# Behavioral Analytic Modeling for Insider Threat Assessment and 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.

**Keywords:** insider threat; nuclear cybersecurity; human factors; behavioral analytics; UEBA; security culture; SOFIT; Expert AI; trusted AI; OT/ICS/SCADA

## INTRODUCTION AND MOTIVATION

The nuclear power industry faces a uniquely complex insider threat landscape because it combines safety-critical operations, high-consequence physical outcomes, and increasingly connected digital systems that span information technology (IT) and operational technology (OT). Insider incidents—whether negligent, misguided, or malicious—are particularly difficult to prevent because insiders possess legitimate access, contextual knowledge of plant operations, and awareness of "how work really gets done" under time pressure. As the sector modernizes instrumentation and control, expands remote connectivity, and integrates vendors and contractors, the number of pathways by which an insider can trigger or amplify a cyber-physical event grows.

Energy-sector studies consistently emphasize that human factors—negligence, lack of awareness, norm violations, and susceptibility to manipulation—are central contributors to cybersecurity incidents [1,2]. Social engineering remains a prevalent vector because it exploits psychological triggers such as trust, fear, and urgency rather than purely technical weaknesses [2]. At the same time, the dominant organizational response—periodic awareness training and compliance reinforcement—often fails to produce lasting behavioral change [3]. In high-security organizations, the interplay of trust and control can also influence

counterproductive work behaviors, affecting both compliance and willingness to intervene when colleagues exhibit concerning behavior [4,5].

This paper argues that nuclear insider threat mitigation must evolve beyond reactive, technically focused monitoring to a proactive, human-centric approach that integrates behavioral science with security analytics. Specifically, it proposes an expert AI behavioral analytic modeling framework that (a) combines technical telemetry with psychosocial and organizational risk indicators, (b) preserves explainability needed for safety-critical decision-making, and (c) supports early intervention that is proportionate and constructive—i.e., "left of harm." The remainder of the paper reviews relevant background, frames the nuclear-specific insider risk problem, describes the proposed modeling framework, discusses implementation barriers and safeguards, and uses illustrative cases to demonstrate how a behavioral analytic lens can improve detection and mitigation.

## BACKGROUND: INSIDER RISK, HUMAN FACTORS, AND NUCLEAR CONTEXT

In high-consequence environments such as nuclear facilities, insiders pose disproportionate risk because they can exploit access rights and operational knowledge to bypass dedicated security measures. Insider risk spans a spectrum that includes negligent behavior (careless policy violations, unsafe workarounds, poor cyber hygiene), misguided behavior (attempting to "help" by testing systems or introducing unauthorized tools), and malicious behavior (sabotage, theft, espionage, and facilitation of external attacks). Importantly, the same observable action—accessing a system after hours, copying files, or probing a procedure—may reflect benign work demands, negligence, or hostile intent; therefore, context and behavioral history matter for interpretation [5].

Awareness campaigns and training remain common controls, but multiple studies suggest they often fail to change daily practices over the long term [2,3]. Behavioral science provides a useful explanation: secure behavior is shaped not only by knowledge, but also by attitudes, perceived norms, and perceived behavioral control—core constructs of the Theory of Planned Behavior [6]. In practice, this means that training yields limited impact if it focuses solely on rules and compliance, without addressing social norms (e.g., local workarounds), resource constraints (e.g., time pressure), and the perceived costs of compliance. Moreover, organizational narratives that treat employees as "deficient users" can shift attention away from systemic organizational contributing factors such as workload, insufficient tooling, or unclear governance [2,7].

Nuclear OT environments share characteristics with other industrial control systems (ICS) and supervisory control and data acquisition (SCADA) deployments: complex socio-technical work, safety constraints, specialized engineering workflows, and long-lived systems. Surveys of SCADA cybersecurity techniques highlight that operator error, negligence, and lack of situation awareness [8] can contribute substantially to vulnerabilities and failures [1]. Because OT failures can cascade into real-world impacts, the nuclear sector must treat human performance variability—fatigue, cognitive overload, and procedural drift—as a cybersecurity and safety concern, not merely a training issue. More broadly, critical infrastructure research has emphasized the "human factor" as a persistent entry point through which security incidents occur, reinforcing the need for continuous cultural, behavioral, and organizational transformation alongside technical controls [2,9].

## PROBLEM: THE HUMAN ELEMENT AS A CRITICAL VULNERABILITY

Despite substantial investment in perimeter defenses, monitoring technologies, and compliance programs, nuclear organizations struggle to detect early behavioral indicators associated with insider risk—especially when those indicators manifest as low-magnitude deviations embedded within largely legitimate activity. Two structural challenges recur: First, insider risk signals are distributed across departments and data sources (HR, physical security, IT security, OT engineering, and management), but

many organizations lack governance and tooling to integrate these views, leaving "whole-person" risk assessment underdeveloped. Second, detection systems and security operations centers (SOCs) are often optimized to suppress noise and avoid alert fatigue; as a result, early-stage insider activity can be observed yet not escalated until later in the event lifecycle [10,11].

Practical barriers further inhibit a preventive approach: siloed departments, privacy concerns, lack of senior ownership, budget constraints, and the difficulty of integrating behavioral and psychosocial data with cyber telemetry. Employees may also resist monitoring if it is perceived as punitive surveillance, reducing trust and participation in reporting mechanisms. Consequently, many programs skew reactive—responding to technical alerts after an incident—rather than identifying and addressing stressors, cultural drift, and risky work patterns before harm occurs [2,5].

# ILLUSTRATIVE NUCLEAR INSIDER-THREAT CASES AND BEHAVIORAL IMPLICATIONS

The following publicly available cases illustrate how insider actions—malicious or negligent—often present detectable precursors in hindsight. Rather than treating each case as an anomaly, a behavioral analytic framework examines them to identify recurring patterns (e.g., combinations of indicators like disgruntlement, probe-and-test behavior, organizational complacency, and contractor-enabled access). When considering these and other historical cases, it is compelling to consider how a behavioral analytic approach might have succeeded in mitigating these risks through early intervention.

- *Disgruntlement and Sabotage: San Onofre (2012).* In 2012, contaminants were reportedly introduced into a backup diesel generator oil system at the San Onofre Nuclear Generating Station, and reporting suggested suspicion of sabotage linked to workplace tensions and potential disgruntlement. As a behavioral case, San Onofre emphasizes that grievances, perceived unfairness, or low morale may correlate with elevated risk in high-access technical roles. An integrated model would treat such indicators as contextual risk amplifiers—especially when coupled with unusual access, boundary testing, or changes in adherence to procedures—rather than waiting for conclusive proof of intent [12–14].

- *Undetected insider sabotage with major operational impact: Doel-4 (2014).* At Belgium's Doel-4 nuclear plant, an insider deliberately opened a valve that drained a large volume of turbine lubricant, causing extensive damage and a prolonged outage. The perpetrator was not identified publicly, highlighting how insider actions can occur within normal access privileges unless critical actions are instrumented and correlated with identity, role expectations, and operational context. From a modeling perspective, this case supports controls such as tighter segmentation of critical systems, enhanced logging around high-impact physical actions, and identity-conditioned escalation logic that flags low-frequency, high-consequence behaviors without overwhelming analysts [15–17].

- *Attempted espionage by former NRC employee: Eccleston (2013).* Charles Eccleston, a former DOE and NRC employee, exfiltrated and attempted to sell PII and other information, and subsequently sent spear-phishing emails to DOE employees to introduce a computer virus that could allow a foreign government to infiltrate or damage their computers. This case shows how an insider or former insider can facilitate external cyber operations by leveraging trusted relationships and domain knowledge. Behaviorally, this scenario highlights indicators such as deteriorating performance, unexplained financial motivation, and risky foreign contact patterns—

signals that are typically not visible to SOC tools unless integrated through governance and continuous evaluation. It also reinforces that contractors and affiliates require monitoring and intervention pathways comparable to full-time staff [18,19].

- *"Probe-and-test" precursors: GE Wilmington LEU theft (1979).* A temporary contractor employee at the General Electric fuel-fabrication facility in Wilmington, North Carolina, removed low-enriched uranium and attempted to extort money for its return. This low-enriched uranium (LEU) diversion incident is frequently cited as an example of an insider testing defenses over time, exhibiting repeated boundary testing, unauthorized after-hours activity, and exploitation of knowledge about badge design. Behavioral analytics can operationalize this concept by defining role-consistent access envelopes and escalating repeated deviations—especially when paired with anomalous interest in security procedures [20].

# AN EXPERT AI BEHAVIORAL ANALYTIC MODELING FRAMEWORK

To be effective, a behavioral analytic insider threat assessment approach for the nuclear power industry must encode nuclear-security related insider threat expertise into an explainable decision-intelligence model. The goal is not to replace analysts or existing controls, but to integrate behavioral science and socio-technical context with technical indicators to (a) identify early warning signals, (b) discriminate between careless and malicious behaviors, and (c) support proportionate interventions that reduce risk while sustaining workforce trust.

This "whole person" approach supports two complementary objectives: (1) earlier recognition of risk trajectories (e.g., stress → disengagement → non-compliance → escalation), and (2) preventive response options that include support, oversight, mitigation actions, and workflow changes—not only punitive action.

## Foundational Concepts: Behavioral-Science Grounding

The modeling framework should be grounded in a structured knowledge base of sociotechnical, psychosocial, and organizational contributors to insider risk. A key resource is SOFIT (Sociotechnical and Organizational Factors for Insider Threat), which articulates how individual stressors, team/organizational climate, policy enforcement patterns, and workplace dynamics can increase risk and reduce the likelihood of timely intervention [21]. A high-level diagram of the individual factors branch of the SOFIT taxonomy is shown in Fig.1 (not shown are the risk indicators at the bottom of the hierarchy, or the organizational factors branch of SOFIT. At the lowest level of the hierarchy, the Potential Risk Indicators (PRIs) represent basic observables that may be detected in varied data that are ingested into the model.

The framework integrates multiple classes of behavioral and technical indicators:

- **Behavioral monitoring and analytics including User and Entity Behavior Analytics / User Activity Monitoring (UEBA/UAM):** e.g., deviations from established baselines, such as unusual access times, unexpected data movement, repeated boundary testing ("probe-and-test"), atypical remote connections, or attempts to bypass controls.
- **Psychosocial indicators:** e.g., observable changes linked to stress, financial strain, substance concerns, interpersonal issues such as aggression or threats of violence, or deteriorating commitment to safety/security; these factors inform risk trajectories and intervention likelihood [5,21].
- **Socio-technical context:** e.g., workload, cognitive stressors, and situation awareness demands that impact likelihood of human error in OT/ICS operations [1].

- **Organizational factors:** e.g., security culture strength, policy clarity/enforcement consistency, reporting climate, and cross-functional coordination—factors that influence both compliance and detection [2].

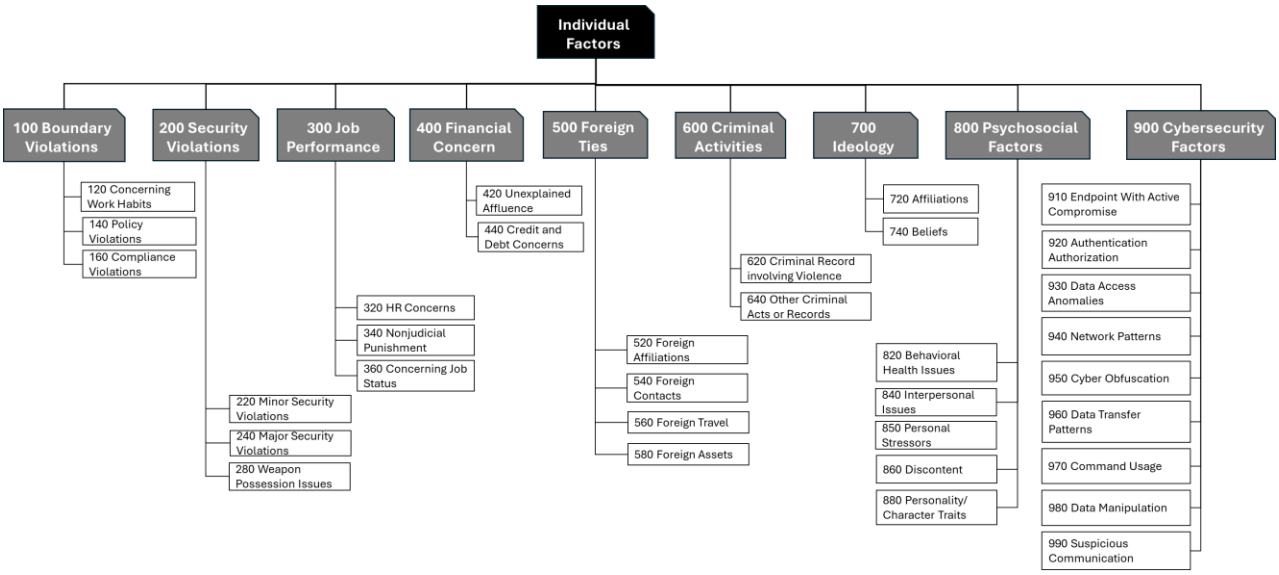


*Figure 1. SOFIT Taxonomy Structure -- Individual Factors Branch*

A small sample of SOFIT PRIs is illustrated in Fig. 2, which shows PRIs in the Boundary Violations class within subclass 120 ("Concerning Work Habits") and PRIs in the Psychosocial Factors class within subclass 840 ("Interpersonal Issues"). PRI 121 reflects situations where staff exhibit unauthorized after-hours activity, which may be detected based on electronic access control (badging-in) or UEBA/UAM monitoring. PRI 126, Reconnaissance, reflects suspicious behaviors by authorized staff in leveraging their legitimate access to gather information, map systems, or locate sensitive data for unauthorized purposes. Psychosocial Factors within the subclass "Interpersonal Issues" are generally considered "non-technical" indicators that are detected (reported) in performance evaluations or disciplinary records.

A dominant feature of the PRIs belonging to the SOFIT classes numbered in the 100s-800s is that they typically occur "left of harm," i.e., earlier in the attack lifecycle than the 900-class cybersecurity violations. Monitoring and analysis of these behavioral factors provides a unique opportunity for early detection and proactive mitigation actions that may reduce the risk or even help at-risk individuals find "offramps" from the critical pathway to insider risk [21,22].

In nuclear settings, insider risk management programs are focused on operators and engineers with elevated OT access; system administrators; contractors and vendors with privileged access; and physical security personnel. While the basic SOFIT knowledge base of PRIs applies generally to this domain, it is necessary to perform more specific PRI "calibration" that defines new PRIs, as needed, or modifies existing ones; and that adjusts PRI mappings and weights associated with threat behaviors. Further, the risk assessment model must reflect nuclear-specific vulnerabilities such as the potential for human error to produce cascading OT/ICS failures, susceptibility of specialized staff to spear-phishing, and organizational silos that prevent a unified view of risk across HR, IT, OT engineering, and security. Tailored analytics may also include abnormal control-room interaction patterns, dynamic fatigue/workload models, and risk scoring for high-impact remote access paths.

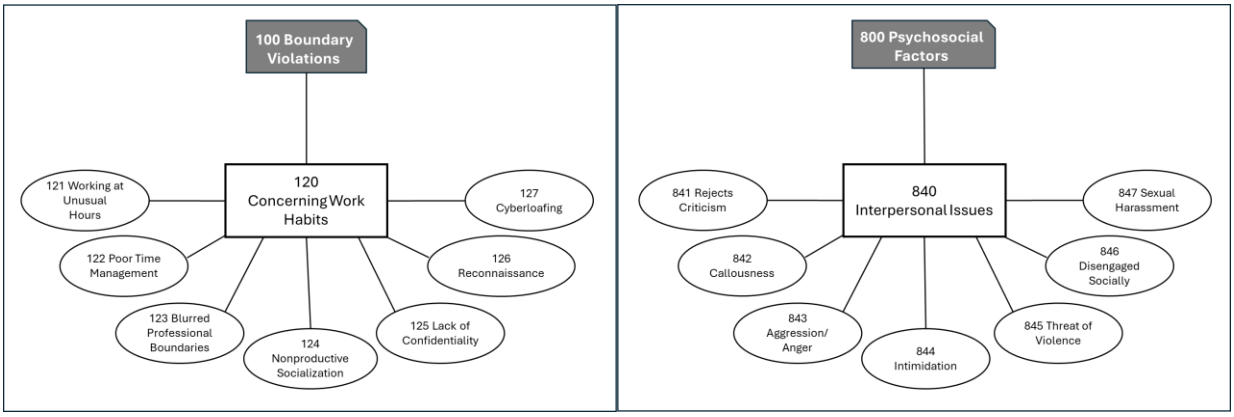


*Figure 2. PRIs Associated with SOFIT "Concerning Work Habits" Subclass 120" and "Interpersonal Issues" Subclass 840*

## Behavioral Analytic Modeling

An effective insider risk assessment approach must address the above behavioral and technical factors while also meeting the following operational requirements:

- **Expert AI Decision Intelligence [23] Approach to Model Expert Decision Making**: The approach should be based on an expert AI framework to model human experts' decision processes in support of high-consequence, human-in-the-loop decision making.
- **Continuous Monitoring and Data Ingest:** The solution must process and evaluate all risks continuously, focusing the analyst's attention on critical issues and improving efficiency.
- **Transparency and Auditability:** The approach must support full provenance to provide visualization of supporting information and relationships to enhance trust and facilitate information sharing and auditability.
- **Proven, Scalable Solution:** An integrated, scalable, and interoperable open-architecture solution can adapt rapidly to emerging threats, while enabling a future-proof environment that meets the highest operational standards.

Various possible technical approaches and decision support frameworks may be considered, including qualitative approaches (e.g., clinical/analyst judgment, structured professional judgment), quantitative models (e.g., Bayesian Belief Networks and probabilistic models), machine learning approaches (e.g., decision trees, random forests, artificial neural networks, reinforcement learning approaches), AI expert systems, and hybrid combinations of multiple approaches (see Fig.3). Qualitative modeling approaches are not readily validated and may reflect possible idiosyncratic backgrounds or biases of individual analysts who inform the methods. Quantitative approaches generate testable predictions but may not address contextual factors that are recognized and

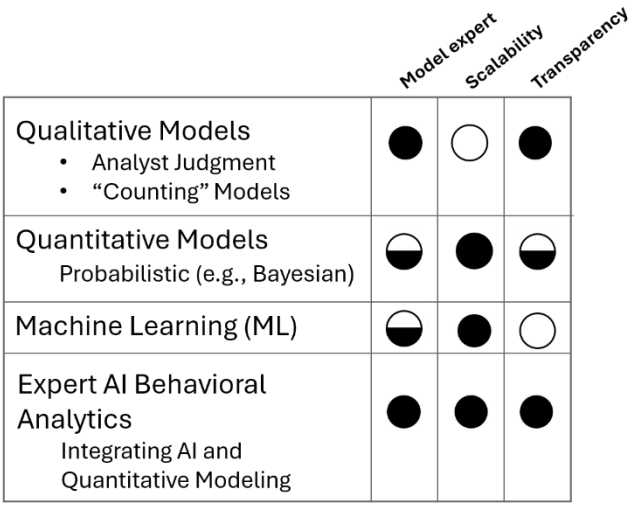


*Figure 3. Comparing Risk Assessment Modeling Approaches*

accounted for by expert analysts. Machine learning approaches produce quantitative/testable outputs, but they are limited by the range of cases over which they are trained and they tend to reflect opaque or "black box" solutions that are not readily explainable. AI expert systems are built to reflect human expertise and, depending upon the type of implementation, they too may present difficulties for a human expert to interpret and evaluate. Combinations of approaches and the integration of generative AI Large Language Models are being adopted to address these types of drawbacks.

A trusted AI approach can integrate important technical features within a behavioral science framework that facilitates early detection of behavioral indicators such as malicious intent or severe disengagement. Key technical elements are the ability to recognize complex patterns that traditional approaches often miss, explainability/auditability that provides clear provenance of diagnostic results, and human-in-the-loop oversight that places the AI in the position of augmenting, rather than replacing, human judgment [24]. Cogynt.ai [25], an expert AI behavioral analytic decision intelligence platform, is described in an accompanying paper in this *2026 INMM Proceedings* [26]. The Cogynt.ai platform provides a mix of automated support and human-in-the-loop expert-oversight – with complete transparency and explainability by design – that offers a powerful trusted AI solution for insider risk assessment and management in the nuclear power industry.

# IMPLEMENTATION CONSIDERATIONS: GOVERNANCE, PRIVACY, AND TRUST

## Cross-Functional Governance to Break Silos

Because key signals span people, process, and technology, effective insider risk management depends on a governance model that integrates HR, legal, physical security, cybersecurity, and OT engineering while clearly defining decision rights and privacy boundaries. A centralized program owner (or steering committee) can reduce information silos, establish consistent response playbooks, and align insider risk efforts with safety culture initiatives. Without such integration, behavioral risk indicators remain fragmented, and interventions become delayed or inconsistent.

## Privacy, Workforce Trust, and Proportional Response

Privacy concerns and perceived surveillance can undermine insider-risk programs by reducing employee trust and discouraging reporting. Nuclear environments therefore require a transparent "proportionality" principle: monitoring and analytics should be aligned to legitimate safety and security objectives, constrained by policy, and paired with response options that are not automatically punitive. Emphasizing early support (e.g., fatigue management, workload adjustment, counseling resources, or supervisory oversight) can help sustain a reporting culture and reduce the risk that programs are seen as adversarial. Behavioral Observation Programs and continuous evaluation mechanisms can be more effective when employees believe the system is fair and oriented toward prevention.

## Trusted AI Safeguards for Safety-Critical Decision Support

When AI is used to support insider-risk decisions, trustworthiness depends on transparency, auditability, and security. In practice, this means models should provide interpretable rationales for alerts (why the system flagged the behavior), enable analyst review and override, and be tested for bias and performance drift. In addition, the AI itself becomes part of the attack surface and must be protected against manipulation. National guidance emphasizes that insider threat mitigation should integrate people, process, and technology with clear governance and response actions [27]. For nuclear operators, an explainable expert AI approach can reduce cognitive overload in analysts while preserving accountability for decisions made in high-stakes contexts.

## DISCUSSION

The insider risk in nuclear settings does not only reflect a "bad actor" problem; it is also a performance, culture, and governance problem. Disgruntlement-linked sabotage and ideologically motivated acts point to the need for continuous evaluation and workforce support mechanisms. Probe-and-test behaviors and contractor-enabled pathways point to the importance of identity- and role-conditioned monitoring. Organizational negligence cases point to security culture, resourcing, and leadership accountability as central risk determinants. A behavioral analytic framework unifies these themes by treating context as evidence: risk is inferred from patterns over time rather than from isolated anomalies.

Operationally, nuclear organizations must manage the base-rate problem: true insider attacks are rare relative to benign activity, so naive anomaly detection can overwhelm analysts with false positives [11]. This supports two design requirements for an Expert AI approach. First, escalation logic should be conditioned on identity and role context (expected access, typical workflows, and risk-critical actions). Second, alerts must be explainable and actionable—linking observed signals to plausible hypotheses and recommended next steps. This yields more efficient triage and defensible intervention decisions: Transparent analytics, clear governance, and proportionate intervention pathways reinforce institutional trust, support continuity of operations, and improve decision quality under uncertainty. This enables not only earlier warning but also consistent, accountable, and lawful handling of early indicators.

The expert AI approach described in this article emphasizes structured reasoning and explainability: Instead of producing opaque risk scores, it encodes analyst knowledge into hierarchical models that relate low-level signals (events) to mid-level patterns and high-level risk hypotheses. This supports traceable justifications—critical in safety-regulated environments where decisions must be auditable and defensible. A practical extension of this idea is "identity-conditioned monitoring," which reframes insider detection as a probabilistic pipeline in which identity-specific context increases the chance that meaningful early-stage signals are correlated and escalated without indiscriminately lowering alert thresholds [10,11]. By integrating context and behavioral baselines, the framework aims to reduce false positives and analyst overload while enabling earlier interventions left of harm.

Finally, because many risk trajectories begin with stress, fatigue, or procedural drift, interventions should not default to punitive action. Instead, the program should provide graded response options—ranging from supervisor check-ins and temporary access adjustments to formal investigation—aligned with a nuclear security culture that encourages reporting and learning. This "left of harm" posture is consistent with the broader conclusion of energy-sector research: cybersecurity is as much a human issue as a technical one, and durable improvements require cultural and organizational reinforcement [2,9].

## CONCLUSION

Insider threat mitigation in nuclear power environments must evolve from reactive, technically centered monitoring toward proactive, human-centric risk management. Negligence, manipulation susceptibility, and organizational conditions routinely shape security outcomes; but awareness training alone seldom produces lasting behavioral change [1–3]. An expert AI behavioral analytic modeling framework—grounded in SOFIT [21] and implemented as explainable, identity-conditioned decision intelligence—offers a path to earlier detection with fewer false positives and stronger accountability. Achieving these benefits, however, requires cross-functional governance, privacy-preserving program design, and a trusted, transparent approach to analytics that supports proportional intervention and sustained nuclear security culture. More broadly, the value of such an approach should also be understood in terms of organizational resilience: its ability to reinforce institutional trust, support continuity of operations, and improve decision quality under uncertain and safety-critical conditions. Future work should refine nuclear-specific indicator taxonomies, validate models in realistic OT environments, and define evaluation metrics that demonstrate not only better detection, but stronger prevention, trust, and operational resilience.

## REFERENCES


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

[2] 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). https://doi.org/10.36948/ijfmr.2025.v07i06.63932

[3] Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? https://arxiv.org/abs/1901.02672, accessed May 10, 2026.

[4] 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).

[5] 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*.

[6] Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

[7] Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "deficient user" in cybersecurity discourses. *Science, Technology, & Human Values, 46*(6), 1316–1339.

[8] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32–64. file:///D:/Cogility%20Software/Marketing%20Material/AI%20evolution%20paper/Endsley_MR_Toward_a_Theory_of_Situation_Awareness_.pdf

[9] Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., … Baker, T. (2018). Security threats to critical infrastructure: The human factor. *The Journal of Supercomputing, 74*(10), 4986–5002.

[10] Gabbay, L., Nickerson, C., Noonan, C. (2026). SHIFTING DETECTION LEFT: Identity-Conditioned Monitoring for Early Insider Threat Detection in High Consequence Systems. *International Conference on Nuclear Security (ICONS),* Vienna, Austria, May 11-15, 2026.

[11] Axelsson, S. (1999). The base-rate fallacy and its implications for the difficulty of intrusion detection. *Proceedings of the 6th ACM Conference on Computer and Communications Security*, Nov 1-4, 1999. Kent Ridge Digital Labs, Singapore. https://www.engineering.iastate.edu/~guan/course/backup-0982/CprE-592-YG-Fall-2002/paper/intrusion/baserate.pdf

[12] UtilityDive. (2012). Sabotage suspected in San Onofre plant investigation. https://www.utilitydive.com/news/sabotage-suspected-in-san-onofre-plant-investigation/77606/, accessed May 10, 2026.

[13] Power Engineering. (2012). Sabotage suspected in San Onofre nuclear plant investigation. https://www.power-eng.com/nuclear/sabotage-suspected-in-san-onofre-nuclear-plant-investigation/, accessed May 10, 2026.

[14] HuffPost. (2012). San Onofre nuclear plant sabotage. https://www.huffpost.com/entry/san-onofre-nuclear-plant-sabotage_n_2215260, accessed May 10, 2026.

[15] World Nuclear News. (2014). Doel 4 shuts down after worker action. https://www.world-nuclear-news.org/Articles/Doel-4-shuts-down-after-worker-action, accessed May 10, 2026.

[16] Brussels Times. (2021). Enquiry into nuclear plant sabotage comes to no conclusion. https://www.brusselstimes.com/181163/enquiry-into-nuclear-plant-sabotage-comes-to-no-conclusion, accessed May 10, 2026.

[17] VRT. (2019). Five years on, still no clue as to who sabotaged Doel nuclear reactor. https://www.vrt.be/vrtnws/en/2019/08/05/five-years-on-still-no-clue-as-to-who-sabotaged-doel-nuclear-rea/, accessed May 10, 2026.
[18] Center for Development of Security Excellence (CDSE). (2014). *Insider Threat Case Study: Charles Eccleston*. https://www.cdse.edu/Portals/124/Documents/casestudies/Insider-Threat-Case-Study-Charles-Eccleston.pdf, accessed May 10, 2026.
[19] U.S. Department of Justice (DOJ). (2013). Former U.S. Nuclear Regulatory Commission employee sentenced to prison for attempted spear-phishing attack. https://www.justice.gov/archives/opa/pr/former-us-nuclear-regulatory-commission-employee-sentenced-prison-attempted-spear-phishing, accessed May 10, 2026.
[20] U.S. Nuclear Regulatory Commission (NRC). (1979). *Circular 79-08: Uranium diversion incident*. https://www.nrc.gov/reading-rm/doc-collections/gen-comm/circulars/1979/cr79008.html, accessed May 10, 2026.
[21] Greitzer, F. L., Purl, J., Leong, Y. M., & Becker, D. E. (2018). SOFIT: Sociotechnical and organizational factors for insider threat. In *IEEE Security and Privacy Workshops (SPW), Workshop on Research for Insider Threat (WRIT)* (pp. 197–206).
[22] Shaw, E. D., & Sellers, L. (2015). Application of the Critical-Path Method to Evaluate Insider Risks. *Studies in Intelligence, 59*(2) (Extracts, June 2015).
[23] Gartner. (2024). *Market Guide for Decision Intelligence Platforms*. Gartner Research. https://www.gartner.com/en/documents/5599159, accessed May 10, 2026.
[24] Intelligence and National Security Alliance (INSA). (2025). Recommendations when using AI in insider risk management. insa_ai_irm_paper.pdf, accessed May 10, 2026.
[25] Cogility. (2026). *Cogynt.ai Decision Intelligence Platform*. https://cogility.com/resources/cogynt-ai-datasheet/, accessed May 10, 2026.
[26] Greitzer, F. L. (2026). Trusted AI decision intelligence support for nuclear material accountability and control. *Proceedings of the INMM 67th Annual Meeting.*
[27] Cybersecurity and Infrastructure Security Agency (CISA). (2022). *Insider Threat Mitigation Guide*. https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf, accessed May 10, 2026.

**Frank L. Greitzer, PhD** is Chief Behavioral Scientist at Cogility Software, where he supports development and deployment of advanced decision intelligence solutions, including insider risk management. With a PhD in mathematical psychology, he has worked as a research psychologist for the US Navy, a human factors and AI researcher in the aerospace industry, and Chief Scientist in cognitive informatics at the U.S. DOE Pacific Northwest National Laboratory (1992-2012). In 2012 he founded PsyberAnalytix to perform consulting in the intersection of social/behavioral sciences and information security. His contributions to research and practice include numerous journal articles, conference papers, and invited talks.

**Christine Noonan** is an applied social scientist and project manager at Pacific Northwest National Laboratory (PNNL). She holds a doctorate in Law and Policy and a master's degree in Anthropology, bringing a rare combination of legal-policy expertise and cultural analysis to insider threat research. Her work integrates organizational dynamics, ethics, and culture with risk assessment and security science to develop practical, evidence-based strategies to mitigate insider risk across critical infrastructure and national security and defense missions.