A Study on the Applicability of STPA Method to Digital I&C Design Assessment with Regard to Safety Requirements

Seung Ki Shin*, Sung-Min Shin, Sang Hun Lee, Inseok Jang

Korea Atomic Energy Research Institute

skshin@kaeri.re.kr

2020.12.17

CONTENTS

Introduction

- Safety systems are designed to automatically perform the safety functions identified in the early design stage of a nuclear facility.
  - Safety systems should be designed in accordance with various regulatory requirements.
- As digital technologies are adopted in design of I&C systems, the failure mechanisms of I&C systems becomes more diverse and complicated.
  - It is necessary to carefully consider an effective way to assess the design of digital I&C systems with regard to reliability.
- In this study, it is investigated how to utilize the STPA method when evaluating the safety design of digital I&C systems according to associated regulatory guidance

Guidance on Safety Design Assessment

- IEEE Std. 603, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*
  - Establishes minimum functional and design criteria for the power, instrumentation, and control portions of nuclear power generating station safety systems
  - Provides various design requirements for safety systems such as single-failure criterion, independence, and reliability

Guidance on Safety Design Assessment

- Safety system criteria on ‘Reliability’ in IEEE Std. 603
  - Appropriate analysis of the design should be performed to confirm the quantitative and qualitative reliability goals have been achieved.
  - The qualitative reliability analysis is performed to assess conformance of safety systems to applicable design criteria such as single-failure criterion, independence, and channel integrity.
    - Failure modes and effects analysis (FMEA)
    - Fault tree analysis
    - Reliability block diagrams
  - The quantitative reliability analysis is performed to establish initial periodic testing intervals for safety equipment and to provide a means for evaluating operational performance against requirements.
    - Mathematical modeling methods for reliability and availability estimation

Guidance on Safety Design Assessment

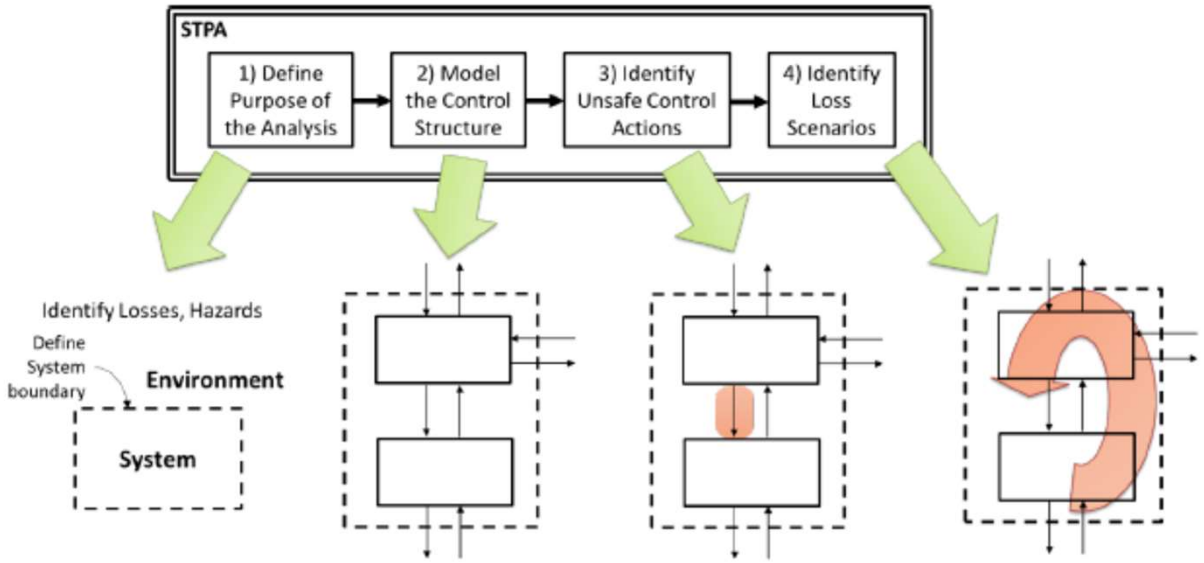
- Safety system criteria on ‘Software CCF’ in IEEE Std. 603
  - Engineering evaluation for software CCFs of digital safety systems should be performed including use of diverse means to accomplish the function that would otherwise be defeated by the CCF.
  - Diversity and defense-in-depth (D3) analysis should be performed to evaluate the digital I&C design against potential software CCFs of safety systems in accordance with NUREG-0800 BTP 7-19 and NUREG/CR-6303.

System-Theoretic Process Analysis

- The STPA is a hazard analysis method that is part of a relatively new set of safety engineering methods rooted in the theory of Systems-Theoretic Accident Model and Process (STAMP).
- In addition to component failures, STPA assumes that accidents can also be caused by unsafe interactions of system components, none of which may have failed.
  - The system is treated as a whole, not as the sum of its parts.

System-Theoretic Process Analysis

- Overview of the basic STPA method



① To define purpose of the analysis

② To build a model of the system called a control structure

③ To analyze control actions in the control structure to examine how they could lead to the losses defined in the first step

④ To identify the reasons why unsafe control might occur in the system

System-Theoretic Process Analysis

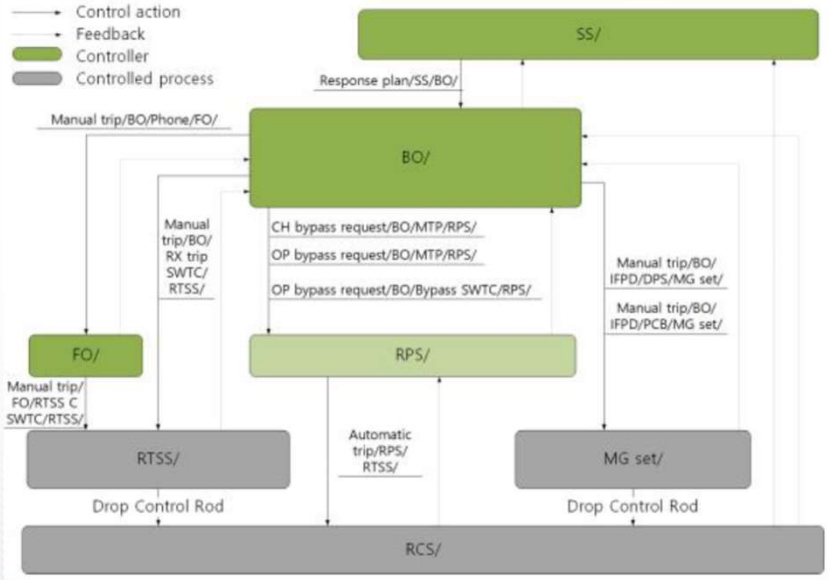
- Main advantages of STPA with regard to the safety design assessment of digital I&C systems
  - STPA can be started in early concept analysis to assist in identifying safety requirements and constraints.
  - STPA includes software and human operators in the analysis, ensuring that the hazard analysis includes all potential causal factors in losses.
  - STPA can be easily integrated into system engineering process.

Applicability of STPA to Safety Design Assessments to Digital I&C Systems

- Use of STPA in reliability analysis
  - The FMEA focuses on the independent failure of each hardware component, thus it is difficult to figure out the potential system failure caused by multiple components' failures or a software related failure.
    - Conventional methods such as the FMEA and fault tree analysis begin with decomposing a system into individual components.
  - The STPA can be utilized to address those failures as it finds all the causal scenarios leading to an identified loss.
    - The STPA considers the system behavior as a whole and unsafe interactions of components not failed can be captured as a loss scenario.
  - It can be expected that the STPA identifies causal scenarios of system failures that traditional methods cannot find.

Applicability of STPA to Safety Design Assessments to Digital I&C Systems

- The control structure built in the second step of the STPA can be utilized as one of resources for human reliability analysis (HRA).
  - In the detailed level of control structure, the signal interfaces between systems or components including the list of control and feedback signals are described including human operators.
  - It can be easily found which feedback signals are credible given that a certain component has failed.
  - The credible transmission path of a control signal from human operators can be discriminated in the control structure.



Control structure in a very abstract level for digital I&C systems

Applicability of STPA to Safety Design Assessments to Digital I&C Systems

- Use of STPA in D3 analysis
  - The control structure of STPA can be utilized to identify the potential vulnerabilities to a software CCF and verify whether the required safety functions of safety systems can be substituted by other systems unaffected by the CCF.
  - The control structure can be used as an important schematic diagram to check the compliance with guidelines of D3 analysis in NUREG/CR-6303.
    - Guideline 9 – Output Signals
    - Guideline 12 – Diversity Among Echelons of Defense
    - Guideline 13 – Plant Monitoring
    - Guideline 14 – Manual Operator Action

Summary and Conclusion

- In the licensing process, it is required to assess the design of I&C systems whether various safety requirements are met in I&C design using appropriate analysis approaches.
- As digital technologies are adopted in designing I&C systems, the signal interactions among components and the failure mechanisms become more complicated compared to analog-based systems.
  - To overcome the limitations of conventional approaches for safety design assessment of digital I&C systems, it is required to utilize an appropriate method to support the conventional methods.
- The STPA method can be utilized effectively with conventional methods for safety design assessments such as qualitative and quantitative reliability analysis and D3 analysis.
  - A well-modeled control structure is very useful for design assessment of digital I&C systems in many ways.