October 2025
Volume 1
Issue 4

DOI: 10.48308/IJCE.2026.243620.1021

Interdisciplinary Journal of Civil Engineering
Shahid Beheshti University

Risk Analysis of Critical Energy Infrastructure Considering Domino Effects in Petrochemical Complexes in Accordance with API 780

Authors:

Zeynab Askary[1], Mohammad Yaser Radan[1,*], Firouz Ranjbar[1]

Abstract

This research undertakes a comprehensive risk analysis of critical energy infrastructure within petrochemical hubs, paying special attention to the Domino Effects that result from interconnected asset dependencies. The entire framework adheres to the API 780 standard and relevant national energy guidelines. The analysis pinpoints three core, mission-critical power plant components: the turbine, the generator, and the control system. Failure in any one of these can trigger cascading failures across the facility, impacting areas like boilers, power grids, and safety protocols. Threat assessment reveals that hard threats (e.g., military action) and cyber-attacks present the highest likelihood of initiating large-scale domino sequences. Semi-hard threats, such as terrorism, pose a medium-to-high risk to primary generation and control units. While human factors and economic threats may have fewer direct physical consequences, they introduce considerable operational strain. Therefore, the recommended defense strategy centers on substantially bolstering the physical and cyber security around these three pillars. Furthermore, building redundancy into the system architecture is crucial for effective crisis management and breaking the chain of potential domino disruptions.

Keywords: Security Risk Assessment, Critical Energy Infrastructure, Domino Effect, Petrochemical, API 780

1. Faculty of Passive Defense, Malek Ashtar University of Technology, Tehran, Iran

*Corresponding Author: radan@mut.ac.ir

1. Introduction

The rapid advancement of technology, alongside improvements in quality of life, has led to a significant increase in man-made (technological) safety risks. Growing dependence on chemical substances and the expansion of industries such as petrochemicals—which store vast quantities of hazardous materials—have heightened the potential for serious incidents such as chemical leaks. Such events can escalate into major disasters with severe consequences, including loss of life, economic damage, and serious environmental harm (Cvetković et al., 2024). Critical infrastructure in chemical process industries is not only exposed to traditional safety risks such as equipment failure or human error, but, with increasing digitalization, is also vulnerable to cyber–physical security (C2P) threats and intentional attacks. The dynamic and data-driven integration of safety and security management, based on multi-source information, enables the timely identification of changes in risk levels and the optimization of mitigation strategies. This integrated approach not only reduces operational costs, but also enhances the reliability and resilience of critical systems against unforeseen events, ensuring business continuity and protecting personnel, the environment, and capital investments (Shuaiqi Yuan et al., 2025).

Petrochemical facilities, due to the storage and processing of hazardous chemicals, have long been exposed to deliberate attacks and sabotage, as evidenced by drone attacks on Saudi Aramco facilities and acts of sabotage in Libya, both of which resulted in severe economic and security consequences. These events have intensified attention to security considerations within risk management frameworks for this industry, prompting various organizations—particularly in the United States—to develop standardized methodologies such as API 780 for threat assessment and vulnerability analysis. These methodologies include stages such as planning, facility characterization, threat assessment, risk analysis, and identification of countermeasures, among which threat assessment and vulnerability analysis play a critical role (Han Gao et al., 2025). Given the history of catastrophic accidents, substantial human and economic costs, the inherently high-risk nature of the petrochemical industry, increasing project complexity, and the need for effective planning, risk management assessment in this sector represents a vital necessity and a strategic investment for accident prevention, loss reduction, asset protection, and the assurance of sustainable development (Mojtaba Karami et al., 2020).

The domino effect in petrochemical environments refers to the sequential or simultaneous propagation of an initial incident that triggers one or more secondary events, ultimately resulting in consequences far more severe than those of the original event. In such industries, this propagation primarily occurs through escalation vectors, including thermal radiation that heats adjacent equipment and may lead to failure or explosion (such as BLEVE), overpressure

from explosions that damages structures, and projectiles or fragments ejected from the initial explosion site. Consequently, an incident such as the explosion of a storage tank can release energy that spreads to nearby process units, forming a larger chain of cascading accidents (Xu Diao et al., 2025).

Growing concerns regarding the security of critical energy infrastructure and the economic, environmental, and social consequences of intentional incidents have underscored the need to reconsider existing approaches to security risk analysis. Utility units—particularly power generation systems—as the backbone of safe and stable operation in petrochemical complexes, can, if targeted, initiate a chain of disruptions and domino-type accidents. Therefore, conducting research that integrates the API 780 framework with domino effect analysis constitutes a necessary step toward improving the accuracy of risk assessments, enhancing managerial decision-making, and strengthening the resilience of these complexes against sabotage.

As components of critical energy infrastructure, petrochemical complexes face a wide range of hazards due to high concentrations of hazardous materials, strong interdependencies among process units, and the pivotal role of utility units. In this context, intentional and malicious threats may not only disable a single piece of equipment or unit, but can also, through domino effects, lead to the escalation of fires, explosions, and cascading production shutdowns across the entire complex. Despite the development of standards such as API 780 for security risk assessment in the oil, gas, and petrochemical industries, many studies have not comprehensively incorporated domino effects or the critical role of utility units—particularly power generation and distribution systems—into security risk analyses. This gap limits the ability of assessments to accurately reflect the real consequences of intentional threats under the complex operational conditions of petrochemical complexes.

This study seeks to address the fundamental question of how the API 780 standard can be used to comprehensively assess the risk of intentional and sabotage-related threats to power generation utility units in petrochemical complexes while accounting for domino effects. To this end, critical and vulnerable assets within the power generation utility units of one of the country's petrochemical hubs are identified, and the manner in which the consequences of security incidents propagate to other dependent units is examined. In addition, the role of domino effects in amplifying the overall risk level of the complex is evaluated.

Previous studies in this field include the following:

1) Shariatmadari and Nahavandi identified 104 internal and external risks in petrochemical construction projects in Iran (case study: Bakhtar Petrochemical Holding) using document analysis and expert interviews. Their intuition-based evaluation indicated that international

sanctions, inadequate requirement definition, exchange rate fluctuations, infrastructure shortages, and banking financial constraints were the most significant risks (Mohammad Shariatmadari & Nasim Nahavandi, 2020).

2) Gholampour et al. applied the API 780 risk assessment method to analyze the risk of key assets at Amirabad Port against hard man-made threats. The results showed that commercial piers, the access channel, the gas power plant, and hazardous goods warehouses faced the highest risk, and that proposed mitigation measures significantly reduced threat levels (Gholampour et al, 2021).
3) David A. Moore introduced the ANSI/API 780 standard for security risk assessment in the oil and petrochemical industries, demonstrating its systematic approach to identifying and analyzing threats, vulnerabilities, and consequences. The study concluded that this method supports managers in selecting cost-effective countermeasures and effectively managing residual risks through risk-based performance criteria (David A. Moore, 2013).
4) Sadeghi et al. employed the Security Vulnerability Assessment (SVA) method and showed that thermal power plants, as strategic infrastructure, are vulnerable to intentional physical and cyber threats. Assets such as diesel storage tanks and industrial buildings were found to have the highest physical risk due to fuel volume and location, while turbine control systems and IT infrastructure were highly vulnerable to cyberattacks. Realization of these threats could lead to widespread energy disruptions, economic losses, and environmental consequences, necessitating simultaneous implementation of measures such as hardening, concealment, and enhanced cyber security (Abbas Sadeghi et al., 2017).
5) Marroni et al. proposed an interdisciplinary approach for the integrated assessment of safety and security in process facilities in the Maghreb region, combining qualitative analysis with quantitative simulation using UniSim. Their findings indicate that the region's specific geopolitical conditions increase the likelihood of intentional attacks and highlight the need to strengthen physical protection systems and integrate safety and security considerations (Giulia Marroni et al., 2022).

Varadharajan and Bajpai reviewed the evolution of security risk assessment methods in process industries, presenting a systematic review and comparative analysis of deterministic approaches (such as SVA, API 780, and RAMCAP) and dynamic probabilistic methods (including Bayesian networks, Petri nets, and game theory). Their conclusions suggest that while deterministic methods have been useful in early stages, dynamic approaches offer greater reliability due to their ability to model uncertainty and evolving threat behavior. The development of security incident databases and the integration of human and environmental factors into risk assessment are identified as key future needs in this field (Surendar Varadharajan & Shailendra Bajpai, 2023).

2. Materials and Methods

The case study of this research focuses on the utility unit of one of the country's major petrochemical hubs. The research methodology is based on the security risk assessment framework of the API 780 standard and adopts the Security Vulnerability Assessment (SVA) approach to analyze intentional threats and domino effects in critical energy infrastructure.

First, the critical assets of the power generation utility unit within the selected petrochemical hub were identified, and their level of importance was determined based on their functional role and the consequences of potential failure. Next, potential human-induced threats—including physical sabotage, targeted attacks, and unauthorized access—were defined in accordance with the threat classification provided in API 780 and the guidelines issued by the National Iranian Gas Company.

Subsequently, asset vulnerabilities were assessed by considering design characteristics, safety distances, physical protection measures, and the level of attacker accessibility. In the consequence analysis phase, in addition to the direct impacts of incidents, the propagation of accidents in the form of domino effects—such as fires, explosions, and cascading shutdowns of dependent units—was also examined.

Finally, the security risk level of each scenario was calculated as a function of threat, vulnerability, and consequences, and the identified risks were prioritized accordingly.

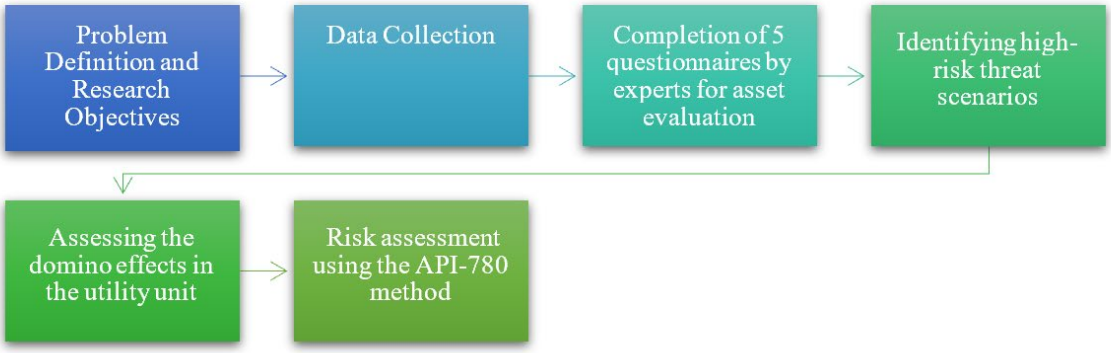

Figure 1. Research method diagram

3. Results and Discussion

Modern warfare, the destruction of critical infrastructure—particularly oil and gas networks—has become a top priority among offensive objectives. This is because such infrastructures play vital economic, social, political, and defensive roles under normal conditions, during crises, and in post-crisis periods. Countries possess a wide range of critical infrastructures, including oil and gas pipelines, power grids, transportation systems, telecommunications networks, water supply systems, and key buildings. Disruption of oil and gas networks, as demonstrated during the 2022 Russia–Ukraine war, can result in extensive financial and political damage. Consequently, planning for operational continuity and reducing the vulnerability of these networks is essential. Achieving this goal requires vulnerability analysis and the identification of high-risk points, which is considered one of the most important risk assessment approaches for oil and gas networks and other critical infrastructures (Seyed Ehsan Abtahi, Reza Kelaher, Davood Seddaghat Shayegan, 2022). Accordingly, this study employs the API-780 methodology, as issued by the National Iranian Gas Company, which shows better compatibility with oil and gas infrastructures, to calculate a localized risk index.

The security vulnerability of petrochemical infrastructure is analyzed through a systematic five-step process known as Security Vulnerability Assessment (SVA). This process includes: (1) identification of critical assets (such as facilities, hazardous materials, control systems, and critical infrastructure), (2) threat assessment (including terrorism and internal and external sabotage), (3) vulnerability analysis (physical, cyber, and operational weaknesses), (4) risk assessment (combining the likelihood and consequences of a successful attack), and (5) development of countermeasures (such as deterrence, detection, delay, and response). This methodology was developed through collaboration between API and NPRA and focuses on risk management, protection of personnel, the environment, the national economy, and the continuity of industrial operations (American Petroleum Institute & National Petrochemical, 2004).

The vulnerability of petrochemical infrastructure, as part of the energy system, is defined as the degree to which these facilities are susceptible to damage, destruction, or disruption resulting from various threats—natural, physical, cyber, or technological. Such vulnerability may arise from internal system weaknesses (such as poor design or aging equipment) or from critical dependencies on supporting systems (including electricity, water, transportation, or human resources), which, if affected by a threat, can disrupt petrochemical operations. Vulnerability assessments also take into account recovery time and the availability of resources required to restore damage (U.S. Department of Energy, 2024). As a component of the energy sector (oil and gas subsector), petrochemical infrastructures face serious cyber and physical threats. Cyberattacks can target industrial control systems (ICS) and monitoring systems used

in refineries, leading to disruptions in critical processes, explosions, or widespread damage. Physical attacks, such as sabotage or bombings, may also be carried out by extremist groups or disgruntled employees, posing significant risks to safety and operational continuity. Due to their critical role in the energy supply chain and the economy, these facilities represent attractive targets for both state and non-state malicious actors (Bridget R. Kane et al., 2024).

Domino effects refer to cascading and escalating events in which an initial incident (such as a fire) in a unit or storage tank spreads to neighboring units or tanks due to aggravating factors such as thermal radiation, blast waves, or the release of hazardous materials. This leads to an expansion of the incident's scope and an increase in the severity of its consequences. Although such events have a relatively low probability of occurrence, their consequences can be extremely severe, making them one of the primary concerns in process industries such as oil and gas refineries. Effective management of domino effects requires the identification of critical points, vulnerability analysis, and the development of robust preventive and responsive strategies (Maryam Ghaljahi et al., 2024). Statistical analyses indicate that the highest frequency of domino accidents occurred during the periods 1971–1980 and 1981–1990, coinciding with the expansion of the chemical industry and the increase in the number and capacity of process facilities. Geographically, most of these incidents were reported in developed countries; however, trends in the twenty-first century show a relative decline in such countries and a significant increase in developing nations, highlighting the growing need for enhanced safety measures in these regions. In terms of origin, approximately 75% of incidents occurred in fixed facilities (process and storage units), while 25% were associated with transportation and loading/unloading operations. Mechanical failure was identified as the primary cause, followed by human error and external events as major contributors to domino accident chains (Jun Wu et al., 2015).

The utility unit is a critical and infrastructural component of an industrial complex, responsible for providing the essential services required for the operation of core production processes. In petrochemical industries, this unit functions as the beating heart of the facility by supplying steam for heating and chemical reactions, cooling water for temperature control of equipment, compressed air for instrumentation and control, and industrial gases such as nitrogen to create inert atmospheres. Without this unit, the main production processes come to a halt (Utility Unit, 2025). Auxiliary and utility services are considered the operational backbone of the petrochemical industry and are as vital as a circulatory system; without them, even the most advanced production units cannot continue operating. Supplying water through advanced desalination systems, cooling towers, and treatment plants; generating and distributing highly reliable electricity; managing steam systems at various pressure levels; and ensuring a stable supply of critical gases such as compressed air and nitrogen are among the complex challenges in this field. Additionally, wastewater treatment systems, waste management, extensive

distribution networks, and security and firefighting systems are integral components of these services (Mahmoudi, 2024).

The power and steam unit (sometimes referred to as the power and steam utility unit) is a facility that simultaneously generates electricity and steam (heat) to support petrochemical operations. Electricity is used for motors, pumps, control equipment, lighting, and other applications, while steam is utilized for heating, distillation processes, reboilers, chemical reactions, feed preheating, and related operations.

Risk assessment using the API 780 method is a standardized, team-oriented process designed to identify, analyze, and prioritize security risks in the oil and petrochemical industries. This method follows five main steps: describing the facilities, assessing threats, evaluating vulnerabilities, analyzing risks, and providing countermeasures. By combining factors such as threats, target attractiveness, vulnerabilities, and potential consequences, it aids management in making informed decisions to mitigate security risks including sabotage, theft, and terrorism (American Petroleum Institute (API), 2013). The operational basis of this study in risk assessment is the guidelines for identifying and assessing security risks set by the National Iranian Gas Company, which is formulated based on the international API 780 standard.

Step One (Identifying Assets): Asset evaluation is performed as a comparative assessment, irrespective of the type and nature of the threat, using five sub-indices that are determined and weighted accordingly. Based on the scoring guidelines provided in the National Iranian Gas Company's security risk assessment protocol, the asset evaluation table is completed. Five asset evaluation questionnaires were filled out. To facilitate the review and assessment process, the assets were categorized into seven distinct units: gas turbine unit, generator unit, boiler unit, control unit, electrical distribution unit, safety unit, and support unit.

Step Two (Contrasting Threats and Assets to Develop Scenarios): In this step, potential scenarios are developed by juxtaposing threats with assets. A list of probable identified threats is first compiled, and scenarios are created based on the interaction between assets and threats to determine risk. All units, including the gas turbine, generator, boiler, control, electrical distribution, safety, and support units, have their threats categorized into four main groups: hard (ground-based, air-based, and space-based), semi-hard or terror-related (including man-portable missiles, briefcases, vehicles, and drone bombs, as well as assassination or hostage-taking), technology-based (including electromagnetic bombs, graphite bombs, chemical, bioterrorism, radiation, and cyber threats), and people-centered (sabotage, riots and strikes, economic sanctions). The units are largely exposed to similar threats, although some units, such as the boiler, are more limited to technology-based and terror-related threats, while the safety unit encompasses all options except for man-portable missiles.

Step Three (Estimating Vulnerability): In this step, the vulnerability status of the facilities against each of the threats is assessed based on the existing defensive layers and evaluated according to their qualities.

Evaluating the Status of Defensive Layers (LOP): According to the scoring guidelines provided in the National Iranian Gas Company's security risk assessment protocol, the status table of the defensive layers of the energy supply unit, which is one of the hubs of the petrochemical sector, is completed.

Calculating Success Probability (Parameter L2):

First Stage: Determining the effectiveness of sub-indices of defensive layers against each of the threats: Each component of the defensive layers does not impact all threats equally and does not lead to a reduction in their success probability. The desired effectiveness is assessed and established as a zero-one matrix (present/not present).

Second Stage: Calculating the failure probability in each of the defensive layers: Given the effectiveness status of each of the defensive layer sub-indices (from the previous stage), the failure probability of each layer needs to be calculated. For this purpose, the success probability for each of the developed scenarios must be obtained. The average scores assigned to the sub-indices of each layer will be equivalent to the success probability, and the failure probability for each layer is derived by subtracting this from one.

Third Stage: Calculating success probability (L2) differentiated by various intensities of incidents: Considering the different combinations of success or failure for each of the defensive layers, various intensities of a potential incident may arise. These varying intensities are generated based on the success (Safe) or failure (Fail) of each of the six layers, leading to twelve distinct states ranging from no occurrence to disaster. Accordingly, after determining the failure and success probabilities of each of the defensive layers for each scenario, the success probability of each layer (conditions that follow the green line) is calculated by subtracting the failure probability from one.

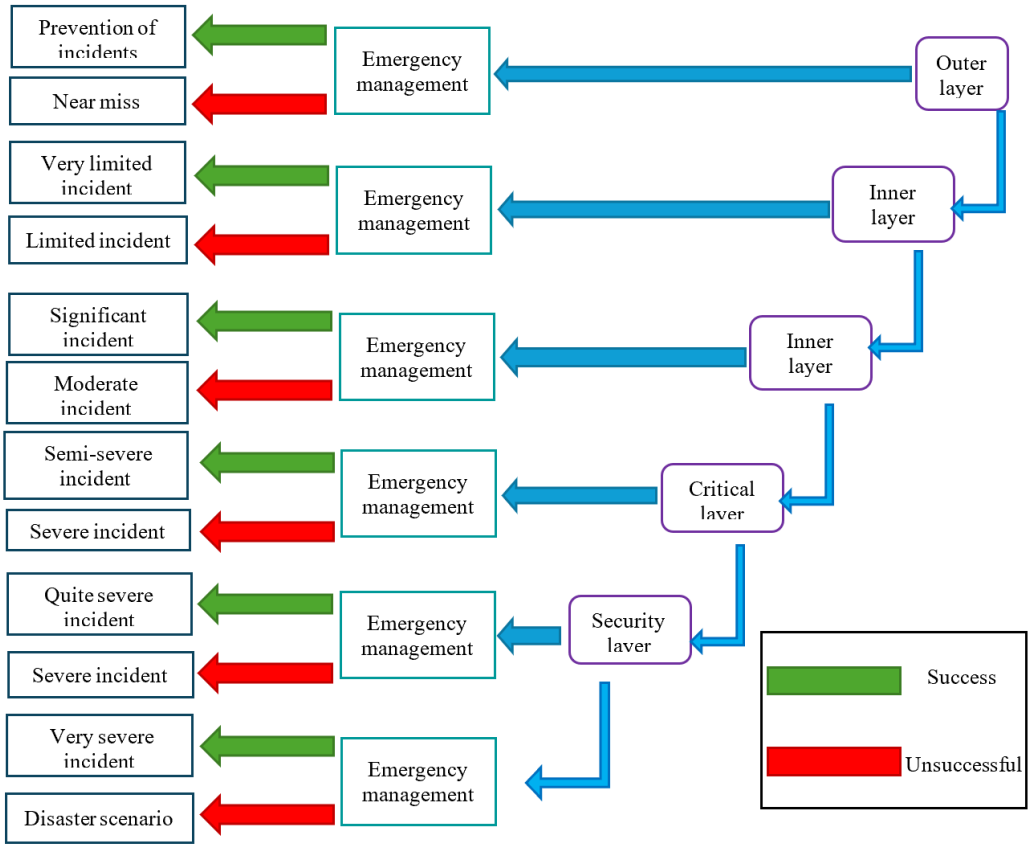

Figure 2. Event tree diagram for various outcomes during an accident

Step Four (Determining the Threat Number (T)): In the studied dataset, the occurrence of offensive threats is identified as a crisis-inducing incident, with the risk level of each threat being dependent on one or more parameters. According to the guidelines provided in the risk identification and assessment protocol of the National Iranian Gas Company, the threat index table is completed.

Step Five (Determining the Attractiveness Index Score (A)): The attractiveness of an asset is defined as a measure to evaluate the likelihood of threats occurring. Following the scoring guidelines from the National Iranian Gas Company's security risk assessment protocol, the attractiveness index table is filled out.

Step Six (Determining the Occurrence Probability Parameter (L1)): The occurrence probability parameter (L1) is calculated from the combination of scores obtained for the attractiveness index (A) and the threat index (T). The calculated occurrence probability (L1) for each scenario is derived from the multiplication of the corresponding threat and attractiveness values, and will be computed for each scenario.

Step Seven (Determining the Probability Parameter (L)): The probability parameter (L) is derived from the combination of occurrence probability and success probability. Given the independence of the probability scores, the parameter (L1) is the product of the occurrence probability (L2) and the success probability (L). Since the success probability parameter (L1) has been calculated as an array of twelve elements, there is no need to calculate the parameter L for all incident states (ranging from non-occurrence to disaster). Since the goal of risk assessment is to determine the adequacy and quality of all defensive layers, the disaster scenario (complete failure of all layers) is considered the worst-case scenario and will serve as the basis for risk calculations. Therefore, the combination of parameters L1 and L2 will only be relevant for measuring success probability under disaster conditions.

Step Eight (Determining the Consequence Parameter of Occurrence (C_T)): To conduct a more comprehensive and realistic risk assessment in the utility unit, especially when employing the API 780 method, the consequence analysis must go beyond direct outcomes and also consider extensive chain effects. Accordingly, in the consequence analysis stage, the overall consequence is divided into two separate components: the initial direct consequence C_API (which is calculated based on the standard API 780 model and the estimated losses from the initial failure, such as equipment damage or direct production stoppage) and the domino or secondary consequence C_Domino. This domino consequence reflects secondary impacts that occur due to systemic interdependencies (e.g., loss of electrical or steam supply by the utility unit) on other sectors of the petrochemical complex. Ultimately, the total consequence is defined as a combination of these two components. The following formula expresses this relationship:

$$C_T = C_{API} \times C_{Domino}$$

Initial Direct Consequence: The initial consequence parameter (C_API) for each scenario will be assessed based on the characteristics of the threat, the nature of the asset, the outcomes of consequence modeling, and the functional role of that asset within the system. It is important to note that this parameter will be used under worst-case conditions, that is in the disaster scenario (complete success of the threat and failure of all defensive layers).

As mentioned, the domino effect refers to conditions where a failure or incident in a single utility asset increases the likelihood or severity of consequences from failures in other dependent assets or units.

In this study, the domino effect is incorporated into the risk assessment by expanding the consequence analysis in accordance with the API 780 standard. In addition to direct consequences, secondary impacts arising from interdependencies between the utility units generating electricity are also considered. The overall logic of domino effect analysis in

petrochemical power plants is based on the premise that assets are interconnected in a series-parallel structure; such that the failure of one asset can either increase the consequences of failure in other assets or lead to a chain reaction of failures throughout the entire energy and safety network of the complex. This domino effect is determined based on three key criteria: dependency intensity (Functional Dependency), redundancy or alternative capacities (Redundancy), and unit sensitivity. The asset dependency matrix of the electricity utility serves as a structured tool for modeling and visualizing the relationships between various components of the system, playing a central role in domino effect analysis. This matrix is typically designed as a square table, listing the main assets of the power plant (such as power generation units, processing units, safety systems, and critical equipment) in its rows and columns. Each cell in this matrix indicates the type and intensity of dependency of one asset on another; if a failure in the row asset causes a failure or disruption in the operation of the column asset, a dependency relationship is recorded. By establishing these relationships, risk transmission pathways (domino chains) can be identified, leading to a clearer understanding of how an initial defect can result in widespread consequences across the entire complex.

Table 1. Asset Dependencies in the Petrochemical Power Generation Utility Unit

Asset	Dependent Asset	Dependency Types	Domino Effect Level	Explanation of the effect
Gas Turbine	Generator	Functional	Severe	Loss or Stoppage of Mechanical Power, Power Generation Interruption
Gas Turbine	Boiler	Process	Moderate	Disruption of Auxiliary Steam/Heat Supply
Gas Turbine	Power Distribution	Energy	Severe	Reduction in Internal Grid Capacity
Generator	Power Distribution	Energy	Severe	Shutdown of Process Units
Generator	Control Unit	Control	Moderate	Loss of Signals and Monitoring
Boiler	Gas Turbine	Thermal Support	Moderate	Efficiency Drop or Turbine Trip
Boiler	Process Units	Process	Severe	Process Stoppage or Instability
Control Unit	Gas Turbine	Control	Severe	Sudden Turbine Trip
Control Unit	Generator	Control	Severe	Emergency System Disconnection/Outage
Control Unit	Power Distribution	Control	Moderate	Load Management Failure
Power Distribution	Process Units	Energy	Critical	Complex-wide Chain Reaction Shutdown
Power Distribution	Safety Unit	Energy	Critical	Deactivation of Safety Systems
Safety Unit	Complete System	Safety	Critical	Increased Probability of Secondary Incidents
Support Unit	Generator/Gas Turbine	Maintenance	Moderate	Increased Failure Rate
Support Unit	Safety Unit	Operational	Moderate	Diminished Emergency Response Capability

Gas Turbine Unit: The failure of the gas turbine directly leads to the cessation of mechanical power production and the generator being taken offline. This initial disruption reduces the capacity of the power distribution system and, in the absence of adequate redundancy, results in the shutdown of process units. The continuation of these outages affects safety systems reliant on electricity, creating a domino effect across the entire complex, thereby escalating the consequences from major to severe levels.

Generator Unit: The breakdown of the generator results in the loss of generated electricity and its transmission to the internal grid. This situation dominoes into the shutdown of process units, disruptions in control systems, and a diminished capacity to monitor operational conditions. In critical scenarios, this disruption can trigger the activation of safety systems and ultimately lead to a complete shutdown of the complex.

Boiler Unit: A boiler failure is a primary cause of reduced or halted steam and heat supply necessary for processes. This can disrupt the stability of the gas turbine's operation and increase the likelihood of an emergency shutdown (Trip). The domino effect of the boiler mainly manifests by affecting the operational stability of other units, leading to significant indirect consequences, particularly in continuous operation processes.

Control Unit: As the central core of the system, a failure in the control unit leads to the loss of command, monitoring, and protection capabilities. This malfunction typically causes simultaneous Tripping of the turbine, generator, and disruption in the load management of the power grid. The domino effect resulting from the failure of this unit is very rapid and extensive, to the extent that the associated risk is classified at the highest level as "unacceptable."

Power Distribution Unit: Disruptions in the power distribution system pave the way for chain outages in dependent units, including process units and safety systems. This asset plays a vital role in transmitting domino effects and is regarded as one of the essential critical points in the overall system structure, leading to a critical risk with the potential for widespread incidents.

Safety Unit: The failure of the safety unit, even in the absence of failures in other equipment, significantly increases the potential consequences of incidents. If a safety failure coincides with a power outage or a simultaneous control failure, the likelihood of fires, explosions, or the release of hazardous materials rises significantly.

Support Unit: Decreased efficiency in support units (including maintenance, spare parts provision, and specialized personnel) directly increases the failure rate of key equipment and weakens the system's recovery capability. The domino effect of this unit usually appears with a time delay, leading to a heightened likelihood of secondary failures in the long term.

Step Nine (Determining Risk): After determining the likelihood (L) and consequence scores for each scenario, the risk parameter is calculated based on the combination of likelihood and consequence. According to the API-780 method, a matrix is used to combine these two parameters and arrive at a risk number.

Table 2. Division of the Risk Number and its Match with Risk Exposure Levels

		Probability				
		5	4	3	2	1
consequence	5	5	5	4	4	3
	4	5	4	4	3	2
	3	4	4	3	2	2
	2	4	3	2	2	1
	1	3	2	2	1	1

Table 3. Risk Number Assignment for Assets within the Energy Supply Unit of a National Petrochemical Hub

Row	Threat Category		Gas Turbine Unit Risk Score	Generator Unit Risk Score	Boiler Unit Risk Score	Control Unit Risk Score	Power Distribution Unit Risk Score	Safety Unit Risk Score	Support Unit Risk Score
1	Hard Threats	Ground-based	4	4	4	4	4	3	2
2		Air-based	5	5	5	4	4	4	4
3		Space-based	4	4	4	4	4	3	3
4	Terroristic Threats	Shoulder-fired Weapons	4	4	4	3	3	2	2
5		Explosive-laden Briefcase	3	3	2	2	2	1	1
6		Car Bomb	4	4	3	3	3	3	2
7		Drone Bomb	4	4	4	4	4	3	3
8		Assassination and Kidnapping	1	2	Non-Inclusion	2	2	2	2
9	Technology-based Threats	Non-Inclusion	Non-Inclusion	Non-Inclusion	Non-Inclusion	4	Non-Inclusion	Non-Inclusion	Non-Inclusion
10		Electromagnetic Bombs	4	4	3	4	4	3	2
11		Chemical Weapons	2	2	Non-Inclusion	2	2	2	2
12		Bioterrorism	2	2	Non-Inclusion	2	2	1	2
13		Radiological Threats	3	3	Non-Inclusion	3	3	2	3
14		Cyber Threats	4	4	4	4	4	4	4
15	People-centric Threats	Sabotage	3	3	4	2	2	1	2
16		Rioting and Strikes	2	2	Non-Inclusion	2	2	2	2
17		Economic Sanctions	4	4	4	4	4	3	3

It should be noted that in cases specified in the “Non-Inclusion” it means that the mentioned threat is not defined for this asset and has not been considered in the relevant scenario.

The analysis of threats against power plants can be classified into five main categories, each affecting critical units with varying intensities. In the category of hard threats (military), which includes ground, aerial, and space attacks, the highest risk corresponds to aerial attacks (risk 5) that directly target the turbine and generator. Damage to these units creates a domino effect:

the stoppage of the turbine leads to a decrease in mechanical production, reduced generator capacity, disruption in the boiler and control systems, ultimately resulting in diminished distributed power and jeopardizing safety systems; hence, designing resilience against physical attacks for these sectors is crucial.

The second category, semi-hard terrorist threats such as handheld rocket launchers, drones, and vehicle bombs, poses medium to high risk (2 to 4) for key units. Here again, the turbine, generator, and boiler are constantly exposed to chain effects; for instance, an explosion from a vehicle bomb near the turbine can indirectly lead to the shutdown of the generator and boiler, subsequently disrupting power distribution and safety. Human threats like hostage-taking carry less risk but can disrupt the normal operation and emergency response of the plant. Technology-based threats include EMI, graphite bombs, chemical agents, bioterrorism, and cyber-attacks. Among these, cyber threats (risk 4 across all units) gain the highest significance, as damage to the control and automation systems of the plant can have a severe domino effect on all components: disruptions in control, malfunction of turbine and generator operations, disruptions in boiler and distribution, and compromising safety systems. Other technological threats focus more on control and power distribution units.

The fourth category includes people-oriented and economic threats such as sabotage, unrest, and economic sanctions. These have less direct impact on physical equipment, but by disrupting the supply of materials, fuel, and human resources, they can create domino effects on the turbine, generator, and boiler. Economic sanctions, with a risk rating of 4, demonstrate that even indirect threats can pose serious challenges to the performance of the entire power plant.

The turbine, generator, and control systems, as the main points of energy production and management, are the most critical units with the most severe domino effects. In contrast, the boiler and power distribution are relatively vulnerable. To mitigate these chain risks, a comprehensive design of physical, cyber, and operational protective protocols, along with creating redundancy in equipment and defining emergency response scenarios, is necessary.

4. Conclusion

With technological advancements and increasing dependency on industries such as petrochemicals, human-made safety and security hazards have also risen. These industries, storing vast amounts of hazardous materials, are not only susceptible to traditional incidents but also face cyber-physical threats and intentional attacks (such as sabotage) due to digitization. Given the critical role of petrochemical industries in the national economy and the strategic position of facilities like one of the country's petrochemical hubs, a systematic assessment of security risks based on standards such as API 780 is essential. The main goal of

this research is to identify and evaluate security risks (both physical and cyber) and weaknesses in the critical infrastructure of one of the country's petrochemical hubs to help enhance national energy security.

The API 780 method is a standardized, team-oriented process for assessing security risks in the oil and petrochemical industries. This method includes key steps such as facility description, threat assessment, vulnerability evaluation, risk analysis, and proposing mitigation strategies. In this research, the assets of the utility unit of one of the country's petrochemical hubs were first identified and classified into seven units (gas turbine, generator, boiler, control, power distribution, safety, and support). Next, potential threats were defined in four main categories (hard/military, semi-hard/terrorist, technology-based, and people-oriented), and confrontation scenarios for these threats with assets were developed. The vulnerability of the facilities was assessed based on 20 sub-indicators through various defensive layers (such as military systems, fencing, cameras, control systems, and firefighting systems).

By calculating the likelihood of threat occurrence and the success probability of defensive layers, the domino consequences for each asset against each threat were obtained. Based on the threat assessments, the turbine, generator, and control system were identified as the critical units of the plant; damage to any of these main components could impose a series of domino effects on other sections, including the boiler, power distribution, and safety unit, disrupting the overall plant performance. The severity of these threats varies, with hard (military) threats and cyber-attacks posing the highest risk and the broadest domino effects across all units. Conversely, semi-hard terrorist threats impose a medium to high risk on production and control units, while people-oriented and economic threats, though having less direct impact on physical equipment, exert significant pressure on plant performance through disruptions in resource supply and operational processes. The domino effect of risks is a fundamental principle in this analysis; even threats that seem to be focused only on one unit (such as a direct attack on the turbine) can significantly impact the performance of other critical assets due to internal chain dependencies. Therefore, the primary priority should be the protection of core infrastructure, namely the turbine, generator, and control system.

Effective countermeasures should include designing and deploying enhanced physical and cyber protective systems for these units, creating redundancy and emergency support to mitigate potential damages, and focusing on continuous monitoring and control to facilitate early identification of threats and prevent the spread of their adverse effects. The final summary indicates that the main vulnerability of the power plant lies against hard and technology-based threats, and maintaining overall functionality requires special attention to the protection of the three main pillars of energy production and management.

5. References

Abtahi, S. E., Kalehr, R., & Sadeghat Shaygan, D. (1401). Risk assessment and management of oil and gas infrastructures in border provinces to reduce threat impacts. *Farazdno Journal, 17*(77), 70–90.

American Petroleum Institute. (2013). *ANSI/API Standard 780: Security risk assessment methodology for the petroleum and petrochemical industries*.

American Petroleum Institute. (2025). *About API*. https://www.api.org/about

American Petroleum Institute & National Petrochemical Association. (2004). *Security vulnerability assessment methodology for the petroleum and petrochemical industries* (2nd ed.).

Cvetković, V. M., Renner, R., & Jakovljević, V. (2024). Industrial disasters and hazards: From causes to consequences—A holistic approach to resilience. *International Journal of Disaster Risk Management, 6*(2).

Diao, X., Jiang, J., Mebarki, A., Ni, L., Duo, Y., Chen, S., Wang, Y., & Zhang, S. (2025). Risk analysis of domino effect of leakage accident of petrochemical pipeline based on analytic hierarchy process and fuzzy fault tree analysis. *Safety Science, 187*.

Gao, H., Shi, H., Yang, Y., & Han, K. (2025). Vulnerability assessment of petrochemical facilities impacted by bomb fragments: A simplified methodology using machine learning. *Process Safety and Environmental Protection, 2000*.

Ghaljahi, M., Omidi, L., & Karimi, A. (2024). Evaluation of domino effects and vulnerability analysis of oil product storage tanks using graph theory and Bayesian networks in a process industry. *Journal of Health and Safety at Work, 14*(4), 736–755.

Gholampour, H., Alvani, S. S., & Fallah, M. (1401). Assessment and risk analysis of vital arteries with a focus on passive defense (case study: Amirabad Port). *Scientific Journal of Safe City*.

Kane, B. R., Webber, S., Tucker, K. H., Wallace, S., Chang, J., McCarthy, D., Murphy, D., Egel, D., & Wingfield, T. (2024). *Threats to critical infrastructure: A survey*.

Karami, M., Samimi, A., & Ja'fari, M. (2020). The necessity of risk management evaluations in petrochemical industries. *Advanced Journal of Chemistry Section B*, 151–158.

Mahmoudi, H. (1403). *Comprehensive analysis of ancillary services and utilities*. http://hanimahmoodi.com/blog/utilities-&-services-analysis

Marroni, G., Piemonte, A., Tamburini, F., Caroti, G., Pannocchia, G., & Landucci, G. (2022). An interdisciplinary approach towards the integrated safety security assessment of process facilities operating in the Maghreb context. *Chemical Engineering Transactions, 91*.

Moore, D. A. (2013). Security risk assessment methodology for the petroleum and petrochemical industries. *Journal of Loss Prevention in the Process Industries, 26*, 1685–1689.

Negin Makran Petrochemical Development. (1404). *Provision of ancillary services*. http://mokran.ir/tyility

Sadeghi, A., Jabbari, M., Alidoosti, A., & Rezaeian, M. (2017). Vulnerability and security risk assessment of a thermal power plant using SVA technique. *Journal of Integrated Security Science*.

Shariatmadari, M., & Nahavandi, N. (1399). Identification and risk assessment in petrochemical construction projects in Iran: Case study Bakhtar Petrochemical Holding. *Scientific-Research Journal of Structural Engineering and Construction, 7*(Special Issue 2), 101–123.

U.S. Department of Energy. (2024). *Risk assessment essentials for state energy security plans*.

Utilities Unit. (1404). *Summary*. Farajad Development Company. http://tfarjadco.com/utility-unit

Varadharajan, S., & Bajpai, S. (2023). Chronicles of security risk assessment in process industries: Past, present, and future perspectives. *Journal of Loss Prevention in the Process Industries, 84*.

Wu, J., Yang, H., & Cheng, Y. (2015). Domino effect analysis, assessment, and prevention in process industries. *Journal of Systems Science and Information*.

Yuan, S., Reniers, G., & Yang, M. (2025). Dynamic and integrated safety and security barrier management: A new framework to manage major event risks in chemical plants. *Journal of Loss Prevention in the Process Industries, 96*.