A SYSTEMIC APPROACH TO INFORMATION AND CYBER SECURITY

F. L. LEMOS
IPEN/CNEN _ National Nuclear Energy Commission
Sao Paulo, Brazil
Email: fllemos@ipen.br

P. H. BIANCHI
IPEN/CNEN _ National Nuclear Energy Commission
Sao Paulo, Brazil

Abstract

Design Based Threat, or DBT, is a common principle for physical and cyber protection, which is based on threat assessments. The protection, cyber or physical, will be planned based on the type of the identified threat.

While we acknowledge the importance of the DBT, we argue that following this line of reasoning may limit our ability to grasp other vulnerabilities the system may have due to the following assumptions:

a) The system will behave according to the way we think it should, based on a predetermined fashion.
b) If each component of the system is reliable, then the system will be reliable.

Systems theory assumes that accidents are a result of systemic factors, and does not have a single root-cause, generally a failure, that starts a chain of events leading to the accident.

Moreover, systems theory assumes that security and safety are emergent properties of a system that result from the interactions between the components of that system. Therefore, accidents are a problem of control of the interactions between the components of the system rather than a problem of failures of components.

In the systemic approach a cyber security system is treated as part of the whole socio-technical complex system, where humans are components of the system and interact with the computerized controls.

The organizational culture permeates the entire system affecting decisions and, consequently, the interactions between the components. Weak safety and security cultures will eventually contribute for the system to migrate to hazardous states leading to losses or accidents.

The paper analyzes the roles of organizational, safety and security cultures, as underlying factors that can lead to the deterioration of the hierarchical control structure, which is supposed to keep the interactions between the components of the system within desirable constraints.

1. INTRODUCTION

The importance and the complexity of cyber security have been emphasized in the literature, [1]. The growing and intensive use of computerized systems in all aspects of the industry lifecycle has been imposing new challenges as for the best approach to computer and information security.

It has been suggested that the physical protection systems principles could be applied to cyber protection systems. However, due to the nature of the cyber space, this is not a straight forward task, [1].

The paper argues that the nature of cyber space lends itself to a systemic approach.

It has been demonstrated, in the literature, [1], the need for integration between the cyber protection system and all other systems necessary for the operation of an installation. This includes all management and support systems related to safety, administrative measures, policies, regulations, and every other aspects of the installation operation.

All of the systems must work in harmony in order not to interfere in the good work of each other and to assure that the installation achieves its goals safely and securely.

A systemic approach, [2], offers tools that can help on the integration of all the other systems as will be seen in the next section, especially considering potential conflicts between safety and security requirements.

2. STAMP_ SYSTEMS THEORETIC ACCIDENT MODEL AND PROCESSES

STAMP is an accident causality mode based on systems theory and systems thinking, [2]. According to systems theory, accidents are a problem of control of the interactions between the components of the system, rather than exclusively failures of components.

STAMP is a methodology for analysis of the interactions between the components of the system. One important characteristics of the systemic approach is that it does not consider only failures, including human errors, as causes for accidents. Rather it assumes that accidents are a result of unwanted consequences due to unintended interactions between the components. In other words, accidents can happen even if all components are doing exactly what they are supposed to do.

This leads us to conclude that accidents are ultimately a problem of control of the interactions rather than failures of equipment.

Some tools, based on STAMP, were developed to help on the analysis of the interactions and find the necessary constraints for the interactions to work towards the goals of the system.

One of the tools is STPA, Systems Theoretic Process Analysis, [2].

Due to limitations of space, we recommend the reader to seek more information elsewhere.

3. STPA _ SYSTEMS THEORETIC PROCESSES ANALYSIS

STPA is a hazard analysis technique based on STAMP. It helps on the identification of possible problems on the controls of the interactions between the components of the system by tracking how the inadequate control could lead the system to hazardous states.

It also helps on the identification of how the previously inadequate controls could occur, [2].

Again, due to limitation of space, we recommend the reader to seek more information elsewhere.

Due to its nature, STPA can offer many opportunities for the study of the many aspects of cyber protection systems integration with the installation operation systems.

The first stage for the study of the interactions is to build a functional hierarchical control structure. This control structure is a feedback control of the flux of information within the system.

One very interesting aspect of STPA technique is that it is possible to analyze how the functional hierarchical control structure could deteriorate with time. For example, it can show how organizational culture, and its subsets security and safety cultures, are can affect the decisions, or control actions, perception of feedbacks, etc.

Another natural application of STPA is on the study of the harmonization between safety and security requirements.

4. THE HIERARCHIAL CONTROL STRUCTURE

As mentioned earlier, the functional hierarchical control structure is the representation of the system in terms of feedback control that should be enough to enforce the correct interactions between the components.

According to systems theory, safety and security are emergent properties of the system that result from the interactions between the components. Therefore, if the interactions are not properly enforced, the control structure can deteriorate leading the system to hazardous states.

Figure 1 shows some of the possible components of a system that includes the nuclear installation.

Each box represents a major player in the system. Every component has to be assigned a responsibility as for its function in the system. The decisions, or control actions, are based on the knowledge the controller has about the state of the system. This information is provided by the feedback.

Therefore, in case of conflicts between the actual state of the system and the information provided, for example, the decisions can potentially lead to hazardous states.

It can be understood then why organizational culture, and its subsets security and safety cultures, are major factors to help keep the control structure working properly.

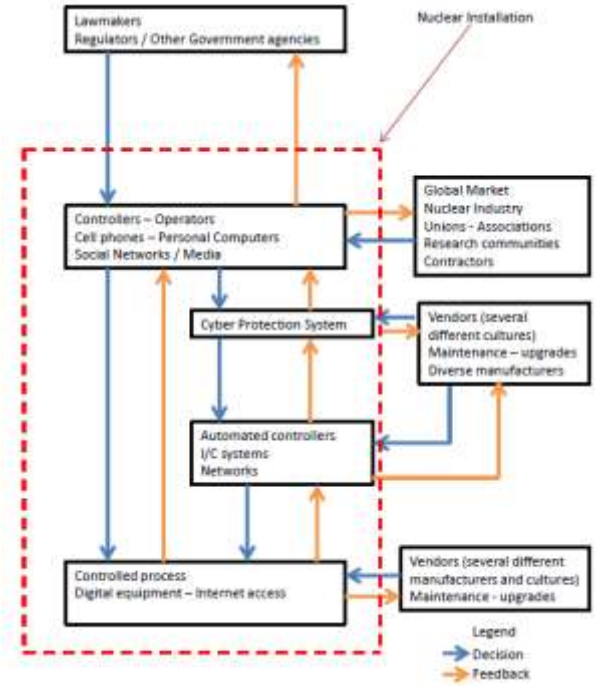

FIG. 1.A suggested functional hierarchical control structure for a nuclear installation.

5. ORGANIZATIONAL CULTURE

Organizational culture permeates all the instances of the system. Figure 1 depicts an example of a system in which the nuclear installation is one of the components. The system comprises regulators, the nuclear industry, associations, unions, vendors, market. This is not an exhaustive list of components.

It is important to note that equipment and software are designed by humans and, therefore, are affected by their cultures, in this case especially safety and security cultures.

This is especially important in renovations or upgrades where equipment from different companies are bought and introduced in an old system.

5.1. Safety and Security harmonization

One of the main advantages of the systemic approach is that it naturally leads to the harmonization between safety and security issues, since all the interactions between the components of the system are considered.

In terms of consequence, there is no difference between safety and security related accidents. The difference will be on the existence of intentional acts that may lead, or contribute, to the accident.

The advantage to treat safety and security in the same framework is that gaps in the safety procedures can be exploited by malevolent people, maybe with help of insiders.

6. DEVELOPING SCENARIOS

With the help of the hierarchical control structure it is possible to create scenarios for possible vulnerabilities in the system.

In this case we would not consider any protection barriers or levels of security, since the whole system is being considered equally.

Every decision and feedback can have a direct or indirect effect in the perception of the state of the system by any of the controllers. In this sense it is important to emphasize that we live in a world extremely connected, including social media, internet of things, etc.

Every of the boxes, controllers, can also have different cultures. This will certainly have impacts on perceptions of different natures, according to, [3]. Consequently, decisions and interpretation of feedback as well, can be heavily influenced in ways that would contribute to the system to migrate to hazardous states.

In the Figure 1 we can see many other possibilities for interactions such as regulation, equipment with internet access, contractors and vendors.

7. APPLYING STPA

STPA is indeed a methodology for hazardous analysis, i.e. STPA seeks to identify ways that the system can be unsafe or unsecure. In this sense STPA is complementary to the performance based analysis, where it is seek to prove that the system is safe or secure.

Some definitions are important to understand the methodology. These definitions are based on , [2].

Accident is an unacceptable loss defined according to the stake holders

More than one accident can be considered. For example: damage to reputation; monetary loss; death or injury to individuals from public or workers; environmental contamination.

In systemic approach we can consider not only accidents related to radiological consequences, but also loss of reputation and monetary, for example.

A hazardous state is a systems state that can lead to an accident, or loss, given a worst case scenario related to the external conditions.

The above listed accidents can result from release of radioactive material from an installation. In this case the release of radioactive material is the hazardous state of the system.

External conditions are the worst condition that together with the hazardous state leads to the loss. Note that we can have control over the system´s hazardous state only, while the external conditions are outside the system control.

For example, for the accidents death or environmental contamination, the release of radioactive material can only be harmful if it occurs in a situation that will affect humans or the environment.

In systemic approach we can only work on the conditions over which we have control, i.e. we can only control the interactions between the components through the proper constraints. Therefore, although important, the external conditions are not the focus of the analysis.

For example, in the case of theft of critical information, the accident would be composed as:
Accident, A1 = Information stolen

For the information to be stolen the system should be in a hazardous state plus there must be a person or group willing to get the information.
In this case, the hazardous state of the system can be:

H1 = Information available for access

External condition:

E1= People willing to get the information

Note that we cannot control the will of the people in the external condition. We can only control the conditions that would make the information available.
Likewise, if the information is not available, it would not be stolen even if there is some people willing to get it.

In systemic approach, we still can work with the DBT, however, instead of relying only on the cyber protection system, we consider the whole system is working for a common goal, i.e. keep the information safe and secure.

Remember that security and safety are emergent properties of the system that result from the interactions between the components of the system.

Also note that we do not consider accidents, or losses, those events that can result in radiological consequences. This allows us to have a broader view of the problems related to safety and security.

Figure 1 is a high level representation of the system. In this figure there are no details about the any of the components. This would be a first stage in the analysis.
As the study progresses, and more data is available, including a better risk assessment for DBT, more elements can be added, and new interactions are considered.

8. CONCLUSION

Cyber security is a very complex issue that requires a good understanding of all its interfaces and interactions with the many facets of the installation lifecycle.

In a constant developing and connected world, the study of cyber and information security lends itself to a systemic approach, where instead of look for root causes, it would be more reasonable to look for possible interactions between the components of a system that could lead to vulnerabilities that would be exploited by malevolent people.

In this context, it is not the objective of the systemic approach to identify failures only, but rather develop scenarios, where even though all components work the way they should, the system can migrate to situations of vulnerability in regard with security and safety.

ACKNOWLEDGEMENTS

We would like to thank the IAEA for the financial support to participate in this event.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No 17, IAEA, Vienna, 2011.
[2] LEVESON, N., Engineering a safer world: Systems thinking applied to safety. MIT Press, 2011
[3] SHEIN, E.H., Organizational Culture and Leadership. Jossey-Bass Edition, 2004.