Behavioral Analytic Modeling for Insider Threat Assessment & Mitigation in the Nuclear Power Industry

Frank L. Greitzer, fgreitzer@cogility.com, Cogility Software
Christine F. Noonan, Christine.noonan@pnnl.gov, Pacific Northwest National Laboratory

Abstract

Traditional cybersecurity controls in the nuclear industry fail to adequately address human error, social engineering, and organizational factors that increase insider risks. Despite significant investment in technical defenses, the nuclear sector struggles with early detection of behavioral indicators linked to stress, poor security culture, complacency, or intentional harm, underscoring the need for a modern behavioral science–driven approach. We present an advanced Expert AI Behavioral Analytic Modeling framework designed to strengthen insider-threat assessment and mitigation within the nuclear power industry. The framework integrates behavioral monitoring, psychosocial indicators, technical and organizational factors to identify potential risks and differentiate careless versus malicious insiders. By incorporating behavioral + technical risk factors, this decision-intelligence framework delivers explainable, context-rich insights tailored to nuclear-specific roles, vulnerabilities, and operational dynamics. Adoption of this integrated solution will facilitate early detection while promoting a stronger nuclear security culture, improving cross-functional collaboration, and aligning risk management practices with evolving human-centric regulatory expectations. Overall, this work promises to advance proactive, human-centric insider threat mitigation and improve safety and operational resilience in nuclear power environments.

Introduction & Motivation

The nuclear power industry faces one of the most complex insider threat landscapes of any critical infrastructure sector due to its unique combination of operational technology (OT), safety-critical systems, and multiple threat vectors, e.g., sabotage, cyberattacks, drone-assisted intrusions, human exploitation. Insider incidents—both negligent and malicious—are increasing across energy sectors, with human error and carelessness remaining leading contributors to cyber-physical vulnerabilities. (Nazir et al., 2017). Research from the energy sector highlights **human factors** such as **negligence, lack of awareness, violation of workplace norms,** and **susceptibility to manipulation** that play a central role in counterproductive workplace behaviors and cybersecurity incidents (Panful et al., 2025; Searle and Rice, 2024). Social engineering, exploiting psychological triggers like trust and urgency, continues to be the most prevalent targeted attacks against energy firms (Panful et al., 2025).

Problem: The Human Element as a Critical Vulnerability in the Nuclear Power Industry

The nuclear domain, with its elevated safety, regulatory, and geopolitical stakes, requires mature human-centric risk models that move beyond compliance-based security controls. Despite substantial investment in perimeter defenses and traditional cybersecurity technology, organizations still struggle to detect early behavioral indicators of insider threats—especially those motivated by stress, complacency, poor security culture, or intentional harm. Studies show that traditional awareness training, lack of confidential reporting processes, and employee reluctance to report a colleague's behavior change often **fails to produce long-term effects** in altering security practices (Bada et al., 2019; Bell et al, 2019). An integrated behavioral-science–based approach is needed.

Advanced Expert AI Behavioral Analytic Modeling for Insider Risk Management

We describe an advanced **Expert AI Behavioral Analytic Modeling Framework**—Cogility's Cogynt decision intelligence platform—that integrates behavioral science and advanced security analytics to proactively identify early insider risk indicators. Key counter insider threat elements for the nuclear power industry should include:

- **Behavioral Monitoring & Analytics.** Analyze technical and behavioral data to detect at-risk behavioral patterns (e.g., indicators reflecting unusual access, off-hours activity, and unexpected data movements).
- **Psychosocial Indicators.** Modeling framework built upon the Sociotechnical and Organizational Factors for Insider Threat (SOFIT) knowledge base (Greitzer et al., 2018), which informs behavioral/risk models and helps employees who exhibit risky behavior before incidents occur.
- **Socio-Technical Context Modeling.** Modeling situation awareness and operator workload identifies cognitive stressors that contribute to insider risk in SCADA/ICS environments that are highly susceptible to human error.

- **Organizational Factors.** Apply and extend the SOFIT knowledge base of potential organizational risk factors to address security culture factors that strongly influence compliance, resilience, and willingness to report anomalies. Organizational support and internalization of security values are essential for behavior change.
- **Expert AI modeling framework.** An advanced, decision intelligence modeling approach incorporates all the elements above into an Expert AI modeling framework that encodes insider threat assessment expertise into a hierarchical, multi-layer complex event processing model informed by knowledge structures and inference processes used by trained analysts. This yields operationally powerful and explainable AI driven insights.

An Expert AI behavioral analytic modeling framework for the nuclear industry represents specific operational features that support recognition of and discrimination among relevant entities and constructs. Entities include operators and engineers with elevated OT access, contractors and vendors with privileged system access, system administrators, and other critical personnel susceptible to recruitment by adversaries. Vulnerabilities are constructs such as human error leading to cascading OT/ICS failures, nuclear operator susceptibility to spear-phishing campaigns, and organizational silos preventing holistic risk visibility across HR, IT, and security teams. Analytics tailored to the nuclear industry include behavioral criteria for identifying abnormal control-room interactions, dynamic workload models predicting operator fatigue or cognitive overload, risk assessment to detect high-risk remote connections, and cultural diagnostic instruments to measure security climate in nuclear facilities.

Expected Outcomes of Implementing the Framework

Implementation of a comprehensive behavioral analytic Expert AI insider risk management solution in the nuclear industry will yield numerous benefits:

- **Enhanced Early Detection.** Models that integrate behavioral, cognitive, and technical factors will enable earlier identification of both careless and malicious nuclear insiders.
- **Reduced False Positives.** Contextualized behavioral and technical monitoring will help identify and prevent alert fatigue, improving analyst focus and response.
- **Strengthened Nuclear Safety and Security Culture.** Intrinsic motivation and cultural reinforcement outperform compliance-based training in producing lasting behavioral change.
- **Improved Cross-Functional Collaboration.** A centralized governance framework integrating HR, OT engineers, cybersecurity, and management reduces information silos.
- **Better Alignment with Regulatory and International Best Practices.** Behavioral modeling helps nuclear organizations meet evolving expectations for human-centric cybersecurity risk management.

Conclusion

Insider threat mitigation in nuclear power plants must evolve past reactive, technically focused monitoring to **proactive, human-centric behavioral analytics**. Four decades of research underscores that cybersecurity is fundamentally a human issue intertwined with cultural, cognitive, and organizational factors. By integrating behavioral science with advanced analytics, the nuclear sector can significantly reduce insider risk, strengthen safety, and enhance operational resilience.

References

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.

Bell, A.J.C., Rogers, M.B., & Pearce, J.M. (2019). The Insider Threat: Behavioral Indicators and Factors Influencing Likelihood of Intervention. *International Journal of Critical Infrastructure Protection, 24.*

Greitzer, F. L., Purl, J., Leong, Y. M. & Becker, D. E. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. *IEEE Security and Privacy Workshops (SPW), Workshop on Research for Insider Threat (WRIT),* San Francisco, CA, pp. 197-206.

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security, 70*, 436-454.

Panful, B., Apaflo, B., Filani, A., Nnadi, K., & Hutchful, N. (2025). Human Factor Vulnerabilities in Energy Industry Cybersecurity: Assessing Employee Awareness and Behavior in Breach Prevention. *International Journal for Multidisciplinary Research, 7(6)*.

Searle, R.H. & Rice, C. (2024). Trust and High Control: An Exploratory Study of Counterproductive Work Behaviour in a High Security Organization. *European Journal of Work and Organizational Psychology, 34(3)*.