Transactions of the Korean Nuclear Society Autumn Meeting
Gyeongju, Korea, October 26-28, 2016

Review of Studies on Systemic Approach to Nuclear Safety

Jihan Lim*, Myunghyun Yoon, Young Sung Choi
Safety Policy Department, Korea Institute of Nuclear Safety
**Corresponding author: k732ljh@kins.re.kr*

1. Introduction

The traditional approaches tend to focus on a single component failure and handle risk by focusing on the technical aspects to look for the cause of the accidents. However, complexity of a system has reached a new level. Significant changes have occurred in the type of system we are building today which made applying traditional approach less effective. In January 1999, Mars Polar Lander failed to land without component error or failure [1] and Fukushima Accident was the result of complex and dynamic interactions of the system. Therefore, to ensure safety, understanding organizational failures and human errors becomes as important as focusing on technical causes of accidents.

Systemic approach to safety can be understood by seeing how the system is configured in a large network of other system and how those spread out to affect, and be affected by factors that lie far away in time and space from the moment things went wrong. It is important to recognize the entire range of interactions of human, organization and technology at all level.

This paper points out the limits of traditional approach and addresses some systemic approach models to cope with the problems we are facing today's dynamic and complex system. We hope this review serve to introduce the systemic approach to manage better safety of nuclear industry in Korea.

2. Limitation of traditional approach

The traditional approach to safety in engineering is a reductionist approach. In general, reductionist may consider a system in terms of a hierarchy of level of organization. It is assumed that the macro properties of a system (e.g. safety) is a function of the components constituting it and events are treated as the result of a linear sequence of separate and identifiable issues. As a result, if a single component does not fail, there is no accident. However, regarding each factor separately does not explain how a complex system works, and how the system's safety can be achieved. Safety can be determined only in the context of the whole. [2] It is impossible to know whether a plant is safe or not, for example, by inspecting a single component in the plant. We can just ensure the reliability of a certain component like a valve, not the safety of system. In order to achieve safety of system, there is no choice but to consider the system as the whole.

In the nuclear industry, lack of HTO(Humans, Technology and Organization) interaction consideration has been consistently identified as cross-cutting contributor to significant events. Report by the IAEA Director General presented an assessment of the cause and consequences of the accident at the Fukushima Daiichi nuclear power plant in Japan [3]. In its observation, while the stakeholders were aware of the possibility of isolated issues, they were not able to anticipate, prevent or mitigate the outcome of the complex and combination of these issues within sociotechnical system.

3. A systemic approach models for safety

3.1 An SSMS model

The SSMS(Systemic Safety Management System) model is proposed to manage risk within an acceptable range during organization's operations. It consists of a set of five interrelated sub-systems, called systems 1-5, which interacts in a various way with its external factor, 'environment.' Those who support the SSMS said that it has a fundamentally preventive potentiality in that if all the sub-systems and connections are present and working effectively the probability of a failure should be less than otherwise. [4]

The first characteristic of the proposed SSMS model is its 'environment' which lies outside the system but interact with it. The 'environment' has three other factors: 'socio-political factor,' 'economic factor,' 'physical factor.' Each of the factors consists of legislation, regulatory enforcement, insurers, trading conditions, geographical location, etc. These are important to consider because they are the source of circumstances to which the system response is necessary.

Among sub-systems, system 1 is the core of the SSMS model and deal with the organization's main activities directly. For instance, system 1, *safety policy implementation*, with the safety management unit, system 1 can monitor the resource and information entering the organization, plan safety objectives, manage risk proactively and devise risk control systems. System 2-5 promote the function of system 1. In this manner, decisions can be made at local level and decision-making is distributed throughout the whole organization.

3.2 An STAMP model

The STAMP (Systems-Theoretic Accident Model and Processes) focus on not the event itself but safety constraints. The model take into account three concepts

of the systems theory. Firstly, the model explains ensuring safety as a control problem rather than a failure problem. STAMP model assumes safety problem as an emergent properties that arise from the interactions among the system components. [2] Another characteristic is that the STAMP view system interacts between hierarchical structures, meanings failure to control high level constrain leads to failure of low-level behavior. Lastly, STAMP regards failure could happen if the process model did not reflect the real process or changed by the interaction among components.

According to STAMP model, safety can be controlled and achieved through imposing constraints on the behavior of and interactions among the components. That is to say, a new holistic approach to safety, based on control and enforcing safety constraint in the entire sociotechnical system, is essential to ensure safety. For this reason, understanding the role of the safety control structure, as shown in Fig. 1. is the first step to deal with the STAMP model. Identifying system-level constraints is important. In the system design stage, safety constrain is divided into sub-requirements. To enforce them, requirements are allocated to appropriate individuals or group.

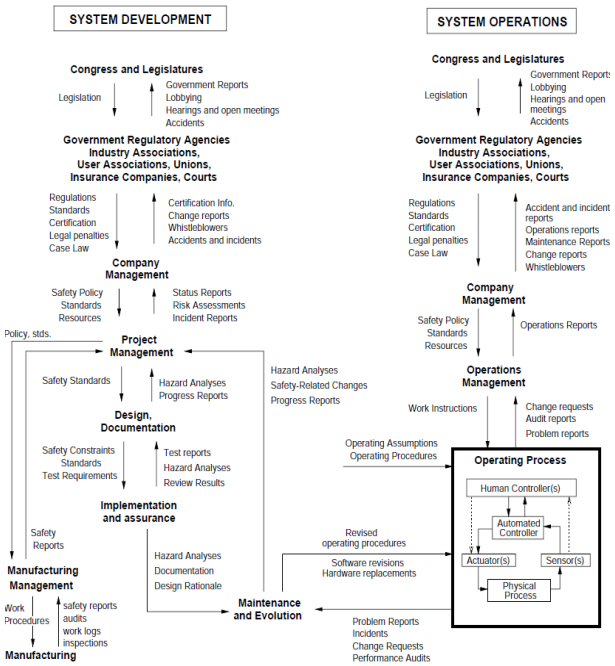

Fig. 1. General form of safety control structure (Nancy G. Leveson, 2011.)

4. Status of systemic approach in Korea

The significance of systemic approach to safety in the nuclear industry has continuously been recognized in Korea. For instance, KINS (Korea Institute of Nuclear Safety), which is responsible for regulating licensee's nuclear facilities and activities is taking systemic approach in various ways. When deciding event scale in event investigation report, not only technical aspect but also the HTO aspect. When human error exist, they are taken into account by upgrading the severity level. Even though, most inspections are still focusing on finding root cause in terms of technical issue separately, human and organizational factors are becoming one of the crucial factor when implementing event investigation.

In the same vein, KINS began to apply systemic approach concept when implementing cause analysis composed of four steps. Among the steps, the first step is to identify the interactions between HTO with systemic methodology. In addition, it is encouraging that KINS consistently participate in relevant training or workshop to strengthen ability to build up systemic thinking, which leads to augment inspector's expertise on systemic approach conducting safety regulation.

A combined model is proposed to establish regulatory policy/activities and implementation plan such as decision making, handling public confidence in utility. [5] This model is designed in light of integrating instantaneous risk from the configuration of systems in nuclear facility and long-term safety constituted by diverse feedback loops. It assumed that the nuclear safety is achieved by utilities, regulatory bodies, residents, NGO and the media and demands more responsibility when they get involved.

5. Discussion

This paper describes the traditional approach on safety as compared with systemic approach. In doing so, some limits are addressed because of properties of safety and complexity of big engineering industries. And two models – an STMAP and an SSMS - of systemic approach are introduced for more detailed understanding. Finally, we addressed the conditions of nuclear industries in Korea. To establish systemic approach solidly in Korea, nuclear accident case study should be performed deeply to verify possibility of application of systemic approach. Also even though IAEA GSR part 2 partly referred the need of systemic approach, we need to form a consensus on the usability of systemic approach with the persons concerned. We hope our review contribute to next study regarding implementation of practical application on real case of Korea using systemic tools which lead to enhance safety .

REFERENCES

[1] JPL, Report on the Loss of the Mars Polar Lander and Deep Space 2 Missions, 2000
[2] Nancy G. Leveson, Engineering a Safer World, 2011.
[3] IAEA, The Fukushima Daiichi Accident, 2015
[4] Jaime Santos-Reyes, and Alan N. Beared, A systemic approach to managing safety, 2007.
[5] Kwang Sik Choi, etc., "New Approach for Nuclear Safety and Regulation," 2007.