Contribution ID: **32** Type: **Paper**

A systemic approach to information and cyber security

Monday 10 February 2020 12:00 (15 minutes)

Usually information is classified into different levels of sensitiveness which will dictate the measures for its protection. Information protection measures include barriers for access such as people clearances, cyber security, physical access controls, etc
Also, Design Based Threat, or DBT, is a common principle for physical and cyber protection, which is based on threat assessments. Then, the security will be planed based on the risk assessment.

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, because this follows the assumptions that:

a) The system will react 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.

However, nowadays technology evolves at fast pace, and the complexity of the systems is always increasing, with computer intensive machinery, allowing for interactions that had never been experienced before. Therefore, there are not enough data for statistical decision making. Also, very often we see accidents that could not be attributed to a single obvious cause, or root cause. The complexity of the interactions between the components of a system can lead to unwanted consequences due to unintended interactions, even if each individual component is working as it was supposed to.

Alternatively, systems theory assumes that accidents are caused by a number of systemic factors, and not by a single root-cause, generally a failure, that starts a chain of events leading to the accident.
Therefore, accidents are a problem of control of the interactions between the components of the system rather than a problem of finding root causes. The control of the interactions is represented by a hierarchical control structure, which is basically a representation of the system as a hierarchic structure where the higher levels control the interactions of the lower levels in order for the system to achieve the desired levels of safety and security.

A cyber security system can be approached as a socio-technical complex system, and in such humans are as part of the system as the computerized controls. In fact, human factors are present in every component of a socio-technical system, since all technological aspect is designed by humans. Therefore, of particular importance are the human factors, such as safety and security culture, and its effects on the interactions between all components.

Safety and security cultures are part of the organizational culture. The organizational culture permeates the entire system, as mentioned above, affecting decisions and, consequently, the interactions between the components.
Weak safety and security cultures will eventually contribute for the system to shift from a safe and secure state to hazardous states and, therefore, leading to losses or accidents.

This work 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.

Gender

Male

State

Brazil

Authors: Mr DE LEMOS, Francisco Luiz (CNEN _ National Nuclear Energy Commission); Mr BIANCHI, Paulo Henrique (CNEN - National Nuclear Energy Commission)

Presenter: Mr DE LEMOS, Francisco Luiz (CNEN _ National Nuclear Energy Commission)

Session Classification: Identification, Classification, and Protection of Digital Assets in a Nuclear Security Regime

Track Classification: CC: Information and computer security considerations for nuclear security