Volume 11, Issue 4, April – 2026 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1020

Beyond Barriers and Sensors: Integrating Human Reliability into Physical Protection Systems for High-Activity Radioactive Sources

Cyril Cyrus Arwui[1*]; Henry Lawluvi[1]; Nelson Agbemava[1]; Etornam Ann Mensah[1]; Emmanuel Akrobortu[1]; Charles Kansaana[1]

[1]Nuclear Regulatory Authority, Ghana.

Publication Date: 2026/04/22

Abstract: High-activity radioactive sources used in irradiation and industrial applications require physical protection systems (PPS) that can deter, detect, delay and enable response against theft, sabotage and insider-enabled removal. This paper examines PPS effectiveness for high-activity sealed radioactive sources through a socio-technical lens, using cobalt-60 facilities as a representative case. Drawing on international nuclear security guidance, the study integrates design basis threat concepts, performance-based PPS evaluation and human reliability analysis. A simple worked probabilistic model is used to compare two operating conditions: disciplined alarm handling and degraded performance characterized by alarm fatigue, poor communication and slower dispatch. The example shows that when sensor and transmission performance remain unchanged, deterioration in alarm assessment, communication reliability and response timing can reduce interruption probability from 0.578 to 0.150, representing a decline of about 74%. The analysis demonstrates that protection effectiveness is not determined by hardware alone; it depends on the interaction of technical layers, operator performance, organizational routines, insider threat controls and cyber-dependent support systems. The paper argues that regulators and operators should treat human reliability assurance, security culture and performance testing as core components of PPS design and oversight. This approach strengthens interruption capability and reduces the likelihood that high-activity radioactive sources become out of regulatory control.

Keywords: *Physical Protection System; Human Reliability; Security Culture; Design Basis Threat; Insider Threat; Cobalt-60.*

How to Cite: Cyril Cyrus Arwui; Henry Lawluvi; Nelson Agbemava; Etornam Ann Mensah; Emmanuel Akrobortu; Charles Kansaana (2026) Beyond Barriers and Sensors: Integrating Human Reliability into Physical Protection Systems for High-Activity Radioactive Sources. *International Journal of Innovative Science and Research Technology*, 11(4), 1577-1581. https://doi.org/10.38124/ijisrt/26apr1020

I. INTRODUCTION

High-activity sealed radioactive sources are essential to medical equipment sterilization, industrial irradiation, radiography, research and a range of other legitimate activities. At the same time, their loss of regulatory control can create serious security consequences, particularly where a source could be stolen, maliciously used or incorporated into a radiological dispersal or exposure device [1], [2]. For this reason, international nuclear security guidance requires that protective measures for radioactive sources be graded according to the potential consequences of unauthorized removal, sabotage or misuse [1]–[3].

Physical protection systems provide the structured means to deter, detect, delay and support response to malicious acts. In performance-based security practice, the central question is whether the combined system can interrupt an adversary before mission completion. This logic is normally anchored in a design basis threat that defines credible adversaries, capabilities and tactics, including outsider attack, insider abuse of authorized access and collusion [4]–[6].

In practice, however, PPS effectiveness is often assessed too narrowly as a hardware problem. Sensors, locks, barriers, cameras and access control devices are visible and measurable, so they attract most design attention. Yet the effectiveness of those technologies depends on people who assess alarms, communicate credible threats, dispatch responders and maintain procedural discipline. Where alarm triage is weak, response is delayed or organizational culture normalizes deviations, the installed hardware may still function while the protection system as a whole fails [4], [7], [8].

These vulnerabilities are especially relevant for facilities using high-activity cobalt-60 sources. Such facilities may not have the extensive defensive depth typical of major nuclear installations, but the radiological consequences of

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1020

unauthorized removal can still be severe. In addition, growing dependence on networked alarm transmission, digital access control and video assessment introduces cyber-physical dependencies that can silently degrade protection performance if they are not managed appropriately [9].

This paper therefore reframes PPS effectiveness for high-activity radioactive sources as a socio-technical problem. It reviews the relevant security literature, develops an analytical model linking technical detection to human performance and timing margin, and uses a worked example to show how human reliability degradation can materially reduce interruption probability. The objective is not to replace established PPS design methods, but to demonstrate why human reliability, insider threat mitigation and security culture should be treated as core determinants of physical protection performance.

II. LITERATURE REVIEW

A. High-Activity Sources and Graded Protection

IAEA guidance adopts a graded approach to radioactive source security, meaning that sources with higher activity and greater potential consequences require stronger protection. Category-based source management is intended to align regulatory effort, operator obligations and protective controls with the severity of possible misuse [1], [2]. For high-activity sources, the protection objective extends beyond routine radiation safety; it includes preventing theft, diversion, sabotage and any pathway by which the source could leave regulatory control [1], [3].

This graded logic matters for facility design because it frames security not as a generic checklist, but as a risk-informed obligation. For example, the expectations for access control, surveillance, key management and response capability should be stronger where the source attractiveness and radiological consequences are higher. A source facility that is formally compliant but operationally fragile may still be security-vulnerable if the protective measures are not reliable under realistic threat conditions.

B. PPS Performance Logic and the Design Basis Threat (DBT)

Performance-based PPS evaluation focuses on whether the system can interrupt an adversary before the target objective is achieved. In practical terms, the system must first detect adversary action, then delay progress long enough for assessment, communication and response to occur. A design basis threat provides the reference adversary profile against which the system is designed and evaluated [4]–[6].

The design basis threat is especially important for high-activity sources because adversaries may rely on stealth, deceit, force or insider support rather than frontal attack. If the threat definition ignores insider facilitation, timing manipulation or exploitation of routine operational weaknesses, the resulting PPS may appear technically adequate while remaining vulnerable in practice. A credible DBT therefore has to include both technical and human exploitation pathways.

C. Human Reliability, Insider Threat and Security Culture

Human reliability affects several critical PPS functions: enforcing access authorization, assessing whether an alarm is genuine, communicating a security event, initiating dispatch and coordinating response. These are not peripheral administrative tasks; they are the operational bridge between technology and interruption performance [4], [7], [8]. When those actions are unreliable, protective depth is effectively reduced even if every installed sensor and barrier remains intact.

Insider threat further intensifies this concern. An authorized individual may possess knowledge of routines, access routes, response habits and vulnerabilities in key control or alarm handling. Because insiders can bypass or weaken multiple layers simultaneously, effective protection requires separation of duties, access authorization integrity, behavioral monitoring and a security culture that discourages normalization of deviance [7], [8], [13].

Security culture is relevant here because it shapes whether personnel treat alarms seriously, report suspicious behavior, challenge procedural shortcuts and sustain vigilance during routine operations. A poor security culture does not merely increase the probability of human error; it can become a persistent enabler of adversary success.

D. Cyber-Physical Dependence in Modern PPS

Many contemporary protection systems depend on digital components, including alarm annunciation platforms, electronic access control databases, CCTV networks and communication interfaces. These dependencies can create single points of failure if the digital layer is compromised, misconfigured or allowed to drift from its intended state [9], [14].

For radioactive source facilities, the key implication is that computer security cannot be treated as a separate technical domain with no impact on physical protection. If alarm data are delayed, suppressed or misrouted, detection probability in functional terms declines even when the sensor hardware remains physically present. Cyber reliability therefore contributes directly to physical protection effectiveness.

III. METHODOLOGY

A. Analytical Framework

This paper uses a qualitative, case-informed analytical approach based on international nuclear security guidance and standard PPS performance logic. Rather than conducting a full adversary sequence interruption simulation, it develops a transparent micro-model that isolates the operational chain linking detection to interruption. The approach is appropriate for a conceptual paper because the objective is to show how human reliability enters the interruption problem, not to claim facility-specific performance values.

The analysis considers a representative high-activity source pathway in which adversary progress can be interrupted only if three conditions are satisfied: the adversary is detected and the alarm is correctly assessed; communication and

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1020

dispatch of response occur successfully; and the response force arrives before the adversary completes the critical task.

B. Probability Model

The overall probability of interruption is expressed as:

$$P_I \approx P_D \times P_C \times P_T \quad (1)$$

Where P_I is the interruption probability, P_D is the probability that adversary action is detected and correctly assessed, P_C is the probability that communication and dispatch occur successfully, and P_T is the probability that response arrives in time to interrupt the adversary.

To show where human performance enters the detection chain, P_D is decomposed as:

$$P_D = P_S \times P_{Tx} \times P_A \quad (2)$$

where P_S is the probability that the sensor detects adversary action, P_{Tx} is the probability that the alarm is transmitted successfully, and P_A is the probability that operators assess the alarm correctly and treat it as real.

Timing success is represented with a simple normal approximation. Let D be the available delay after detection and let T_R be the response time to the engagement point. Interruption is feasible when the timing margin

$M = D - T_R$ is positive. If D and T_R are modeled as normal variables, then:

$$P_R = \Phi((\mu D - \mu R) / \sqrt{(\sigma D^2 + \sigma R^2)}) \quad (3)$$

where μD and μR are the mean delay and mean response time, σD and σR are their standard deviations, and Φ is the cumulative standard normal function. The model is intentionally simple, but it makes the timing consequences of human reliability degradation explicit.

C. Worked Scenario Design

Two scenarios are examined. The baseline scenario represents disciplined alarm handling in a reasonably configured facility. The degraded scenario keeps hardware performance unchanged but introduces three human and organizational failures: poorer alarm assessment because nuisance alarms have been normalized, weaker communication and dispatch reliability, and slower, more variable response caused by unclear escalation and weak coordination.

The values used in the worked example are illustrative rather than empirical. Their purpose is to show directional sensitivity and to demonstrate that human-performance changes can materially reduce interruption probability even when the physical equipment remains constant. This is consistent with the socio-technical argument advanced in the literature [4], [7], [8].

IV. RESULTS AND DISCUSSION

A. Conceptual Interpretation of PPS Performance

Fig. 1 summarizes the socio-technical logic used in this paper. Technical layers such as sensors, barriers and access control remain essential, but they do not translate automatically into successful interruption. Alarm assessment, communication, dispatch discipline, insider controls, cyber reliability and security culture shape whether detection becomes timely response.

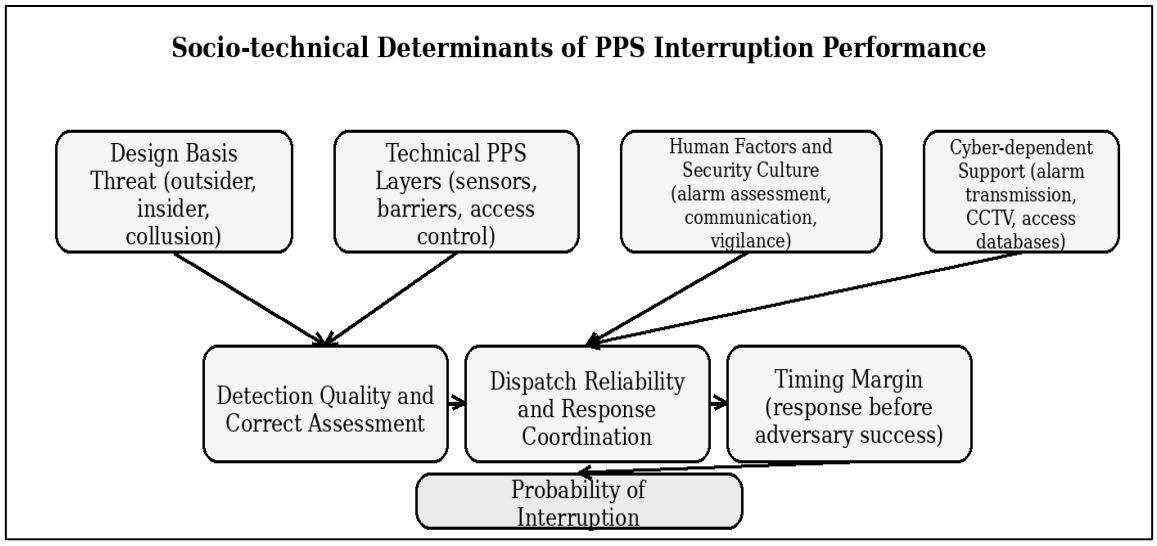

Fig. 1. Socio-Technical Determinants of PPS Interruption Performance.

B. Baseline and Degraded Scenarios

In the baseline scenario, the representative pathway assumes $P_S = 0.95$, $P_T = 0.98$ and $P_A = 0.90$. This yields $P_D = 0.838$. Communication and dispatch success is set at $P_C = 0.95$. The timing model assumes an average available delay after detection of 240 seconds with a standard deviation of 30 seconds, and an average response time of 210 seconds with a standard deviation of 25 seconds. Under these conditions, the timing success probability is $P_R = 0.726$ and the resulting interruption probability is $P_I = 0.578$. The degraded scenario

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1020

holds P_S and P_T constant but reduces alarm assessment reliability to P_A = 0.60 because personnel have become desensitized to nuisance alarms. Communication and dispatch success falls to P_C = 0.70, while mean response time increases to 260 seconds with a standard deviation of 40 seconds. The timing success probability falls to P_R = 0.383 and the overall interruption probability falls to P_I = 0.150.

C. Quantified Effect of Human Reliability

The comparative result is shown in Table 1. The transition from disciplined operations to degraded alarm handling and slower dispatch reduces interruption probability from 0.578 to 0.150. This represents a reduction of about 74%, achieved without changing the sensor layer, alarm transmission hardware or physical barriers.

The implication is that human reliability behaves as a timing amplifier. Small degradations in assessment quality and response coordination compress the response window and can shift the system from probable interruption to probable adversary success. For high-activity sources, where an informed adversary may remove or access the target within a short interval, this change is operationally decisive.

Table 1. Comparative Effect of Human Reliability Degradation on Interruption Performance.

Parameter	Baseline	Degraded	Effect
P_S	0.95	0.95	No hardware change
P_T	0.98	0.98	No transmission change
P_A	0.90	0.60	Assessment quality falls
P_C	0.95	0.70	Dispatch reliability weakens
Response time, μR (s)	210	260	Slower response
Timing success, P_R	0.726	0.383	Margin contracts
Interruption, P_I	0.578	0.150	About 74% reduction

D. Practical and Regulatory Implications

The worked example supports three practical conclusions. First, security culture initiatives should be evaluated not only as compliance activities but as performance interventions that increase P_A and P_C. Second, response drills, role clarity and redundant communication pathways matter because they improve both the mean and variability of response time, thereby increasing P_R. Third, facilities should not infer PPS effectiveness from equipment inventories alone; performance depends on whether technical and human layers function together under credible design basis threat conditions [5], [6], [15].

The analysis also has regulatory implications. Oversight that checks only the presence of sensors, locks and procedures may miss the real determinants of interruption capability. Inspection and periodic review should therefore include alarm handling practices, communication drills, access authorization integrity, cyber-dependent alarm reliability and the quality of insider threat mitigation [3], [8], [9], [15].

A limitation of this paper is that the worked example is illustrative and not based on a site-specific dataset or a full EASI-type facility model. Even so, the example is useful because it clarifies causation: human and organizational degradation can materially reduce PPS effectiveness even when hardware is left unchanged. That finding is directly relevant to high-activity source facilities operating with limited staffing and constrained resources.

V. CONCLUSION AND RECOMMENDATIONS

A. Conclusion

This paper argues that physical protection effectiveness for high-activity radioactive sources is a socio-technical outcome rather than a purely engineering property. Using a cobalt-60 source facility as a representative case, it showed that interruption depends on more than detection hardware and barrier strength. Alarm assessment, communication discipline, response coordination, insider threat controls and cyber reliability all shape whether an adversary is interrupted before mission success.

The worked example demonstrated that deterioration in human and organizational performance can reduce interruption probability by about 74% even when sensor and transmission performance remain unchanged. This finding reinforces a core nuclear security lesson: a technically installed PPS can still fail operationally if the human bridge between alarm and response is unreliable.

B. Recommendations

To strengthen PPS effectiveness for high-activity source facilities, the following measures are recommended. First, regulators should extend oversight beyond hardware verification to include alarm handling, dispatch discipline, response drills and insider threat exercises. Second, operators should reduce nuisance alarms, clarify escalation pathways and train staff to classify and act on alarms consistently. Third, facilities should adopt separation of duties, stronger credential management and proportionate insider threat controls. Fourth, cyber-dependent components of the PPS should be maintained, monitored and backed up so that silent digital

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1020

failures do not degrade physical protection performance. Finally, human reliability and security culture should be treated as measurable security variables that are periodically tested and improved, not as administrative afterthoughts.

REFERENCES

[1]. International Atomic Energy Agency, "Nuclear Security Recommendations on Radioactive Material and Associated Facilities," IAEA Nuclear Security Series No. 14, Vienna, 2011.
[2]. International Atomic Energy Agency, "Categorization of Radioactive Sources," IAEA-TECDOC-1344, Vienna, 2003.
[3]. International Atomic Energy Agency, "Objective and Essential Elements of a State's Nuclear Security Regime," IAEA Nuclear Security Series No. 20, Vienna, 2013.
[4]. M. L. Garcia, The Design and Evaluation of Physical Protection Systems, 2nd ed. Burlington, MA: Butterworth-Heinemann, 2008.
[5]. International Atomic Energy Agency, "Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)," IAEA Nuclear Security Series No. 13, Vienna, 2011.
[6]. International Atomic Energy Agency, "Development, Use and Maintenance of the Design Basis Threat," IAEA Nuclear Security Series No. 10, Vienna, 2009.
[7]. International Atomic Energy Agency, "Nuclear Security Culture," IAEA Nuclear Security Series No. 7, Vienna, 2008.
[8]. International Atomic Energy Agency, "Preventive and Protective Measures against Insider Threats," IAEA Nuclear Security Series No. 8, Vienna, 2008.
[9]. International Atomic Energy Agency, "Computer Security at Nuclear Facilities," Vienna, 2011.
[10]. International Atomic Energy Agency, "Security of Radioactive Sources," IAEA Nuclear Security Series No. 11, Vienna, 2009.
[11]. International Atomic Energy Agency, "Incident and Trafficking Database (ITDB) Fact Sheet," Vienna, 2022.
[12]. J. Reason, Managing the Risks of Organizational Accidents. Aldershot: Ashgate, 1997.
[13]. U.S. Nuclear Regulatory Commission, Insider Mitigation Program Guidance, Washington, DC, 2013.
[14]. International Atomic Energy Agency, Computer Security Techniques for Nuclear Facilities, Vienna, 2020.
[15]. International Atomic Energy Agency, Security During the Lifetime of a Nuclear Facility, IAEA Nuclear Security Series No. 35-G, Vienna, 2018.
[16]. M. L. Garcia, Vulnerability Assessment of Physical Protection Systems. Sandia National Laboratories, 2006.