Use of STPA in digital instrumentation and control systems of nuclear power plants

Rejzek Martin, Christian Hilbes

Institute of Applied Mathematics and Physics
Zurich University of Applied Sciences
Technikumstrasse 9
8401 Winterthur, Switzerland
martin.rejzek@zhaw.ch
christian.hilbes@zhaw.ch

Abstract: Nuclear power plant operators increasingly face the task of replacing their instrumentation and control systems with modern (digital) systems. In this work the "System Theoretic Process Analysis" (STPA) risk analysis method was adapted and amended to enable it to be used in digital instrumentation and control systems.

1 Background Information

Nuclear power plant operators increasingly face the task of replacing their instrumentation and control (I&C) systems with modern systems to ensure their availability, reliability and safety in the future as well. Replacement of these systems typically features simultaneous transition from primarily analog systems to software-based, digital systems.

The "System Theoretic Process Analysis" (STPA) risk analysis method specifically investigates risks which are generated by functional interaction between the control units present in the system as well as risks caused by component failure [Le11]. As a result, STPA is suitable for analysis of software-based and dynamic systems for which it is indeed typical that system failures occur without actual component failure. Modern digital I&C systems belong to this category of systems.

2 Applying STPA to digital insturmentation and control systems

In collaboration with swissnuclear and the Gösgen nuclear power plant, the STPA method was adapted and amended to enable it to be used in digital I&C systems. The actual implementation was demonstrated and discussed on the basis of a case study. Among others, the following aspects formed the focus of the work:

Representation of the system as a hierarchical control structure is a basic prerequisite for carrying out STPA analysis. One of the first questions is therefore how a hierarchical

STPA control structure can be developed efficiently for I&C systems, and how the specific properties can be handled (for example intensive use of the redundancy safety pattern).

While STPA Step 1 is meant to be predominantly based on a functional point of view of the system, STPA Step 2 can be used to perform an analysis based on both a functional and a physical representation of the system. This shift in point of view is explicitely implemented in our procedure, allowing for an easier integration of classical, component based analysis results into the overall effort.

3 Conclusions

STPA is one of several methods which can be used for analysis of nuclear power plant systems. Optimum benefit is generated when the various methods can be combined in suitable fashion. The adapted and amended process of the STPA method was thus designed to allow interfaces to other methods to be realized and, for example, to enable the causes of hazards which have already been established during the course of fault tree analyses to be incorporated in STPA.

References

[Le11] Leveson, N.: Engineering a safer world: Systems thinking applied to safety; MIT Press, 2011.