
# Trusted AI Decision Intelligence Support for Nuclear Material Accountability and Control

Frank L. Greitzer, fgreitzer@cogility.com, Cogility Software

**Abstract**:
Despite significant investment in technical safeguards, the nuclear industry faces challenges detecting human-centric threats to nuclear material control and accountability (MC&A), including information theft, sabotage, nuclear material diversion, and unintentional errors. The high safety, regulatory, and geopolitical demands of the nuclear domain require more mature, human-centric risk models that exceed compliance-focused controls. Traditional perimeter defenses and cybersecurity tools often fail to identify early behavioral risk indicators, leaving analysts in a reactive posture. Effective solutions require proactive strategies that provide timely, reliable, and explainable analytic assessments. This highlights the need for a behavioral-science-driven approach that identifies behavioral indicators of stress, complacency, poor security culture, or malicious intent when assessing anomalies in user behavior, access patterns, and material handling.

## Introduction

Despite major investments in technical safeguards, nuclear material control and accountability (MC&A) programs remain challenged by human-centric risks that are difficult to detect early—e.g., information theft, sabotage, material diversion, and costly unintentional errors. Traditional perimeter defenses and compliance-oriented cybersecurity controls rarely surface early behavioral indicators, leaving analysts reactive and overwhelmed. A behavioral-science-driven, trusted AI approach can proactively detect subtle signals of stress, complacency, deteriorating security culture, or malicious intent in user behavior, access patterns, and material handling—thereby "getting left of harm."

The energy sector's insider-risk profile underscores the stakes: Average costs per malicious insider incident reach ~$14.45M (Seewald, 2023). Insider incidents—both negligent and malicious—are rising across energy domains. Decades of research show that human factors, including negligence, lack of awareness, and susceptibility to manipulation, are central to insider risk in operational technology (OT) and SCADA environments; standard awareness training often fails to produce durable behavioral change (Nazir et al., 2017; Krause et al., 2021; Panful et al., 2025). Nuclear facilities compound these challenges with complex socio-technical interfaces, mixed workforces (employees, contractors, vendors), strict regulation, and expanding digital attack surfaces that increase the opportunity for insider compromise. Workforce volatility and dependency on vendors further elevate exposure. Compared with other sectors, nuclear operations face uniquely severe cyber-physical consequences from insider missteps or malice, emphasizing the need for human-centric risk models.

## Illustrative Cases Exhibiting Behavioral Risk Patterns

Historical nuclear cases illustrate diverse insider archetypes and the need for behavioral and technical detection:

- Disgruntlement—San Onofre diesel generator sabotage. (Zeller, 2012).
- Ideologically motivated sabotage—Koeberg bombing (van Wyk, 2015)
- Espionage/recruitment risks among contractors— Charles Eccleston incident (CDSE/[cdse.edu])
- Probe-and-test behaviors preceding theft—GE Wilmington extortion incident (Hendry, 1980)
- Severe psychosocial crisis culminating in catastrophic action—SL-1 Reactor explosion (Hammer, 2024)
- Undetected operator sabotage with massive economic impact—Doel-4 nuclear plant (Hope, 2021)

These incidents highlight gaps in tracking, continuous evaluation, and psychosocial screening—and the value of comprehensive, cross-functional indicators over siloed technical alerts. Beyond malicious insiders, negligent insider behaviors—unpatched systems, bypassed procedures, or unreported near-misses—pose material risk to nuclear safety and security culture, reinforcing that insider risk management must address both intent and error.

## Decision Intelligence Approach + Expert AI Behavioral Analytics

Decision Intelligence Platforms (DIP) provide a decision-centric architecture that fuses diverse data, scales across the enterprise, and focuses the analyst's attention with explainable insights. DIPs unify data, AI, and analytics into

timely, reliable, and transparent decision support for dynamic risk environments. A DIP behavioral analytic modeling framework can integrate major risk assessment elements that are identified with effective nuclear MC&A solutions (e.g., Nazir et al., 2017; Krause et al., 2021; Panful et. al., 2025), such as: (1) Behavioral monitoring and User and Entity Behavior Analytics (UEBA) to derive personalized baselines and detect anomalies in usage, access, timing, and data movement; (2) Cognitive and psychological indicators from behavioral science to anticipate noncompliance precursors; (3) Cultural and organizational factors (security climate, reporting norms, governance) that shape risk expression; and (4) Differentiation of careless vs. malicious insiders to calibrate proportionate responses that avoid punitive overreach for human error.

AI solutions must be transparent, auditable, and secure, with traceable influence on outcomes to mitigate the "black box" problem and support operator trust and regulatory scrutiny. The objective is to augment human analysts—reducing cognitive overload and bias while preserving human judgment in the loop. To this end, **Cogynt.ai**, an expert AI behavioral analytics platform, uses a pattern-based, hierarchical complex-event processing (HCEP) modeling framework to encode expert analyst tradecraft and domain knowledge into multi-layer patterns that combine psychosocial indicators, cyber-physical signals, and organizational context—yielding explainable, traceable inferences suitable for safety-critical environments for nuclear MC&A. Integrated cyber-physical analytics blends behavioral science and advanced analytics to enhance MC&A by establishing dynamic user baselines to support triaging of anomalous behaviors and suspicious interactions reflecting collusive patterns.

Implementing a decision-intelligence-driven, expert-AI behavioral framework in nuclear facilities will:

- enable early detection of insider MC&A risks by analyzing patterns of behavioral and technical indicators;
- reduce false positives using analytics that align anomalies with roles, workloads, and operational context;
- strengthen nuclear security culture by emphasizing intrinsic motivation and psychologically safe reporting;
- enhance cross-functional collaboration and governance for whole-person risk visibility; and align with evolving regulatory and international best practices on human-centric cybersecurity and MC&A.

**Conclusion**

Insider risk in nuclear operations is inherently human and socio-technical. By integrating behavioral science with trusted, explainable AI in a decision intelligence platform—grounded in UEBA, psychosocial indicators, cultural diagnostics, and OT/ICS context—nuclear organizations can move from reactive alerting to proactive, positive, and proportionate intervention. This approach enhances resilience, advances MC&A effectiveness, and supports operators and analysts with transparent, auditable decision support suited to high-consequence environments.

**References**


CDSE Official CDSE case study, Charles Eccleston. https://www.cdse.edu/Portals/124/Documents/casestudies/Insider-Threat-Case-Study-Charles-Eccleston.pdf

Hope, A. (2021). Enquiry into nuclear plant sabotage comes to no conclusion. The Brussels Times. Feb 11, 2021. https://www.brusselstimes.com/181163/enquiry-into-nuclear-plant-sabotage-comes-to-no-conclusion

Krause, T., Ernst, R., Klaer, B., Hacker, I., & Henze, M. (2021). Cybersecurity in power grids: Challenges and opportunities. *Sensors, 21(18),* 6225.

Hammer, A. (2024). Mystery of America's first fatal nuclear disaster - with rumors still rife over 60 years later that explosion in remote Idaho town was triggered by one man's murderous rage amid LOVE TRIANGLE. Daily Mail, April 6, 2024. https://www.dailymail.co.uk/news/article-13271859/mystery-america-nuclear-disaster-idaho-love-triangle-murder-suicide.html

Hendry, W.J. (1980). Safeguards System Response in an Actual Uranium Diversion Incident. *INMM Proceedings*. https://resources.inmm.org/annual-meeting-proceedings/safeguards-system-response-actual-uranium-diversion-incident

Nazir, S., Patel, S., & Patel, D. (2017). Assessing and augmenting SCADA cybersecurity: 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)*.

Seewald, L. (2023, July 19). *Insider risk in the energy sector – Case study*. Security Boulevard. https://securityboulevard.com/2023/07/insider-risk-in-the-energy-sector-case-study/

van Wyk, J. (2015). Nuclear terrorism in Africa: The ANC's Operation Mac and the attack on the Koeberg Nuclear Power Station in South Africa. *Historia*, *60(2).* https://doi.org/10.17159/2309-8392/2015/V60N2A3

Zeller, T. (2012). San Onofre Nuclear Plant Investigating Possible Sabotage Of Safety System. *Huffington Post*, Nov 29, 2012. https://www.huffpost.com/entry/san-onofre-nuclear-plant-sabotage_n_2215260