Amenaza
TECHNOLOGIES LIMITED

Nuclear Power Operator Risk Analysis

Title: ***The Use of Threat Models to Satisfy Nuclear Regulator (Licensor) Requirements***

Executive Summary

Environmental concerns related to carbon emissions have sparked a nuclear power renaissance. Many legacy nuclear plants are now expected to operate far beyond their original license terms. As a plant's operating license approaches its end date continued operation requires license renewal. To renew a license, operators must demonstrate that operational controls have the security and resiliency appropriate to meet current and future threats. In some cases, this may require significant control system upgrades to advanced digital technology.

The current level of cyber threats is very different from that which existed at the time the previous license was issued (possibly 25+ years ago), as is the control system technology available. In order to qualify for a license renewal, nuclear plants must demonstrate to the license granting agency that the plant's controls are adequate to resist all attacks from possible adversaries. Even low level attacks (which might not result in the emission of radiological material) must be assessed at a very low level of probability in order to gain license approval.

Nuclear safety and security are important to everyone. Health and safety are obvious concerns but other issues are relevant. Power customers must be satisfied that the plant will operate reliably. Equipment suppliers – as well as the entire nuclear power industry – are keenly aware that even a low impact attack may have harmful reputational effects. No one wants to be associated, however remotely, from a nuclear plant breach!

Nuclear Plant Prepares for License Renewal

A foreign nuclear plant has begun the license renewal process. Satisfying the nation's licensing agency requires the replacement of existing control systems with new technology sourced from American suppliers. A major U.S. laboratory is providing expertise and assistance with the process, both to promote nuclear safety and to ensure that no cyber breaches will occur at a facility using American technology.

The laboratory realized that an objective, quantitative risk-based analytic approach was required. Notwithstanding the lab's unparalleled knowledge and expertise in the field of nuclear power, they turned to Amenaza's attack tree-based methodology and SecurITree® threat modeling software.

Amenaza became a core part of a team that visited the nuclear station. Plant operators took several days of training in the attack tree methodology and the use of SecurITree. Once training was complete, Amenaza assisted in the creation of the first attack tree threat models pertaining to the facility.

Amenaza's Approach

Amenaza
TECHNOLOGIES LIMITED

Many industries have their own hostile risk assessment methodologies. In fact, a U.S. research group found over one hundred threat-risk methodologies in existence. However, they noted that virtually all of these methodologies shared fundamental principles. They all need to evaluate both the likelihoods and projected impacts of possible attacks. And, almost without exception, the methodologies provide no guidance as to how attack likelihood should be determined.

In the world of hostile risk statistics either don't exist or are only applicable in a very limited situations. They lack general applicability. Most organizations fall back on qualitative estimates based on the intuition of subject matter experts. Even if these estimates are valid, they fail to capture the reasoning process used to generate them. This leaves the assumptions open to criticism.

Amenaza's threat assessment process understands that attacks are primarily driven by human behavior. The methodology uses attack tree models to assess the feasibility and desirability of thousands of potential attacks from potential adversaries. This identifies high risk scenarios and the most effective mitigation strategies – the effectiveness of which can be validated in the models.

The attack tree-based process captures and documents the decisions that were made. This provides strong evidence of due diligence should an incident still occur.

It should be noted that the applicability of attack trees for nuclear control system security was confirmed in a Regulatory Guide published by the U.S. Nuclear Regulatory Commission as far back as 2010. Section C.3.3 of Regulatory Guide 5.71 indicates that attack tree analysis can be used to demonstrate the efficacy of security controls. See https://www.nrc.gov/docs/ml0903/ml090340159.pdf

Why It Mattered

Amenaza's advisory work, training and technology allowed plant operators to consider a vast number of attack scenarios and evaluate the likelihood and impact of each for various types of attackers. Secur*IT*ree not only makes it possible to identify areas of potentially high risk, but also to identify effective solutions. With Amenaza's help (and the Secur*IT*ree software), the plant is proceeding through the process of license renewal.