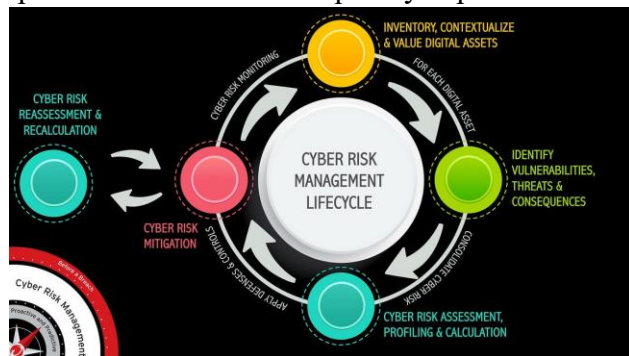


Cyberwiz-Pro: Governing the Convergence of Nuclear Analytics

As US commercial nuclear utilities modernize, they face a critical paradigm shift: the convergence of protected plant systems with enterprise analytics, predictive AI, and cloud services. This shift moves risk beyond the physical plant fence, creating new **"influence pathways"** that standard compliance tools cannot adequately capture.

Cyberwiz-Pro addresses this challenge by extending its core governance capabilities to the analytics lifecycle. It transforms the platform from a compliance repository into a dynamic **operational assurance engine**.

For a deeper-dive on this topic, [visit our WizNucleus Resources page](#)



Extending the Power of Cyberwiz-Pro

The platform extends traditional nuclear cybersecurity governance in three specific ways to handle analytics convergence:

1. From Static Controls to Decision Influence Modeling

Traditional cybersecurity focuses on connectivity and control. Cyberwiz-Pro extends this by modeling **"decision influence"**.



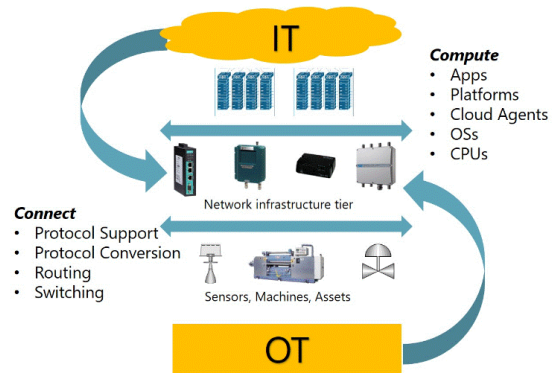
- **The Shift:** It is not enough to know if a system is connected; you must know if its data can alter an operator's judgment or an engineering decision.

- **The Cyberwiz-Pro Extension:** The platform explicitly maps "influence chains," allowing users to visualize how a data point in the cloud could degrade safety margins on the plant floor.

2. From Location-Based to Consequence-Based Scoping

In a converged architecture, Critical Digital Assets (CDAs) often reside outside the protected area—in the enterprise or the cloud.

- **The Shift:** Risk is no longer binary ("inside/outside the fence"). It is cascading.
- **The Cyberwiz-Pro Extension:** The platform classifies assets based on **consequence**, not hosting location. It tracks CDAs across the entire "trust boundary" spectrum—from the reactor core to the cloud analytics provider—ensuring evidence persists regardless of where the software lives.



3. From Compliance Checklists to Engineering Logic (FTA/FMEA)

Checklists confirm the presence of a firewall, but they cannot predict the impact of "model drift" or "training contamination" in an AI system.

- **The Shift:** Analytics require engineering-grade assurance to validate that the *information* remains trustworthy.
- **The Cyberwiz-Pro Extension:** The platform incorporates **Fault Tree Analysis (FTA)** and **Failure Mode and Effects Analysis (FMEA)** directly into the risk model. This allows engineering and security teams to quantify exactly *how* a degraded analytic could distort a decision, providing inspection-grade justification for these complex integrations.

The Strategic Value: Defensible Innovation

By utilizing Cyberwiz-Pro to govern this convergence, nuclear leadership can move from reactive "in-scope/out-of-scope" debates to a **sustained state of assurance**.

The platform ensures that every analytics integration is:

- **Identified** before it influences operations.
- **Governed** as a lifecycle, managing drift and updates over time.
- **Defensible**, with evidence that aligns directly with NEI 08-09 and IP 71130 expectations.