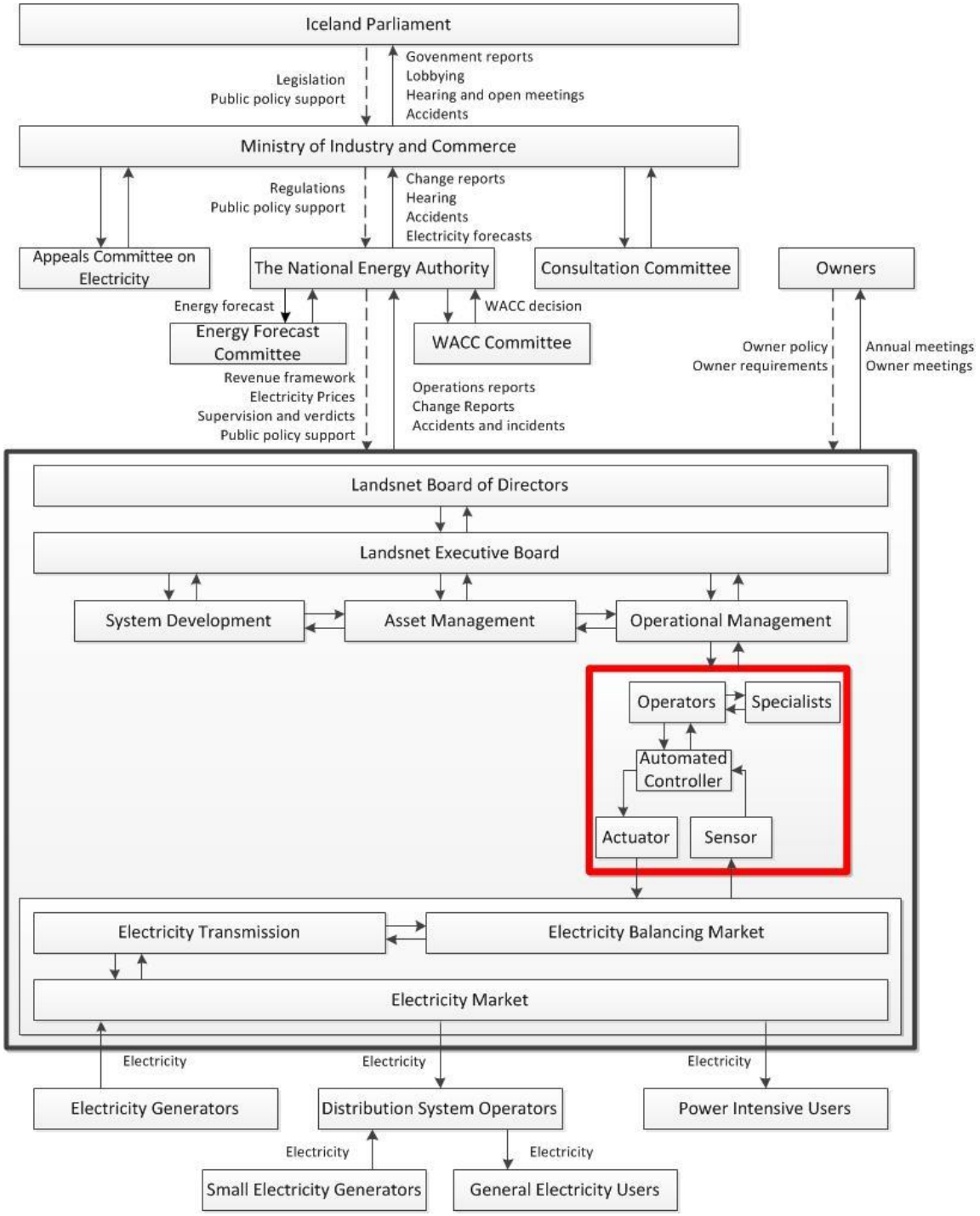
Why STAMP/STPA?

- Power system are getting more complicated
- More interconnection
- More temporary power sources connected to the grid
- Current risk methodology does not capture risk in a holistic way
- Risk factors not identified which can mislead implementation of mitigating controls
- Systematic approach to risk identification and risk analysis is needed

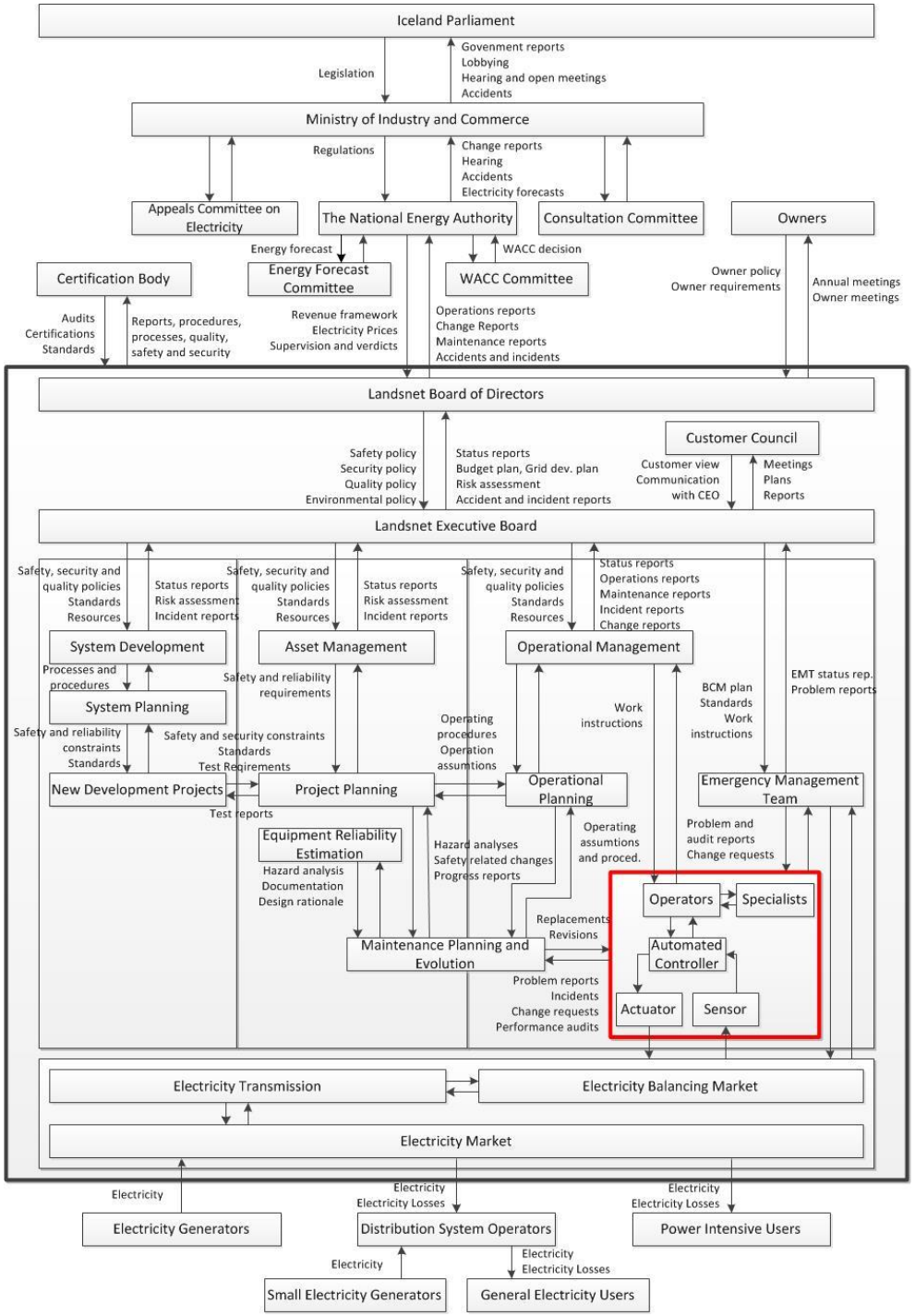
Major Accidents/Losses

- Humans' life
- Loss of power
- Loss of public policy support
- Financial loss
- Damage/loss of equipment and materials

Hierarchical Control Structure



Hierarchical Control Structure



Hazards in Electrical Grid

Hazards causing transmission disturbance in the electrical grid:

H1: Electrical power transmission network is not properly designed

H2: Electrical power transmission network is not properly operated

H3: Electrical power transmission network is not properly maintained

H4: Electrical power transmission network is not properly strengthened (renewed)

UCA for Generator Connection

Example: Operator as a human controller

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
Command control software to **switch on** a connection to a generator	Generator is not connected, thus not providing power to customers (H1,H2,H3)	Unprepared connected generator can damage power transmission system (H1,H2,H3,H4)	Early: Connecting a generator before it was synchronized or someone is still working on it (H1,H2,H3) Late: Not connecting quickly when power demand surges (H1,H2,H3,H4)	N/A
Command control software to **switch off** a connection to a generator	Generator is not disconnected and continues to provide power when it needs to be disconnected (H1,H2,H3)	Generator was disconnected when it should not be and it cannot provide power to customers (H1,H2,H4)	Early: Generator is disconnected before it needs to be disconnected (H1,H2) Late: Generator is disconnected after it needs to be disconnected (H1,H2,H3)	N/A

UCA for Substation Connection

Example: Energy management software as a automated controller

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
Execute **"switch on"** command to a substation	Not switching on substation cannot provide power to customers (H1,H2,H3,H4)	Switching on a substation before it is synchronized or someone is still working on it (H1,H2,H3)	Early: Substation is switched on before it is synchronized or someone is still working on it (H1,H2,H3) Late: Substation is switched on after it is needed, not providing power to customers (H1,H2,H3,H4)	N/A
Execute **"switch off"** command to a substation	Substation is not switched off when it is under maintenance (H1,H2,H3)	Substation is switched off when it is still providing power to customers (H1,H2)	Early: Substation is switched off before it is needed, not providing power to customers (H1,H2) Late: Substation is switched off after maintenance starts (H1,H2,H3)	N/A

Identifying Causal Scenarios

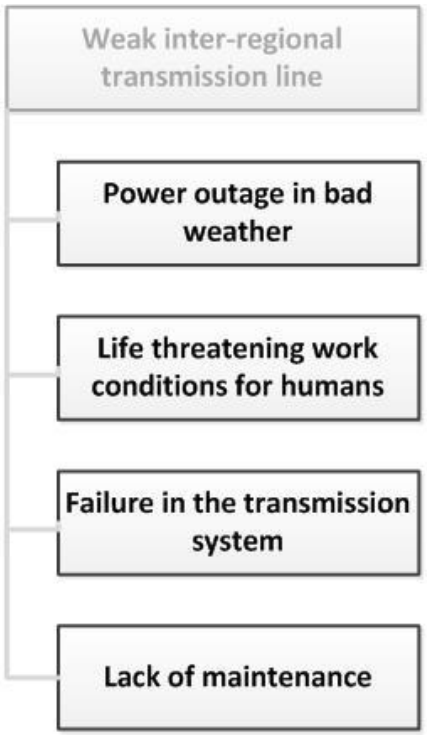
- Transmission disturbances can be caused by either internal or external factors
- Internal factors
  - Operator errors can be either human or technical errors
  - Equipment failures can be caused by component failure, aging of material or poor maintenance
- External factors
  - Environmental factors, such as natural forces
  - Sudden changes in transmission which cause transmission balancing problems in the grid (“smart grid” technology)

FINDINGS AND CONCLUSION

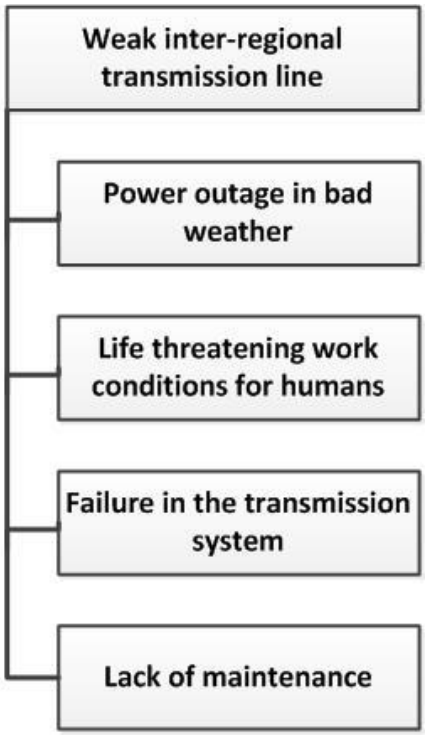
Findings

System Administration Dept.

Network Operation Dept.



STAMP / STPA



Conclusion

- Flaws in the control structure were identified with STAMP/STPA – but not by current method
- One major risk identified which in current bottom-up methodology appears in different ways

Thank you!

Questions?

Svana Helen Björnsdóttir
svana@stiki.eu