

Multi-Perspective Security Risk Assessment for APT Attacks in CPS Environment An Adapted Review of a Knowledge-Driven, Evidence-Based Framework

Pooja Laxman Yelwande¹, P. P. Chavan², A. J. Shaikh³, H. B. Jadhav⁴

Student, Department of Computer Engineering, Adsul Technical Campus, Chas, Ahilyanagar, India ¹

Guide, Department of Computer Engineering, Adsul Technical Campus, Chas, Ahilyanagar, India ²

Co-guide, Department of Computer Engineering, Adsul Technical Campus, Chas, Ahilyanagar, India ³

HOD, Department of Computer Engineering, Adsul Technical Campus, Chas, Ahilyanagar, India ⁴

Abstract: *Advanced Persistent Threats (APTs) are carefully planned, multi-stage cyberattacks in which an attacker attempts to maintain hidden access to a target over an extended period. Their effects become more serious in cyber-physical-social (CPS) environments, where digital systems, physical equipment, people, and organizational processes depend on one another. Traditional security assessment methods often focus on individual technologies or assets and may not fully represent how an attack can spread between these connected layers. This paper presents an adapted review of a multi-perspective framework for assessing APT-related security risks in CPS environments. The framework links knowledge-based attack-scenario generation, a Mission-Critical Target System (MCTS) model, a risk-aware problem-domain ontology (RaPDO), adaptive security requirements engineering (ASRE), and an Integrated Security Risk Assessment Process (ISRAP). It extends the traditional confidentiality, integrity, and availability (CIA) assessment by considering safety and social trust, producing a five-dimensional CIAST view. Risk estimates and security requirements are revised periodically or when new implementation evidence becomes available. The approach is designed to improve traceability, mission alignment, and practical risk prioritization. The reviewed work reports theoretical analysis and case studies involving smart-grid and smart-transportation scenarios, while also identifying limitations in automation and large-scale validation. The paper retains the central ideas of the source study and presents them in a student-paper format.*

Keywords: Advanced Persistent Threats, Cyber-Physical-Social Systems, Security Risk Assessment, Mission-Critical Target System, Security Requirements, CIAST, Ontology.

I. INTRODUCTION

Organizations increasingly depend on connected digital services, automated equipment, communication networks, and data-driven decision-making. These technologies improve efficiency, but they also create opportunities for sophisticated cyberattacks. An Advanced Persistent Threat (APT) is a prolonged and strategic attack in which an adversary uses multiple stages and techniques to gain access, remain undetected, move through a target environment, and achieve a specific objective. The objective may involve stealing information, disrupting services, manipulating processes, or damaging important infrastructure [1], [2].

The risk is especially important in cyber-physical-social (CPS) environments. In this paper, CPS refers to settings where cyber components, physical processes, people, and social or organizational relationships are closely connected. Examples include smart grids, transportation systems, manufacturing environments, and other critical services. A cyber



compromise can affect software and data, but it may also interrupt equipment, create safety concerns, or reduce public and organizational trust [8], [18], [19].

A security assessment must therefore look beyond a single computer or network. For example, an attacker who compromises an application may reach a server, affect an operational process, and eventually interrupt a mission-critical service. The importance of the application, server, process, and personnel depends partly on how they support one another. A method that considers each asset separately may overlook these cascading effects.

Conventional methods—including attack trees, attack patterns, cyber kill-chain models, and traditional risk scoring—offer useful ways to understand threats. However, they may treat attack scenarios as static, focus mainly on technical controls, or fail to connect threat modeling with the continuing revision of security requirements. The framework reviewed here seeks to join these activities in a traceable process: model attacker tactics, identify connected assets, derive security requirements, and assess risk using documented evidence.

A. Problem Statement

The main problem is how to assess evolving APT attacks in CPS environments where cyber, physical, human, and organizational elements are interdependent. A useful framework must identify realistic attack paths, determine which assets are most important to the mission, reflect the potential safety and trust impacts, and update risk estimates when the security situation changes.

B. Objectives and Contributions

- Connect APT lifecycle and Tactics, Techniques, and Procedures (TTPs) to the assets and requirements they affect.
- Represent mission-critical assets and their vertical and horizontal dependencies using an MCTS model.
- Extend CIA-based impact assessment with Safety and Social Trust, forming the CIAST model.
- Use structured knowledge and documented evidence to support traceable risk evaluation and iterative updates.
- Discuss the framework's benefits, limitations, and potential future improvements.

II. RELATED WORK

Research on APT defense has explored intrusion detection systems, event-log analysis, anomaly detection, machine-learning models, and correlation of events from different sources. These methods can improve the identification of suspicious behavior and help security teams respond to incidents. However, detection performance alone does not explain all consequences of an attack across connected assets and operational layers [3], [7], [20]–[28].

A second research direction models APT stages, attacker tactics, and attack paths. Frameworks based on attack trees, attack graphs, lifecycle models, and MITRE ATT&CK help organize the sequence of attacker actions and connect techniques with possible targets [4], [10], [13], [29]–[32]. Such models can support scenario analysis, but a scenario may become outdated as attacker techniques and system configurations change.

Quantitative and mathematical approaches use probability, diffusion models, risk equations, and strategic analysis to estimate attack progression or compare defensive options. These methods are useful for structured analysis, yet abstract models may not represent every operational dependency among technology, people, organizational policy, and physical processes [9], [33], [34].

Dynamic and proactive risk assessment methods update estimates as new information becomes available. Ontology-based methods can organize knowledge about threats, assets, weaknesses, vulnerabilities, and controls so that relationships remain explicit and traceable [11], [14]–[17]. Nevertheless, risk updating by itself does not necessarily provide an end-to-end link from APT modeling to security requirements and mission-level impact.

Multidimensional studies have highlighted the role of social engineering, human decision-making, organizational processes, and cooperation among different attacker roles [6], [35], [36]. These studies broaden the view of APTs, but social and organizational observations are not always translated into a systematic and evidence-based operational risk



process. The reviewed framework addresses this gap by integrating threat scenarios, cross-layer asset dependencies, adaptive requirements, and risk evaluation in one workflow.

III. PROPOSED MULTI-PERSPECTIVE FRAMEWORK

The framework is organized around five connected components: the APT Attack Scenario Model, the Mission-Critical Target System (MCTS) Model, the Risk-aware Problem Domain Ontology (RaPDO), Adaptive Security Requirements Engineering (ASRE), and the Integrated Security Risk Assessment Process (ISRAP). An iterative risk-evaluation mechanism works across these components. The intended workflow links attacker behavior to affected assets, security requirements, implementation evidence, and updated risk scores.

A. APT Attack Scenario Model

The scenario model provides structured descriptions of how an APT may progress. A scenario can be based on a reported incident or a simulated attack. It is represented using five main elements: attacker, attack lifecycle, tactical objectives, actions or techniques, and target. This structure helps analysts connect what an attacker intends to do with the techniques used and the assets that may be affected.

The lifecycle described in the source study contains five stages: Preparation, Initial Intrusion, Expansion, Action on Objectives, and Cleanup. During preparation, an attacker gathers information and plans an approach. Initial intrusion establishes access. Expansion may involve privilege escalation or movement to additional assets. Action on Objectives concerns the attacker's intended outcome, such as data theft or disruption. Cleanup includes attempts to remove traces or reduce the chance of detection. Real incidents may not follow every stage in a fixed order.

Scenario information can be drawn from structured resources such as MITRE ATT&CK, CAPEC, CWE, and CVE, supplemented by technical reports, academic papers, and practitioner knowledge. The knowledge base should be updated as new techniques and vulnerabilities are documented. The framework uses this information to support realistic threat modeling rather than relying only on a fixed, manually prepared scenario.

B. Mission-Critical Target System (MCTS)

The MCTS model represents the organization's protected assets according to their role in achieving a mission. Assets are first identified and classified, their relationships are analyzed, and they are then organized into three connected layers:

- **Cognitive Layer:** mission goals, policies, management processes, operational activities, and personnel.
- **Information-Modeling Layer:** applications, platforms, data, and other information-processing resources.
- **Physical Layer:** servers, computers, mobile devices, appliances, facilities, and other physical infrastructure.

The model records vertical dependencies between different layers and horizontal dependencies within the same layer. For example, a policy may guide how an application is used, an application may depend on a server, and personnel may coordinate through shared information systems. Horizontal links can represent communication between servers or collaboration among employees. Mapping these relationships helps analysts trace how a compromise in one asset can affect other assets and eventually disrupt a mission.

C. Mission-Oriented CIAST Criticality

Traditional asset criticality commonly considers Confidentiality, Integrity, and Availability (CIA). The reviewed framework adds Safety (S) and Social Trust (T), resulting in CIAST. Confidentiality concerns unauthorized disclosure; integrity concerns unauthorized changes; availability concerns whether systems and information remain accessible; safety concerns possible harm to people or physical operations; and social trust concerns confidence in the organization or service.

Each dimension is evaluated using mission-oriented criteria. The source study describes a three-level scale—High = 3, Medium = 2, and Low = 1—and recommends considering dependencies when assigning importance. Supporting



assets may receive higher criticality if essential mission functions rely on them. Assets connected to many others, assets close to mission execution, and assets with important functional relationships may also receive higher priority.

The overall CIAST index is expressed as:

$$CIAST_i = w_C \cdot C_i + w_I \cdot I_i + w_A \cdot A_i + w_S \cdot S_i + w_T \cdot T_i \quad (1)$$

Here, C_i , I_i , A_i , S_i , and T_i represent the five impact scores for asset i , while the w terms are mission-specific weights. Equal weights may be used as a default, or domain experts may assign weights according to the organization's mission. Individual dimension scores should be retained alongside the total so that the reasons for an asset's priority remain understandable and auditable.

IV. KNOWLEDGE REPRESENTATION AND SECURITY REQUIREMENTS

A. Risk-aware Problem Domain Ontology (RaPDO)

RaPDO provides a structured knowledge layer for representing the relationships among APT scenarios, attack techniques, protected assets, weaknesses, vulnerabilities, security requirements, controls, and evidence. An ontology defines the entities in a domain and the relationships between them. Its purpose in this framework is to make the assessment consistent and traceable, rather than to replace expert judgment with unsupported automated conclusions.

The framework links MITRE ATT&CK tactics and techniques to technique entities, CAPEC entries to generalized attack patterns, CWE entries to weaknesses, and CVE entries to known vulnerabilities. Where available, standardized identifiers and reference-based mappings are retained. Normalization rules help represent similar concepts consistently across sources. This supports traceability from an attacker action to an asset, a requirement, and the evidence used to judge whether a control is in place.

The ontology is intended to be lightweight and focused on the information required for risk assessment. It can be extended with additional technique details, mitigation catalogs, or control taxonomies. Its value depends on maintaining reliable source information and documenting how entities and relationships are mapped.

B. Adaptive Security Requirements Engineering (ASRE)

Security requirements describe the protections an organization needs to reduce identified risks. In a changing CPS environment, requirements should not be treated as permanent documents. They may need refinement when new APT techniques are identified, assets are added or reconfigured, vulnerabilities are discovered, or evidence shows that a control is missing or ineffective.

ASRE uses the threat-modeling results and the MCTS asset relationships to elicit and adapt security requirements. For example, if a high-criticality application depends on a server that has weak access control, the assessment may lead to stronger authentication, access restrictions, monitoring, backup, or incident-response requirements. The exact requirement depends on the threat, asset role, mission impact, and available evidence.

Adaptation in the reviewed framework is iterative and evidence-driven. It can occur periodically or after a relevant event, such as an audit result or a change in control implementation. The source does not claim fully automated, real-time reasoning; expert involvement remains important in criticality scoring, weighting, and evidence-compliance evaluation.

V. INTEGRATED SECURITY RISK ASSESSMENT PROCESS

ISRAP brings the framework components together to produce a structured and auditable risk assessment. Its central principle is that a risk estimate should be linked to a defined scenario, an affected asset, the relevant requirements, and documented evidence about the security controls.

A. Main Assessment Steps

- Generate or select an APT scenario from incident information, threat intelligence, or a simulated case.
- Map the scenario's TTPs to target assets in the MCTS model and identify possible paths across connected layers.
- Assess the criticality of affected assets using CIAST and the mission-oriented dependency analysis.



- Identify or revise security requirements through ASRE, connecting each requirement to the threat and asset it addresses.
- Collect implementation evidence, such as audit findings, configuration records, control status, and incident observations.
- Evaluate likelihood and impact using predefined criteria, calculate the risk score, and document the decision.
- Repeat the assessment periodically or when new evidence changes the understanding of likelihood, control status, or asset criticality.

B. Evidence-Based Likelihood Updating

A major feature of the framework is the use of implementation evidence to revise likelihood estimates. Instead of assuming that a control is effective because it has been specified, the assessment considers evidence about whether the control is implemented and operating. Evidence may come from audits, configuration reviews, operational logs, test results, or documented incident reports. Predefined rules are then used to update likelihood and risk scores.

The framework distinguishes expert-driven judgments from rule-based calculations. Experts determine impact and criticality using predefined criteria, mission-specific weights, and documented evidence. Likelihood updates and risk scoring are computed using established rules. This separation improves auditability because an assessor can review the evidence and the rule that led to a changed score.

C. Risk Interpretation and Prioritization

Risk assessment should help an organization decide where to focus limited resources. High-priority assets may require stronger monitoring, hardening, access controls, recovery planning, or incident-response preparation. The combined CIAST score provides a prioritization indicator, but the individual CIAST dimensions should remain visible. Two assets with similar total scores may require different treatments if one presents a safety concern and the other mainly affects confidentiality.

The final output is not simply a list of vulnerabilities. It is a traceable chain from APT behavior to the assets that may be affected, the requirements intended to protect them, the evidence of control implementation, and the risk decision. This structure can help organizations explain why a risk is considered important and what evidence would justify revising the assessment.

VI. DISCUSSION AND EVALUATION

A. Expected Benefits

The framework provides several benefits compared with isolated or static assessment approaches. First, it combines threat modeling with asset dependencies, helping analysts consider the propagation of impact across cyber, physical, and social layers. Second, it connects security requirements to identifiable attack techniques and protected assets. Third, it uses evidence to support iterative changes in risk estimates, which can make the assessment more realistic than a score that remains unchanged after system conditions change.

The use of CIAST also broadens impact analysis. In a smart-grid or transportation environment, a security event may affect not only data and service availability but also operational safety and trust. The MCTS structure helps expose the supporting assets that may be overlooked when attention is limited to the most visible system. RaPDO provides a shared representation for connecting threat knowledge, assets, requirements, and evidence.

B. Case-Study Context

The source study reports theoretical analysis and empirical case studies using representative SmartGrid and SmartTrans scenarios, evaluated by two independent expert groups. It reports statistically significant improvements in comprehensiveness and practicality, with improvement across five evaluation dimensions compared with traditional



risk-assessment approaches. These findings support the potential usefulness of the framework for cross-layer asset identification and evidence-based risk management.

The case-study results should be interpreted within the scope of the reported evaluation. They do not establish that the framework will automatically outperform every existing method in all CPS domains. Outcomes can depend on the quality of scenario information, asset maps, expert criteria, evidence availability, and the operational context. Wider validation is needed before drawing universal conclusions.

C. Limitations

The reviewed framework has limitations. The current ontology and requirements-engineering components are described as conceptual or semi-automated, which may make large deployments difficult. The approach depends on experts to assign mission-specific weights, evaluate criticality, and judge evidence compliance. Poor-quality or outdated evidence can lead to misleading risk estimates. In addition, periodic or event-triggered updates are not the same as continuous real-time automated reasoning.

The method also requires organizations to maintain an accurate inventory of assets and their dependencies. In complex environments, some relationships may be undocumented or may change frequently. The framework's results are therefore only as reliable as the quality of the modeled system, the threat knowledge, and the evidence used during assessment.

D. Future Scope

Future work identified by the source study includes improving ontology reasoning and automated adaptation of security requirements, validating the framework in additional CPS domains such as healthcare and manufacturing, involving larger groups of experts, and incorporating quantitative threat-intelligence measures to improve calibration and interoperability. Automated extraction of evidence and modular deployment may also help scalability, provided that the basis for each risk update remains transparent.

VII. CONCLUSION

This paper has presented an adapted review of a multi-perspective security risk assessment framework for APT attacks in cyber-physical-social environments. The framework links five main elements: APT attack scenarios, the MCTS model, RaPDO, ASRE, and ISRAP. Together, they create a traceable process that connects attacker behavior with cross-layer asset dependencies, adaptive security requirements, implementation evidence, and risk evaluation.

The MCTS model organizes assets into cognitive, information-modeling, and physical layers and captures vertical and horizontal dependencies. CIAST extends traditional CIA analysis by including safety and social trust. RaPDO structures threat and asset knowledge, while ASRE and ISRAP support the iterative refinement of requirements and risk estimates as new evidence becomes available. The reviewed study reports promising results in smart-grid and smart-transportation scenarios, especially for comprehensiveness and practicality.

At the same time, the approach remains dependent on expert judgment, quality evidence, and sufficiently complete asset models. Further automation and broader empirical validation are needed. Overall, the framework offers a useful foundation for organizations seeking to assess APT risks in a way that considers technical, physical, human, and organizational consequences together.

ACKNOWLEDGMENT

This student paper is an adapted summary of the published study by Sihh-Hye Park and Seok-Won Lee. The original authors' ideas and reported findings are acknowledged through the citation below. The content has been reorganized for academic presentation; the original publication remains the primary source for the framework and its evaluation.



REFERENCES

- [1]. S. Singh, P. K. Sharma, S. Y. Moon, D. Moon, and J. H. Park, "A comprehensive study on APT attacks and countermeasures for future networks and communications: Challenges and solutions," *Journal of Supercomputing*, vol. 75, no. 8, pp. 4543–4574, 2019.
- [2]. A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.
- [3]. B. I. D. Messaoud, K. Guennoun, M. Wahbi, and M. Sadik, "Advanced persistent threat: New analysis driven by life cycle phases and their challenges," in *Proc. ACOSIS*, 2016, pp. 1–6.
- [4]. M. Li, W. Huang, Y. Wang, W. Fan, and J. Li, "The study of APT attack stage model," in *Proc. IEEE/ACIS International Conference on Computer and Information Science*, 2016, pp. 1–5.
- [5]. S. Pasandideh, P. Pereira, and L. Gomes, "Cyber-physical-social systems: Taxonomy, challenges, and opportunities," *IEEE Access*, vol. 10, pp. 42404–42419, 2022.
- [6]. P. Cheimonidis and K. Rantos, "A novel proactive and dynamic cyber risk assessment methodology," *Computers & Security*, vol. 154, 2025, Art. no. 104439.
- [7]. The MITRE Corporation, "MITRE ATT&CK," 2021. [Online]. Available: <https://attack.mitre.org/>
- [8]. S. Malviya, A. Fonteles, A. M. Batana, and A. Burch-Dewitt, "Recommending security requirements through asset identification and threat mapping," in *Proc. IEEE International Requirements Engineering Conference*, 2025, pp. 552–560.
- [9]. T. Li, J. Horkoff, K. Beckers, E. Paja, and J. Mylopoulos, "A holistic approach to security attack modeling and analysis," in *Proc. CEUR Workshop*, vol. 1402, 2015.
- [10]. S.-H. Park and S.-W. Lee, "Multi-Perspective Security Risk Assessment for APT Attacks in CPS Environments," *IEEE Access*, vol. 14, 2026, pp. 35790–35814, doi: 10.1109/ACCESS.2026.3670930.

