THREE THREADS OF SECURITY AT NUCLEAR POWER PLANTS

Abstract

"Understanding and evaluating the three threads of cybersecurity—Systems, Structures, and Components (SSC) view of risk, Computer application view of risk, and Target Set view of risk—is crucial for the safety and security of a nuclear facility."

Tim Roxey

Tim.roxey@gmail.com

May 15, 2025

Understanding and evaluating the three threads of cybersecurity is crucial for the safety and security of a nuclear facility.

Three different areas must be evaluated for a complete cyber assessment of a nuclear facility. Two of these areas are easy to understand because they involve either a critical digital component, a so-called Critical Digital Asset (CDA) of a critical system (System, structure, or component that is important to nuclear safety), or are classified as a "Safety Related" software program. The third area is more subtle and involves maintaining command and control with personnel deployed at various defensive positions scattered around the facility. These defensive positions are designed to facilitate the defense of certain target sets critical to the facility's safe operation and shutdown.

Each assessment area evaluates risk and its mitigation to acceptable levels. In the first two areas (SSCs and software applications), the risk evaluation involves the relationship between the cyber components of these SSCs and apps to the facility's Safety Analysis Report (SAR) and the inherent Design Bases Accidents upon which the SAR is based. In the third area, the risk is evaluated based on the facility's Security Plan and associated target sets and their inherent relationship to the facility's SAR and the physical layout of the SSCs.

This breakdown of the risk for NPPs will ensure that focus is given to assessing each of the three interrelated domains.

In summary, the three domains are;

- A Systems, Structures, and Components (SSC) view of risk
- A Computer application view of risk
- A Target Set view of risk

A Systems, Structures, and Components (SSCs) view of risk

Plant systems that fall within two basic categories, nuclear safety and continuity of power, are considered Critical Systems. The nuclear significant systems include safety systems, plant security, emergency preparedness, and auxiliary systems that support safety systems. Systems related to the continuity of power are operational control systems.

Safety systems that typically fall within the Nuclear Significant category are defined as those Systems, Structures, and Components (SSCs) relied upon to prevent or mitigate design basis accidents (DBA) and systems with significant Core Damage Frequencies (CDF) associated with them. The availability of Nuclear Significant systems to prevent or mitigate a design basis accident, as described in a facility's licensing basis documents, ensures the facility's compliance with its NRC license.

Operational control systems are I&C systems utilized for normal operations and to control plant processes, but they are not dependent upon performing safety functions following anticipated operational occurrences or accidents. This category includes systems directly impacting generation, limited to plant primary and secondary generation equipment, including the main generator switchyard relay/breaker.

The assessment

The most obvious group to review is the Systems, Structures, and Components (SSCs) that contribute to protecting the nuclear reactors' fission barriers. Put another way, the SSCs that contribute the most to the Core Damage Frequency (CDF) (A measure of SSC risk significance) in a facility's Probabilistic Risk Assessment (PRA) or Plant Safety Assessment (PSA) program. These SSCs require the greatest degree of scrutiny.

The safety-related functions of these SSCs are well known and carefully documented in site correspondence and documents such as the facility's Updated Final Safety Analysis Report (UFSAR), a site's Maintenance Rule (MR) documentation, or the facility's PRA or PSA. These SSCs' functions are counted on to mitigate the effects of or prevent certain design-based accidents (DBA). As reviewed by the NRC, these DBAs and their prevention or mitigation of consequences constitute the foundational elements of a facility licensing basis.

From one perspective, protecting any cyber components related to these SSCs will help ensure they remain dependable and available to perform their safety-related function when called upon. Conversely, the lack of reliability in these SSCs due to a compromise caused by a cyber intrusion event could lead to a situation where the SSCs' safety function could be denied when needed. This denial of the availability of safety functions would have serious safety and regulatory implications.

An Applications View of Risk

In the application view of risk, certain engineering codes that support the analysis of a critical system (CS) can be considered auxiliary systems and hence would be considered CDAs for this assessment.

Typically, these codes evaluate nuclear core parameters such as heat rates and core temperatures and pressures, structural parameters associated with various components and their behavior under accident conditions, and various other items. In addition, some applications that calculate risk probabilities for various plant evolutions and miscellaneous engineering codes fall within this assessment area.

Fundamentally, the entire group of engineering programs used to evaluate plant conditions or evolutions related to Nuclear Safety, NRC Emergency Response Data System (ERDS) elements, and certain security codes all fall within this assessment area as CDAs.

This assessment will be based on an initial inventory list of "safety-related" software (managed by the facility's SQA program), supplemented with the ERDS and security systems. Although the security and ERDS systems do not have a classical definition of Safety-Related, they support the security access and NRC oversight functions and are deemed important.

A Target Set View of Risk

As in the previous view of risk via SSCs and their association with design-based accident prevention or mitigation, the target set view looks at risks associated with maintaining the viability of physical SSCs and their intended functioning from a physical security perspective.

Although the area of physical security Target Set defense is far more difficult for a cyber vulnerability review, the physical security force implements certain elements of the physical security model that depend on cyber systems. Typically, the dependencies can be thought of in terms of the classical elements of the physical security realm: Command, Control, Communications, and Computers, the so-called C4 model (or C4I model if intelligence is factored in).

In a C4 review, various Target Sets would be reviewed to determine what impact cyber compromises would have on the defense force's ability to defend the Target Set. For instance, if radio communications are susceptible to cyber compromise, is there an alternate “band” for communications, like a landline phone system, personal data network, and voice-over-IP system that can preserve the communication function?

Some terms of art

Design-basis accident (DBA): A design-basis event is a postulated event used to establish the acceptable performance requirements of the systems, structures, and components, such that a nuclear power plant can withstand the event and not endanger the health or safety of the plant operators or the wider public. Similar terms are design-basis accident and maximum credible accident. Subtypes of DBEs are:

Critical digital asset (CDA): A digital device or system that contributes to the operation or maintenance of a critical system and can affect its proper functioning. A CDA may be a component or subsystem of a critical system, a critical system itself, or have a direct or indirect connection to a critical system. Direct connections include both wired and wireless communication pathways. Indirect connections involve manually carrying data or software from one digital device to another and transferring it using disks or other data transfer methods.

Critical system (CS): Plant systems can be divided into two main categories: nuclear-significant systems and continuity of power systems. Nuclear-significant systems encompass safety systems, plant security, emergency preparedness measures, and auxiliary systems that support safety operations. On the other hand, systems that ensure continuity of power are categorized as operational control systems (refer to operational control systems).

Nuclear Significant: Those safety systems required for the protection of public health and safety, as well as important to plant safety, security, and emergency preparedness, including auxiliary systems that support safety systems and are required by the safety systems to accomplish their safety functions.

Operational Control Systems: Instrumentation and control systems are used for normal operations and control plant processes, but are not relied upon to perform safety functions following anticipated operational occurrences or accidents. This category includes systems that directly impact generation and is limited to the plant's primary and secondary generation equipment, including the main generator switchyard relay/breaker.