2021 International Nuclear Atlantic Conference – INAC 2021
Virtual meeting, Brazil, November 29 – December 2, 2021

Systems Engineering Principles Applied to Nuclear Safety and Security

F. Lemos

fllemos@ipen.br, Instituto de Pesquisas Energéticas e Nucleares, Brazil

1. Introduction

A Nuclear Power Plant is a highly complex social-technical system. Besides the plant, the NPP system comprises several interdependent subsystems as for example, the plant technological systems, human resources, supply chain involving multiple companies, regulators, and organized groups in the society. Permeating all those systems we have different organizational cultures, where safety and security cultures are subsets of the organizational culture.

The complexity of this NPP system may hide innumerous opportunities for interactions that may result in unwanted or unsafe consequences. Those hidden vulnerabilities may be exploited by malign individuals or groups in many ways we would not easily foresee.

In traditional methods of safety or security analysis, for example, by postulating initiating events, and calculating or observing the consequent chain of events that follows, the analyst may not grasp all the possible systemic factors that may contribute to unwanted consequences, or that may contribute to make a predicted consequence even worse.

This is not to say that traditional methods of analysis are wrong. However, we argue that traditional methods for safety or security analysis can give a false sense of safety or security, which would be in itself a safety or security issue.

Rather than considering accidents as a result of a chain of events, a systemic approach considers that accidents are a result of a hazardous state of the system that emerges from the interactions between the components of the system.

2. Some Definitions

Following we present some definitions important for systems engineering and systems thinking:

- *System*: a system is defined as a set of components hierarchically organized and that work together towards a common objective. [1]. In this sense, at the highest level, a system of systems is still a system where the subsystems are components of the system. [2]. We named a NPP a system of systems to emphasize that the NPP itself is not an isolated plant and depends on a number of other systems to fulfill its objectives.

- *Systems Level Hazardous State*: is a state of the system that can lead to the loss. The system level hazardous state is a result of the interactions between the components of the system. Accidents are treated not as a chain of component failure events but as the result of inadequate enforcement of constraints on the behavior of the system components.

- *Environmental Conditions*: Are the set of conditions external to the system. These conditions can interact with the components of the system but are not under any control by the systems components.

- *Accident*: Accident is a inadmissible loss. The loss can be loss of life, money, reputation, or any other event that is considered inadmissible by the stakeholders.

Accident = Hazardous conditions + Worse Environmental Conditions

- *Emergent property*: Is a property of the system that emerges as a result of the interactions between the components of the system.
  Some examples of emergent properties are: safety, security, competitiveness, resilience.

Based on the definitions above we can present a very simple example on how a systems approach would differ from a traditional approach.

Let's consider the Stuxnet worm. Basically, the virus was sending false feedback to the controllers informing that the centrifuges were slowing down. The controller then would issue commands to increase the speed. [3]. There was no sign that something wrong was happening. In other words, the controllers were tricked. This example shows that there was no initiating event, and there was no way to react to a predicted attack.

This was a problem of interaction between components, where wrong feedback led the controller to issue a wrong control decision.

Another example is the Belgian Doel 4 NPP. All the oil was intentionally leaked from the turbine causing considerable damage. No one noticed any problem with the system until it was too late.[4].

Again, we have a case of unwanted consequence in the component's interactions, where the controllers were tricked into thinking there was no problem with the system.

3. Safety and Security

As mentioned in the previous section, safety and security are emergent properties of the system. Basically, if a loss is a result of unintended interactions between the components, then it is a safety issue. Whereas, if the loss is a result of intentional acts, then it is security issue. [5].

Note that, as the emergent properties are a result of the interactions between the components, we can conclude that safety and security are related to a better control over those interactions. Here is where the systems engineering principles can be of a great help for the enhancement of safety and security through a better understanding of the interfaces between the subsystems, as well as the commonalities between safety and security and the necessary tradeoffs between their competing requirements.

4. Systems integration

As the NPP system comprises several subsystems, it is of vital importance that all of the systems have a well-planned integration in order to assure that all components are working for the common goal of the system.
We can think of the subsystems as components of a system, [2], which interactions can lead to unwanted consequences. During the integration process all the possible interactions should be investigated in order to find vulnerabilities that could lead the system to a hazardous state and, consequently, to losses.

5. Tools for Systems Analysis

In our studies we apply the STAMP/STPA methodologies. STAMP stands for Systems Theoretic Accident Model and Processes, and STPA stands for Systems Theoretic Process Analysis.
STAMP is a causality model for accidents that was extended for hazardous analysis with the STPA tool.

STAMP is based on systems engineering principles as well as on systems thinking.

The system is modeled as a feedback control loop, where its components are hierarchically arranged and the analysis is performed from top down. In other words, the analysis is performed from state level to components level.
These tools offer significant help on traceability, where components interactions can be traced up to the system level hazard.
We encourage the interested reader to find more information elsewhere. [1].

4. Conclusions

Nowadays every system is getting more and more complex and players are more and more tightly connected. The nuclear industry is no different. The intense use of computerized processes, such as social media, internet of things, online maintenance, banking, etc. that affected our lives in unprecedent ways. This has also created innumerable hidden opportunities for security and safety vulnerabilities.

Besides, malicious people are also evolving and obtaining new capabilities to advance their intents.
Traditional methods, while useful, have some limitations that can be complemented with the use of systems engineering and systems thinking principles and tools.

The STAMP/STPA tool can be of great help for the enhancement of safety and security of nuclear installations in the sense that it allows a throughout investigation of the interactions between all the players within a system, their connections, interactions.

Systems Engineering principles have already been applied in several industries as for example aerospace, aeronautical, aviation, petrochemical, pharmaceutical, insurance, and health services. [1]. It is time for the nuclear industry to do the same.

References

[1] N. Leveson, *Engineering a Safer World*, MIT Press, Cambridge, USA (2012).

[2] N. Leveson, "The Drawbacks in Using the Term 'System of Systems'", *Biomedical Instrumentation and Technology*, vol. 47, pp. 115-118 (2013).

[3] "Mcafee", https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html. (2021).

[4] "Power Engineering International", https://www.powerengineeringint.com/coal-fired/equipment-coal-fired/electrabel-confirms-doel-4-nuclear-power-plant-sabotage/. (2014).

[5] N. Leveson, "An Integrated Approach to Safety and Security Based on Systems Theory", *Communications of the ACM*, Vol. 57, pp 31-35 (2014).