HÁSKÓLINN Í REYKJAVÍK
REYKJAVIK UNIVERSITY

Application of System Safety to Design and Construction of a Hydropower Station

Katrin D. Sigurdardottir[1)], Pall Jensson[1)] and Svana H. Bjornsdottir[1,2)]
1) Reykjavik University, Menntavegur 1, Reykjavik, Iceland
2) Stiki ehf., Laugavegur 178, Reykjavik, Iceland

Abstract

Safety should be considered on a system level, rather than component level, with a broad view of accident mechanism. STPA (System-Theoretic Process Analysis) is a systematic hazard analysis based on STAMP (System-Theoretic Accident Model and Processes); a new systematic approach to risk assessment where safety is treated as a control issue. A case study, where design and construction of a hydropower station was the subject of this new approach, shows a link between underlying risks that points to a systematic connection.

Introduction

Single risk analysis based on PRA (Probabilistic Risk Analysis) has been used to mitigate risks associated with design and construction of a hydropower station. Such projects are dynamic, complicated and have not been subject to a thorough control. The objective of the research is to estimate if application of STPA could reveal systematic risks that are undetected with PRA and would contribute to safer control of the project.

Case Study

Goals and unacceptable losses were defined for design and construction of a hydropower station. The goals involved operational- and cost objectives for the project to be considered successful, as well as securing no harm to environment and people involved with the project. Unacceptable losses were five. The first three involved violation of the goals, the second two involved loss of public policy support and loss of quality, security and safety in outsourced parts of the project.

Systematic risks were identified that could contribute to unacceptable losses. Hierarchical control structure for external and internal operational environment was drawn to identify where losses could occur (Figure 1). Systematic safety constraints that involved participation of risk manager (RM) in the project was derived as a systematic solution to identified hazards.

Results

The STPA analysis can be seen in Table 1. It demonstrates how early and active risk management can provide securer approach on imposing risks. It also shows how no automation is involved in the project and how the controller needs to function as a sensor to have a complete overview and maintain control of the project (Figure 2).

Conclusion

Application of STPA and STAMP has provided a broader view of accident mechanism than visible with previous methods. It has proven to be applicable for a sociotechnical system that involves cognitively complex human interaction and allows for a more comprehending understanding than when focus is on single risks. Single accident investigation should be involved in the risk assessment, but systematic approach is required for a complete understanding of imposing risks.

Table 1. Identifying Potential Hazardous Control Action

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Timing or Order Causes Hazard	Stopped Too Soon or Applied Too Long
ON *RM is actively involved and taking part in project plans and construction of a hydropwer station*	Risk is not identified or managed, neither during design phase nor construction	Ineffective (incorrect or insufficient) risk management	**Early:** Incomplete risk identification and interrelation **Late:** Not identifying risk and not mitigating risk	**Too Soon:** RM is involved early with project plans but does not follow up **Too Long:** Not Unsafe Control Action
OFF *RM is not actively involved until construction of a hydropower station has started*	Risk is not identified or managed, neither during design phase nor construction	Risk is not identified and managed in early stage	**Early:** Not Unsafe Control Action **Late:** RM is not in control of risk	**Too Soon:** RM is not in control of risk **Too Long:** Not Unsafe Control Action
OFF *RM is not actively involved in project plans and construction of a hydropower station*	Not Applicable	Risk is not identified or managed, neither during design phase nor construction	Not Applicable	Not Applicable

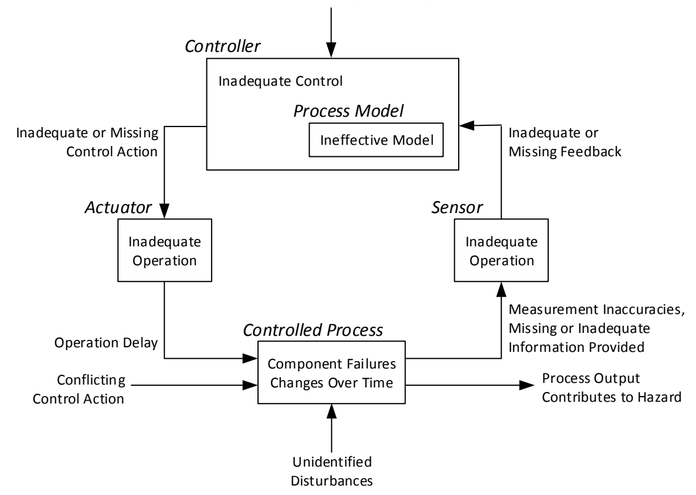

Figure 2. Hazardous Scenarios

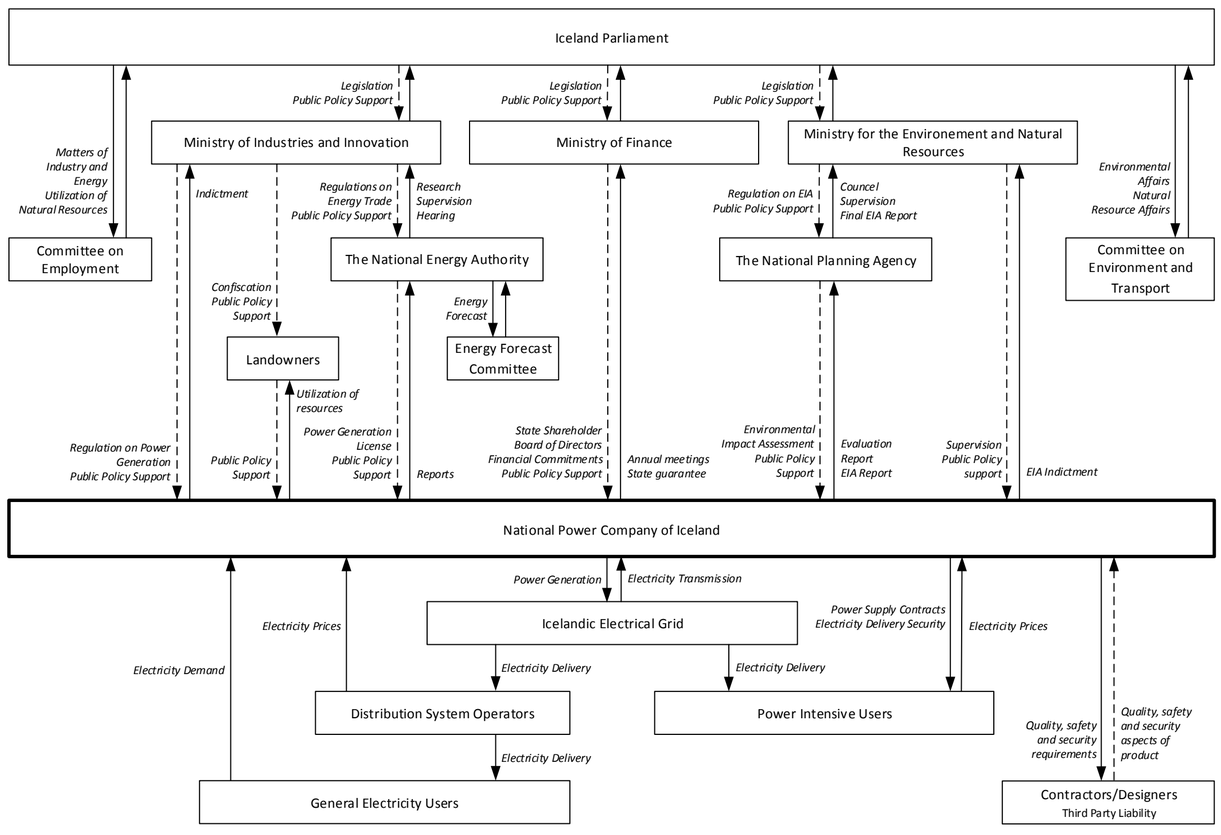

Figure 1. Hierarchical Control Structure for External Operational Environment

Reference

N. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety.* Cambridge, Mass: MIT Press, 2011.

TÆKNI- OG VERKFRÆÐIDEILD
SCHOOL OF SCIENCE AND ENGINEERING