# RISK ASSESSMENT OF PIPELINE ON THIRD-PARTY DAMAGE IN OIL AND GAS INDUSTRY WITH BAYESIAN NETWORK AND GAME THEORY

A Thesis

by

YAN CUI

Submitted to the Office of Graduate and Professional Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

| | |
|---|---|
| Chair of Committee, | Chad V. Mashuga |
| Committee Members, | Mahmoud M. El-Halwagi |
| | Eric L. Petersen |
| Head of Department, | M. Nazmul Karim |

May 2017

Major Subject: Safety Engineering

# ABSTRACT

Tremendous amount of oil and gas products are transported in pipeline worldwide giving rise to a demand to identify the hazards and evaluate the associated risk. Third-party intrusion is usually one of the least factors being considered during the pipeline hazard assessment stage despite the substantial portion contributing to the total number of oil and gas pipeline incident. This is because of the probabilistic risk assessment defect that makes it hard to model human actions and cannot be applied to intentional acts. Due to the distinctive motivations of third-party damage, an unintentional third-party damage Bayesian Network model and a game-theoretic model on malicious intrusion will therefore be built, respectively to examine the mechanism of pipeline failure caused by this mode.

This study is conducted aiming at investigating pipeline risk resulting from third-party damage, and will formulate risk assessment models to identify threats, prioritize risks and determine which integrity plan should apply to different pipeline segments given the condition of third-party interference (both the accidental damage and malicious acts). In other words, it can help to anticipate an optimal planning of the in-line inspection intervals which can decrease the risk of the pipeline to an acceptable level and achieve cost-effective pipeline integrity management.

# DEDICATION

This thesis is dedicated to

my uncle,

Zhigang Cui

# ACKNOWLEDGEMENTS

I would like to express my sincere appreciation to my advisor Dr. Chad V. Mashuga for giving me the opportunity to study in his research group, and his support throughout my master’s graduate life.

I would also like to thank my committee members, Dr. Mahmoud M. El-Halwagi, Dr. Eric L. Petersen for their guidance and contributions throughout the course of this research.

Thanks also go to my parents for their patience, love and financial support, my boyfriend for the encouragement, and colleagues as well as the department faculty and staff for making my time at Texas A&M University a great experience.

# CONTRIBUTORS AND FUNDING SOURCES

## Contributors

This work was supervised by a thesis committee consisting of Professor Chad V. Mashuga, Professor Mahmoud M. El-Halwagi of the Department of Chemical Engineering and Professor Eric L. Petersen of the Department of Mechanical Engineering.

All work for the thesis was completed independently by the student.

## Funding Sources

There are no outside funding contributions to acknowledge related to the research and compilation of this document.

# NOMENCLATURE

| | |
|---|---|
| AHP | Analytic Hierarchy Process |
| ALARP | As Low As Reasonably Possible |
| BN | Bayesian Network |
| DHS | Department of Homeland Security |
| DOT | Department of Transportation |
| EGIG | European Gas Pipeline Incident Data Group |
| GIS | Geographic Information System |
| HCA | High Consequence Area |
| IM | Integrity Management |
| IR | Individual Risk |
| JSA | Job Safety Analysis |
| MOC | Management of Change |
| NGL | Natural Gas Liquid |
| OPS | Office of Pipeline Safety |
| PHMSA | Pipeline and Hazardous Materials Safety Administration |
| QRA | Quantitative Risk Assessment |
| ROW | Right-of-way |
| SOM | Self-Organizing Maps |
| SR | Societal Risk |
| TSA | Transportation Security Administration |

TABLE OF CONTENTS

# LIST OF FIGURES

Page

# LIST OF TABLES

# 1. INTRODUCTION

## 1.1 Background

Within the energy industry, the primary marketing distribution of products include a multitude of forms such as crude oil, lease condensate, natural gas plant liquids, dry natural gas, coal, hydroelectric, nuclear, geothermal, solar, wind, wood and waste electric power that increased from 245 quadrillion BTU in 1973 to 518 BTU in 2011 with approximate 2 percent annual growth rate [2]. In the entire energy world, oil and gas industry is so tangible that has significant impact on our lives in many ways. More than sixty percent of energy in U.S. was supplied by oil or natural gas, which fuel vehicles and planes, heat the residential houses and provide raw materials to fine chemicals (downstream) industry by the process like cracking. The production of crude oil in U.S. had a dramatic growth in the period of 1920's to 1980's while the boom of natural gas started decades later in 1950's and a second boom occurred in the past three decades as shown in the Figure 1 and 2 [3]. The high demand and consumption of oil and gas reveals its important status in economics and business. Thus, the maintenance of this industry in the current configuration becomes a vital issue for many nations.

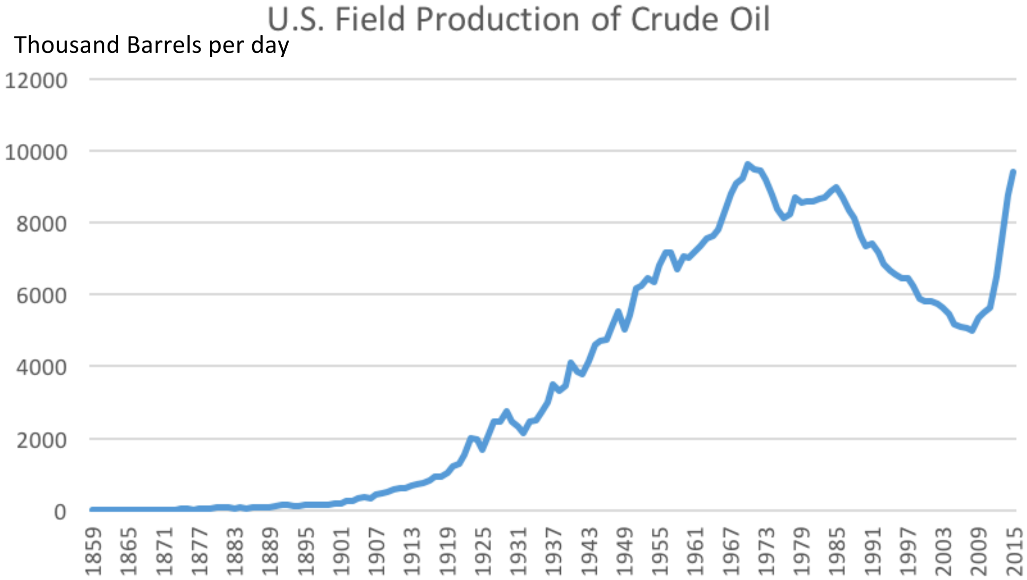


**Figure 1. U.S. Field Production of Crude Oil (source: U.S. Energy Administration)[3].**

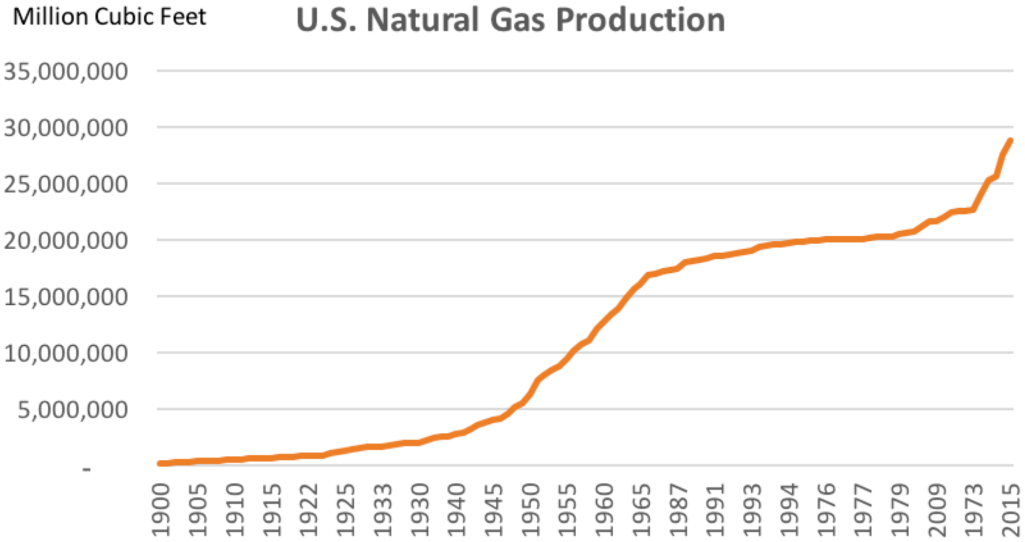


**Figure 2. U.S. Natural Gas Production (source: U.S. Energy Administration)[4].**

One of the essential elements composed of oil and gas industry is the pipeline system. Tremendous pipelines across the country had built a vast and efficient network in natural gas transportation with regards to three different working functions: gathering, distribution and transmission. The first two types of pipelines represent the beginning and the end of gas supply chain system. Like the vessels that transport the blood throughout human body, pipelines connect oil fields both onshore and offshore to refineries and petrochemical facilities carrying oil and gas feedstocks, and deliver these products to consumers and businesses over the country. This massive oil and gas delivering network consists of more than 200,000 miles of liquid petroleum pipelines and over 2,500,000 miles of natural gas pipeline in U.S. reported by Pipeline and Hazardous Materials Safety Administration (PHMSA) [5]. As shown in Table 1 and 2, both liquid and gas pipelines have a stable increase in number of pipeline length during the recent five years, indicating a steady development and promising future in using pipeline.

Compared with other transportation methods such as train or highway to deliver hazardous materials, pipelines have a number of advantages including relatively being safer and higher efficiency due to the nature of pipeline which operates 24/7 without many constrains. Because of this, the use of pipeline is increasingly prevalent in carrying hazardous materials nowadays over other transmission approaches.

However, with such large number of pipelines, the safety problem should also be taken into consideration seriously as the rupture in pipeline could bring catastrophic consequence involving injury, fatality, loss of revenue and irreversible environmental damage. The latest pipeline incident data demonstrated that in 2015, 708 pipeline incidents occurred with about 100,000 Barrels spilled in the United States. The total direct economic losses reached $339 Million. 12 people were killed due to the hazards from pipeline and 49 people got injured.

**Table 1. Number of U.S liquid pipeline miles by system type in 2011-2015 (Portal Data as of 8/31/2016) *The total miles of U.S pipeline (liquid) also include biofuel, $CO_2$ and others by commodity[5].**

| Miles of U.S Pipeline (Liquid) | 2011 | 2012 | 2013 | 2014 | 2015 |
|---|---|---|---|---|---|
| Crude Oil | 56,100 | 57,463 | 61,087 | 66,813 | 72,440 |
| Refined Products | 64,130 | 64,042 | 63,351 | 61,767 | 62,555 |
| Natural Gas Liquids (NGL) | 64,130 | 64,042 | 63,351 | 61,767 | 62,555 |
| Total* | **183,580** | **186,221** | **192,417** | **199,703** | **207,806** |

**Table 2. Number of U.S gas pipeline miles by system type in 2011-2015 (Portal Data as of 8/31/2016)[5].**

| Miles of U.S Pipeline (Gas) | 2011 | 2012 | 2013 | 2014 | 2015 |
|---|---|---|---|---|---|
| Gas Distribution | 2,121,051 | 2,138,001 | 2,149,598 | 2,169,155 | 2,190,549 |
| Gas Gathering | 19,277 | 16,532 | 17,369 | 17,509 | 17,712 |
| Gas Transmission | 305,057 | 303,341 | 302,827 | 301,804 | 301,060 |
| Total | **2,445,385** | **2,457,873** | **2,469,793** | **2,488,468** | **2,509,321** |

Incidents like Qingdao Sinopec explosion in China showed how devastating the outcome could be in terms of pipeline failure and disclosed many safety problems in pipeline management as well, which can be further learned to prevent similar tragedies. The past incidents and near misses are precious textbooks that can reflect different aspects of problematic attributes. In fact, many process safety incidents (pipeline incidents) mostly share similar root causes, therefore, putting considerable attention and efforts to get lessons learned is extremely worthwhile. For this reason, one of the representative pipeline incidents will be briefly discussed to deduct some core causes that will be analyzed in detail later in this manuscript.

On November 22, 2013, a crude oil pipeline suddenly exploded in Qingdao, ripping roads and sidewalks apart, turning cars over and sending thick black smoke over the city. The disastrous blast killed 62 people and injured 136 as one of the deadliest vapor cloud explosions in china. The incident led to the stop in electricity and water in nearby areas. About 18,000 people were then evacuated.

The ignition of crude oil produced by a corroded underground pipeline was the direct cause of the vapor cloud explosion. Workers were using a hydraulic hammer that wasn't explosion-proof, which generated sparks that triggered the blast. Two months later, Sinopec released the official investigation report and pointed out that the pipeline corrosion and human error were the two main causes accounting for this incident.

In addition to the two major causes, several underlying facets also projected the occurrence of the incident. The corrosion of the pipeline that was carrying crude oil was not inevitable. Since 2009, Sinopec pipe storage and transportation branch had conducted three anti-corrosive performance tests, none of the tests did detect the corrosion or potential failure [6]. The negligence of pipeline supervision was exposed in this incident. Carrying out periodic maintenance and careful inspection can dramatically reduce the probability of pipeline rupture, which Sinopec failed to do so. Especially, in this case, the pipelines were buried in a densely populated area that should be treated as high consequence areas (HCA). In the United States, since 2004, all operators of gas transmission pipelines located in the defined high consequence areas have been subject to PHMSA's gas integrity management (IM) program requirements [7]. Similar regulations and socio-organizational management are very worthwhile to learn and to be implemented.

The city's municipal design born the responsibility as well. The extent of corrosion within this pipeline segment was so severe that the pipeline life was actually shorted by about 30 years as the initially designed running span was 70 years. This is largely because the crude oil pipeline intertwined with sewage drains that directly connected with the Yellow Sea of China [6]. It is not hard to imagine that the long-term corrosion by sea water introduced by drain system would fail the pipeline at some point. Obviously, the improper design negatively influenced the pipeline inspection and maintenance and also accelerate the corrosion rate. More seriously, Sinopec did not even get informed of the unreasonable underground utility layout, making it almost impossible to do any management of change (MOC) and planning regarding the design defect.

Besides, the pipeline also experienced frequent traffic-induced vibration which greatly jeopardized the structural integrity, and thus increased the probability of pipeline failure. Once pipeline leaks, the flammable liquid contained in the line could volatile, easily forming a flammable gas phase and all needed is just an ignition source to generate an explosion.

The escalation of the event was not only due to the dense population but also the inadequate emergency response. Considered as the last defense of protection when encountering a process safety incident, emergency planning was so insufficient in this case that the risk of vapor cloud explosion was never covered in the Sinopec safety program. Apart from that, there is no immediate action like evacuation from the dangerous zone. Sadly, most of the fatalities were the pipeline repairing crew.

Many incidents are preventable or can be mitigated to some extent if safety culture is well-cultivated across virtually all levels of an organization [8]. The lack of safety awareness will destroy every layer of protection and facilitate a doomed disaster.

In order to prevent process safety incidents and mitigate the consequences, the hazards should be fully identified, analyzed and assessed beforehand with various applicable methodologies. Based on the PHMSA pipeline incident database, seven major causes resulting in pipeline incidents are summarized as below [9]:

1. Corrosion failure (Internal and external corrosion threat)
2. Equipment failure (Equipment threat)
3. Incorrect operation (Incorrect operations threat)
4. Third-party damage (Third-party excavation threat)
5. Material failure of pipe or weld (Manufacturing, construction, or stress cracking threat)
6. Natural force damage (Weather-related/outside forces threat)
7. Other causes

On the basis of the given major cause categories, the statistics about the number and percentage of pipeline incidents (2011-2015) are listed in Tables 3 and 4. Furthermore, Figures 3 and 4 illustrate the incident counts and percentage distribution by failure cause classification, respectively. As observed from the analyzed data, equipment failure, corrosion, and third-party damage now are becoming the three leading causes weighing 32%, 18% and 15% in the number of pipeline incidents in the past five years.

**Table 3. Number of pipeline incidents by causes from 2011 to 2015 in the United States. Data source: [5]**

| No. of Pipeline Incidents | 2011 | 2012 | 2013 | 2014 | 2015 | Total |
|---|---|---|---|---|---|---|
| Total | 592 | 573 | 619 | 701 | 708 | 3193 |
| Corrosion | 108 | 133 | 97 | 109 | 121 | 568 |
| Equipment Failure | 170 | 176 | 216 | 240 | 212 | 1014 |
| Incorrect Operations | 68 | 77 | 99 | 104 | 79 | 427 |
| Third-Party Damage | 105 | 85 | 98 | 95 | 100 | 483 |
| Materials & Welds Failure | 67 | 53 | 58 | 75 | 99 | 352 |
| Natural Forces | 40 | 24 | 26 | 44 | 47 | 181 |
| Others | 34 | 25 | 25 | 34 | 50 | 168 |

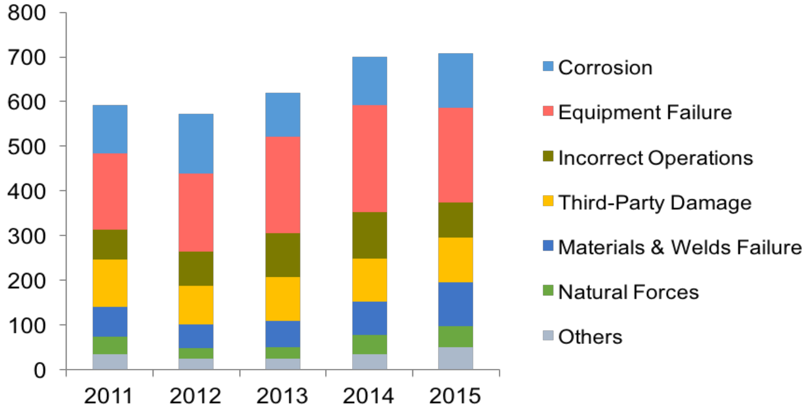


**Figure 3. Cumulative pipeline incident counts by causes from 2011 to 2015.**

**Table 4. Percentage of pipeline incidents by causes from 2011 to 2015 in the United State.**

| Weighing % in Pipeline Incidents | 2011 | 2012 | 2013 | 2014 | 2015 | Total |
|---|---|---|---|---|---|---|
| Corrosion | 18% | 23% | 16% | 16% | 17% | 18% |
| Equipment Failure | 29% | 31% | 35% | 34% | 30% | 32% |
| Incorrect Operations | 11% | 13% | 16% | 15% | 11% | 13% |
| Third-Party Damage | 18% | 15% | 16% | 14% | 14% | 15% |
| Materials & Welds Failure | 11% | 9% | 9% | 11% | 14% | 11% |
| Natural Forces | 7% | 4% | 4% | 6% | 7% | 6% |
| Others | 6% | 4% | 4% | 5% | 7% | 5% |

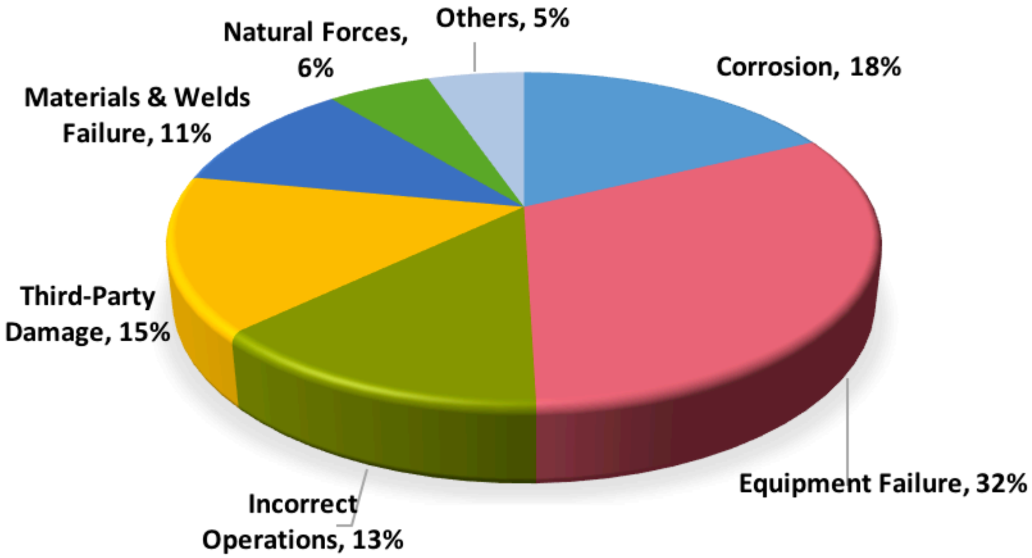


**Figure 4. Percentage distribution of pipeline incidents by failure mode classification (2011-2015).**

Having clearly identified the core causes leading to pipeline incidents, the next step is to establish pipeline risk models using some risk assessment tools. Risk is widely known as a product of failure frequency and the magnitude of undesirable consequences. Conducting a risk assessment is very essential and helpful to prevent adverse incidents during an industrial process when dealing with hazardous materials [10, 11]. Hence, a good and reliable risk assessment is expected to enable safety personnel to manipulate the threats and reduce the outcome as low as reasonably practical (ALARP). Three conventional and commonly used pipeline risk assessment approaches are presented here.

Risk matrix is basically a two-dimensional (sometimes is three-dimensional depending on different analysis scenarios) table with columns containing levels of failure probability and rows involving possible scales of consequence severity, or vice versa. By synthesizing the two risk elements, a risk matrix can stratify the threats with the given specific criteria from previous experience and expert knowledge. The resolution of a risk matrix can be improved by increasing the number of cells in the table and is determined by the need for precision. It is one of the simplest techniques to measure the overall risk and is very easy to understand and apply [12] with intuitive graphical expression. However, this approach lacks of meticulous classification of risk index [13], therefore, cannot handle complex scenarios when demanded.

First used to control the intercontinental missile in 1962 by Bell Telephone Laboratories, fault tree analysis is now one of the most extensively used methods in performing safety studies and testing system reliability [14]. The fundamental idea of a fault tree analysis is to quantitatively evaluate a physical system through a well-built comprehensive diagram implying possible fault attributes and paths. Typically, a fault tree analysis undergoes four steps: system definition, fault tree construction (set a logic diagram through basic elements towards the top event), qualitative assessment and quantitative calculation [15]. An example of fault tree diagram is given by Figure 5.

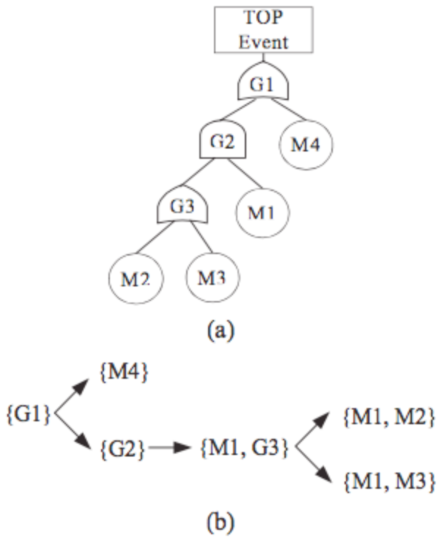


**Figure 5. An example of a fault tree diagram [14]. (a) Fault tree diagram, where symbol G2 represents AND gate, G1 and G3 represent OR gates and M1-M4 represent basic-fault events. (b) minimal cutsets generation.**

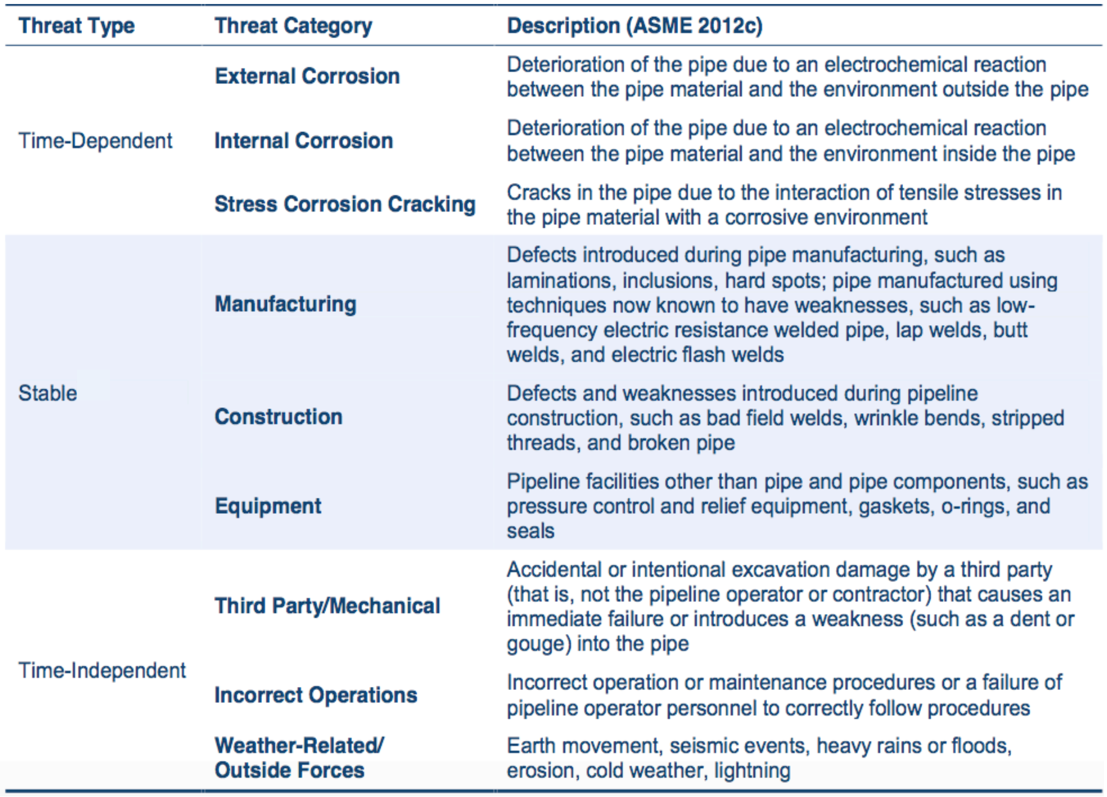
The quantitative risk assessment (QRA) can be derived from the fault tree or event tree techniques with accumulated historical data and statistics, formulating rigorous calculation of probabilities and other numerical risk parameters. The risk assessment by using QRA methodology is now popular among diverse facilities including large chemical plants and nuclear reactors [16, 17].

Indexing risk assessment, known as point scoring system is essentially a widely used technique in the industry to evaluate the performance of pipeline segments by means of adding the scores of assorted variables that related to the pipeline conditions. The assigned numerical values for each variable can either be a risk-increasing item or risk-reducing item [17], while weighting factors associated with each variable reflect its significance judged by engineering experience. These variables contributing to depict pipeline segment activities concern lots of issues including pipeline design, internal or external corrosion, ground or environment condition, etc. [18]. In practice, the global index for each pipeline segment can be obtained by summing up points from each item and multiplying different weighting factors. Having achieved the point values of examined pipeline segments, the safety crew will be more confident in prioritizing future inspection, repair, and many other risk management efforts through the ranking of scored values.

## 1.2 Literature Review

In order to reduce the risk and mitigate the consequence of a pipeline incident, it is critical to familiarize the characteristics of each pipeline hazard category. Knowing the feature of each threat type is conducive to properly choose methods and models for further studies. Table 5 exhibits the classification of pipeline threat types [1] and description defined by ASME 2012c. However, it should be noted that the threats are hard to be strictly classified due to the nature of the hazards, so there exists some overlapping for those threat categories. For example, earth movement like other natural forces remains highly unpredictable and is listed as time-independent hazards. On the other hand, this arrangement seems to contradict the fact that earth does move as the time goes. However, the reason to treat it as a time-independent hazard is primarily due to the stability and randomness from a long-term perspective, though there is no such clear boundary for this case.

**Table 5. Classifications of pipeline threat types [1] and associated threats.**

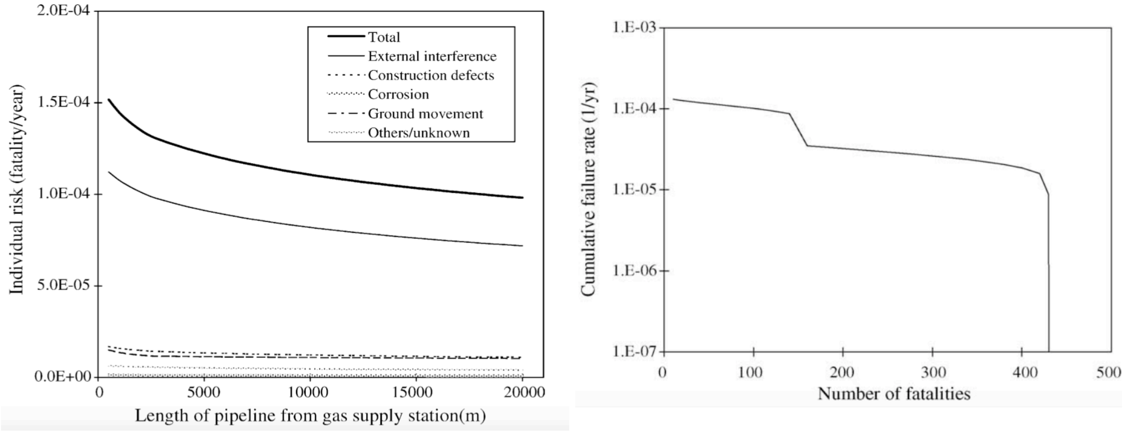


| Threat Type | Threat Category | Description (ASME 2012c) |
|---|---|---|
| Time-Dependent | External Corrosion | Deterioration of the pipe due to an electrochemical reaction between the pipe material and the environment outside the pipe |
| | Internal Corrosion | Deterioration of the pipe due to an electrochemical reaction between the pipe material and the environment inside the pipe |
| | Stress Corrosion Cracking | Cracks in the pipe due to the interaction of tensile stresses in the pipe material with a corrosive environment |
| Stable | Manufacturing | Defects introduced during pipe manufacturing, such as laminations, inclusions, hard spots; pipe manufactured using techniques now known to have weaknesses, such as low-frequency electric resistance welded pipe, lap welds, butt welds, and electric flash welds |
| | Construction | Defects and weaknesses introduced during pipeline construction, such as bad field welds, wrinkle bends, stripped threads, and broken pipe |
| | Equipment | Pipeline facilities other than pipe and pipe components, such as pressure control and relief equipment, gaskets, o-rings, and seals |
| Time-Independent | Third Party/Mechanical | Accidental or intentional excavation damage by a third party (that is, not the pipeline operator or contractor) that causes an immediate failure or introduces a weakness (such as a dent or gouge) into the pipe |
| | Incorrect Operations | Incorrect operation or maintenance procedures or a failure of pipeline operator personnel to correctly follow procedures |
| | Weather-Related/ Outside Forces | Earth movement, seismic events, heavy rains or floods, erosion, cold weather, lightning |

Currently, studies of risk assessment on oil and gas pipelines (considered comprehensive aspects of hazard sources) have been widely conducted by a quantity of research groups because of the significant impact on pipeline safety and security [19-30].

Some quantitative risk assessment (QRA) approaches have been applied to measure the risks in oil and gas piping. Jo [19] developed a simplified consequence-based analysis by incorporating parameters of fatal length and cumulative fatal length to investigate two popular risks namely, individual risk (IR) and societal risk (SR). In this paper, the fatal length by definition is the distance having an integrated fatality along the pipeline where an incident occurs, while the cumulative fatal length is the distance having N or more fatalities. The consequence analysis exploring thermal effect and gas release rate was eventually converted to solving the fatal length and the cumulative fatal length. As a result, the individual risk or societal risk can be achieved by combining the fatal length or cumulative fatal length with the data of pipeline failure probabilities as shown in Figure 6(a) and (b).

**Figure 6. (a) Individual risk as a function of the length from gas supply station. (b) F-N societal risk curve [19].**



This novel method can reduce the complication of quantitative risk assessment by shifting the difficulty of evaluating consequences to calculating fatal length and cumulative fatal length which can be easily estimated by using geographic information systems (GIS). Nonetheless, this approach only considered the consequence of fatality regardless of economic loss or environmental loss. In addition, other physical effects cannot be ignored, because in more practical scenarios, factors like toxicity, overpressure, and explosion are indispensable in the process of consequence investigation.

Similar quantitative risk assessment approaches have been improved in the study carried out by Han [20, 21] and Gharabagh [22] where diverse influential consequence models are incorporated considering various real-case scenarios. But the lack of historical data and structural reliability analysis still seriously constrain the prediction precision.

On the other side, qualitative risk assessment also catches considerable attention to fundamentally clarify the failure mechanism of a pipeline segment by implementing fault tree analysis where the failure modes are degraded to corrosion, errors in construction, design factors and external hazards in Dziubinski's study [23] as observed in Figure 7 and degraded to interference from third party, corrosion, defects of pipe, incorrect operation, unreasonable design and geological hazard in Dong's study [24]. But now, a complete risk assessment is much preferred with more quantified data combined in the model.

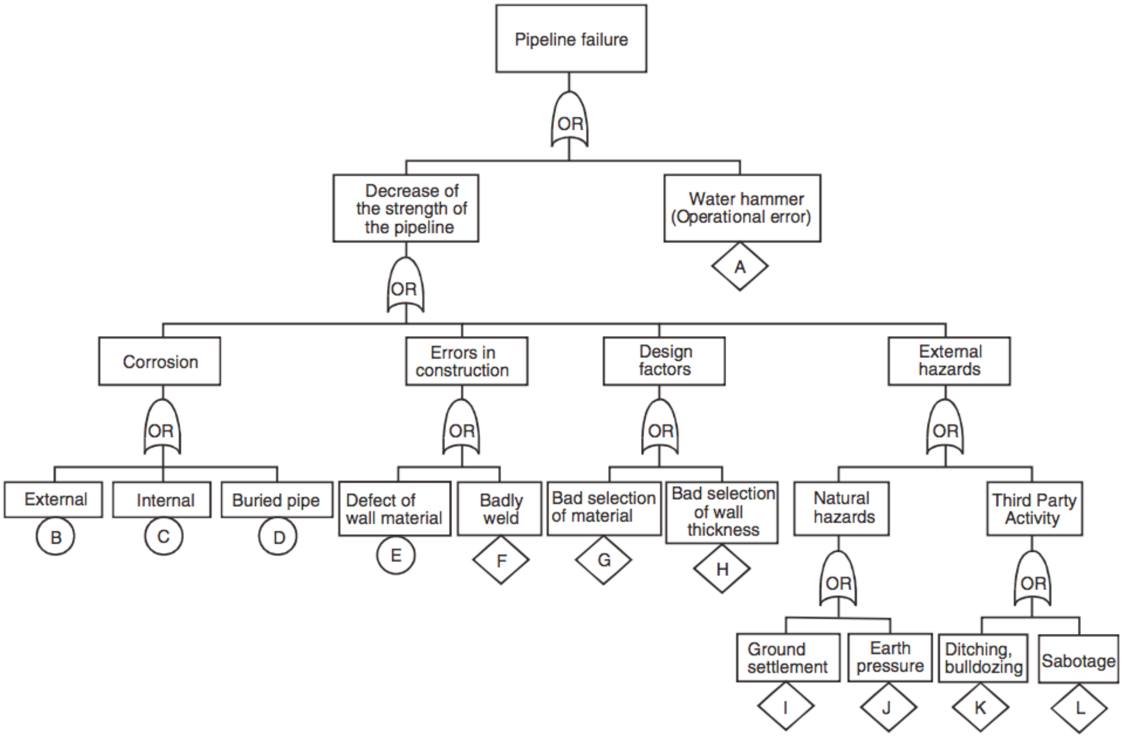


**Figure 7. Fault tree analysis for pipeline failure [23].**

Among the existing methods of pipeline risk assessment, Analytic Hierarchy Process (AHP) is a risk-based model that allows more interactive participation of decision-makers and executives with many years operating experience to examine pipeline problems. Great emphasis has been placed on this empirical method [25-27] industrial-wide since it involves more practical inputs and is flexible and easily understood. The principle of AHP is firstly formulating a structural framework by hierarchy, and then listing the level of goal, main risk attributes, sub-attributes and a few pipeline segments which align with their natural stretch. Once the skeleton is formed (shown in Figure 8), comparisons will be made for each pair of pipeline segments in terms of risk attributes and sub-attributes (assigning credits) to determine the likelihood of failure (normalizing the credit), while the severity of failure is then decided by a Monte Carlo simulation [25]. The results of likelihood and severity for each pipeline segment with regards to various risk factors are elaborated in Table 6. Consequently, the ranking based on assessment provides a powerful reference for decision-makers to adopt a suitable plan for the pipeline inspection and maintenance.

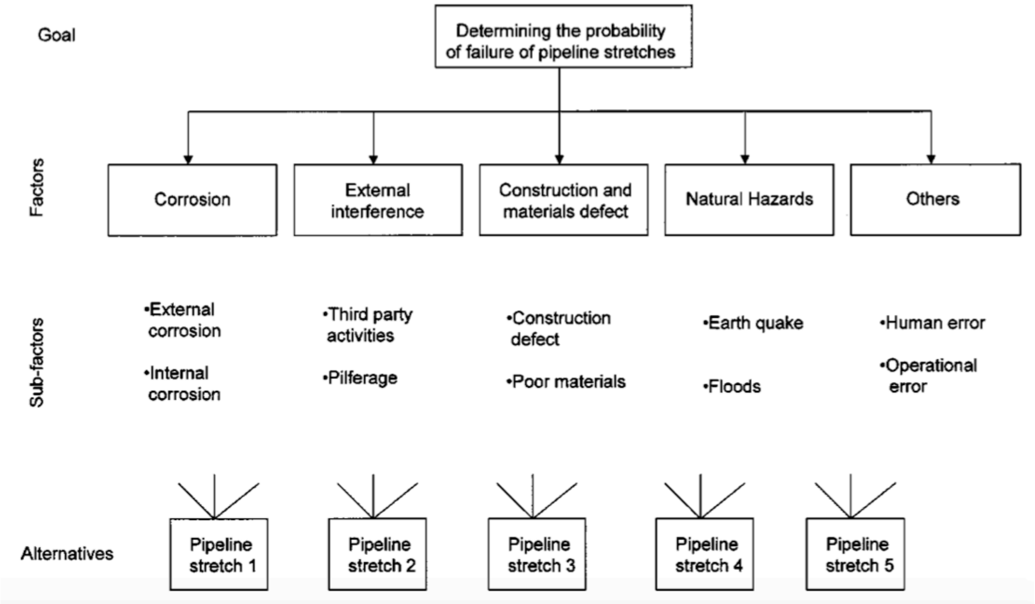
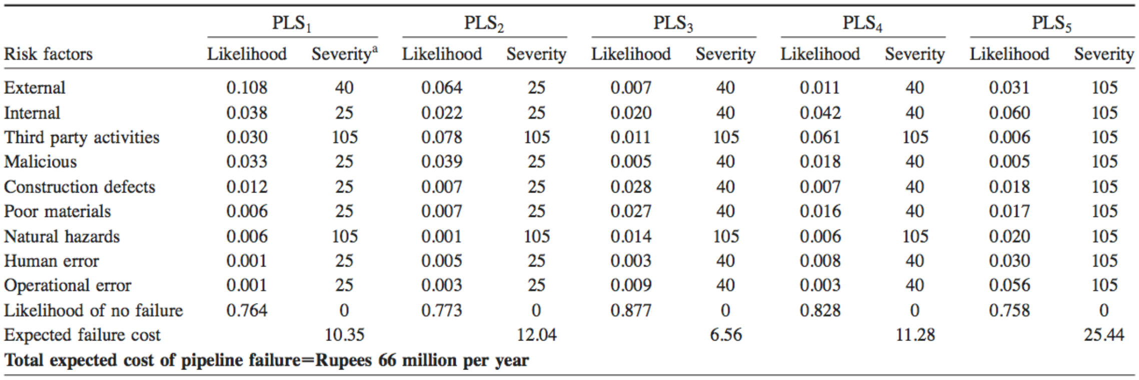


**Figure 8. Framework of AHP on pipeline risk assessment with five different pipeline stretches [25].**

As a matter of fact, representatives who work on the pipeline risk analysis could be buried in the plenty information from pipeline database and numerous contributing factors, which may negatively affect the judgement for pipeline condition and the probability of failure. Therefore, the limitations of this technique lie in the subjective thoughts which can substantially undermine the effectiveness of this model.

**Table 6. Likelihood and severity of each pipeline segment by various risk factors [25].**



| | PLS$_1$ | | PLS$_2$ | | PLS$_3$ | | PLS$_4$ | | PLS$_5$ | |
|---|---|---|---|---|---|---|---|---|---|---|
| Risk factors | Likelihood | Severity[a] | Likelihood | Severity | Likelihood | Severity | Likelihood | Severity | Likelihood | Severity |
| External | 0.108 | 40 | 0.064 | 25 | 0.007 | 40 | 0.011 | 40 | 0.031 | 105 |
| Internal | 0.038 | 25 | 0.022 | 25 | 0.020 | 40 | 0.042 | 40 | 0.060 | 105 |
| Third party activities | 0.030 | 105 | 0.078 | 105 | 0.011 | 105 | 0.061 | 105 | 0.006 | 105 |
| Malicious | 0.033 | 25 | 0.039 | 25 | 0.005 | 40 | 0.018 | 40 | 0.005 | 105 |
| Construction defects | 0.012 | 25 | 0.007 | 25 | 0.028 | 40 | 0.007 | 40 | 0.018 | 105 |
| Poor materials | 0.006 | 25 | 0.007 | 25 | 0.027 | 40 | 0.016 | 40 | 0.017 | 105 |
| Natural hazards | 0.006 | 105 | 0.001 | 105 | 0.014 | 105 | 0.006 | 105 | 0.020 | 105 |
| Human error | 0.001 | 25 | 0.005 | 25 | 0.003 | 40 | 0.008 | 40 | 0.030 | 105 |
| Operational error | 0.001 | 25 | 0.003 | 25 | 0.009 | 40 | 0.003 | 40 | 0.056 | 105 |
| Likelihood of no failure | 0.764 | 0 | 0.773 | 0 | 0.877 | 0 | 0.828 | 0 | 0.758 | 0 |
| Expected failure cost | | 10.35 | | 12.04 | | 6.56 | | 11.28 | | 25.44 |
| **Total expected cost of pipeline failure=Rupees 66 million per year** | | | | | | | | | | |

Other advanced risk assessment tools such as fuzzy logic interference systems [28, 29] and indexing risk models [30] are also used to monitor pipeline safety and have achieved notable success.

But more detailed concerns and discussions on some of the leading causes especially the third-party damage were much less reported in the literature compared with other causes like corrosion [31-36]. The third-party involvement is the third core cause followed by equipment failure and corrosion, weighting 15% in the incident reports during the past five years recorded by U.S. Department of Transportation (DOT) as indicated in Figure 4 [5]. This kind of external interference composed of accidental activities and malicious sabotage or pilferage contributes as high as 75% to the total individual risk [19, 25]. Moreover, the deliberate intent of pipeline damage is more common and rampant in the socioeconomically deprived regions. In some undeveloped areas of China, many oil transmission pipelines are drill by oil stealer for profit each year. For instance, it is documented that 6743 holes were drilled on the pipeline of

Changqing oilfield in 2000 along with the loss of 13,000-ton oil and approximate 15.43 million in U.S. Dollars. The 655.37 km-long Luning pipeline had 227 holes during 1999 to 2003 [37]. Figure 9 displayed a 5m-long drilled pipeline segment with 9 holes. Similarly, data showed that vandalism ranked as the top one cause that challenged the pipeline safety in Nigeria [38].

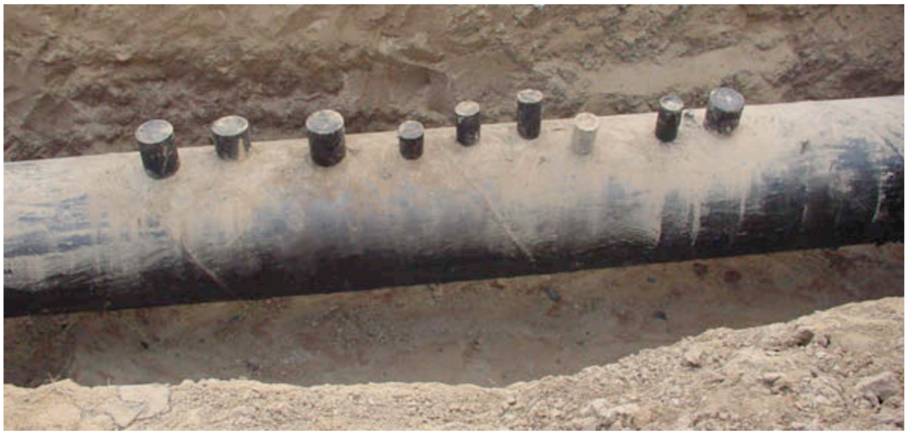


**Figure 9. 5m-long drilled pipeline segment with 9 holes [37].**

The fact that both the accidental third-party excavation and intentional sabotage can result in severe consequences should arise the research attention in this field and cannot be neglected. A few preliminary studies were performed in investigating the third-party interference on failure frequency by pipeline diameter [39] and in employing a self-organizing maps (SOMs) to evaluate the third-party risk pattern[40]. The latter study proposed to use SOM algorithm to reveal main relationships among pipeline section variables. However, there is no such a systematic risk assessment study to distinctively analyze third-party damage on pipeline based on the two different impulses.

## 1.3 Motivation

Maintaining the integrity of pipeline from a number of factors is a far-reaching and challenging subject. It is a vital responsibility for companies of oil and gas industry to prevent significant pipeline failures and mitigate potential consequences both in the technical aspect and in the management aspect.

Risk assessments on pipeline focusing on more controllable factors such as corrosion have been performed with rich results, leading to the considerable decrease in pipeline failure of corrosion during the past decades. In contrast, the other leading cause, third-party damage is still resistant since it's quite difficult to forecast or control in advance. In this context, a systematic risk assessment study that distinctively analyzes third-party damage on pipeline will be developed based on the two different impulses.

## 1.4 Research Objectives

The main purpose of this thesis research is to build models to distinctively investigate the third-party interference (malicious damage vs. accidental damage) on pipeline. In order to reach the goal, the following objectives are settled:

- To demonstrate pipeline risk factors of accidental third-party damage by with Bayesian network approach.
- To predict the probability of pipeline segment failure due to accidental third-party damage with good consistency of real data.

- To device a game theory model to understand the risk pattern and sort out messy scenarios. This will help to support decisions defending malicious third-party damage and mitigate consequences result from the adversarial acts.

## 1.5 Organization of This Thesis

This thesis is organized into five sections:

Section 1 provides background information that states the important role of oil and gas industry in global energy market, the advantages of using pipeline to transport hazardous materials such as petroleum and natural gas, and the severe consequences of pipeline failure. The later part of this section gives the literature review within this subject.

Section 2 presents the general introduction of methodologies that will be applied in the models (developed in later sections) to study the third-party damage on pipeline risk assessment. Bayesian network and game theory will be briefly addressed.

Sections 3 and 4 will each explore a model to examine the risk from the accidental third-party interference and the intentional third-party activities. The former model is formulated with Bayesian network approach, visualizing the cause-effect relationship among diverse risk attributes, and at the end predicts the probability of pipeline failure. The latter model is established by game theory to establish and sorts out a variety of security related risk scenarios.

Section 5 is devoted to make conclusions, and recommendations for future work.

# 2. METHODOLOGY

## 2.1 Bayes' Theorem and Bayesian Network

Probability of occurrence was inclined to be treated constant and independent in many fundamental models, while in the real-world case, that's probably not true. The belief in Bayes' Theorem is that all probabilities are conditional. Assuming there are two events H and E, where H is a hypothesis that can cause event E. Oppositely, E is the evidence that reflects an effect from H and thus the two events are mutually dependent. Let's also assert that events E and H are the only two nodes in the system. In this case, the terminology of probability E, represented as P(E) would be more accurate to be substituted as P(E|H), where event H indeed is the background or context that can strongly affects E [41]. Similarly, the term P(H|E) represents the probability of H given by the information of E. The Bayes' Theorem summarized this relationship between the probability of the occurrence of E and H by a succinct equation:

$$P(H\,|E) = \frac{P(E\,|H)P(H)}{P(E)} \tag{1}$$

The correlation can be expanded as much as one desired depending on the subjective scenarios, bringing more relevant events. Thus, the joint probability of event E, P(E), is derived by a series of conjugated events H = $H_1$, $H_2$, …, $H_n$ shown as:

$$P(E) = \sum_{i=1}^{n} P(E \mid H_i)P(H_i) \tag{2}$$

With this revision, the probability is given by:

$$P(H_i|E) = \frac{P(H_i, E)}{P(E)} = \frac{P(H_i, E)}{\sum_{i=1}^{n} P(E \mid H_i) P(H_i)} \tag{3}$$

Bayes' Theorem is highly adaptive that allows us to update or change the predictions and diagnoses based on the new knowledge and observations in hand [41]. The formula can be rewritten as follows [42] when new data got observed. The posterior probability is able to get revised from time to time when new evidence is obtained, where the system uncertainty can thus be reduced.

$$Posterior\ probability = \frac{Likelihood \times Prior\ probability}{Marginal\ Likelihood} \tag{4}$$

With the understanding of Bayes' Theorem, Bayesian networks can be established by identifying variable nodes, building interrelated cause-effect relationship and putting initial data. Variable nodes directly linked by arrows are computed via the fundamental basis of Bayes' Theorem for probabilistic reasoning. The increasing number of associated variable nodes propagates the Bayesian network. Figure 10. demonstrated a simple example of Bayesian network.

The Bayes' Theorem has been proved to be a very powerful tool in a wide range of domains such as artificial intelligence, brain imaging, machine learning, human object recognition. The success in the application of Bayes' Theorem in the above spectrum inspired people to use the same tool in process safety and risk assessment modeling and gained notable results [43, 44].

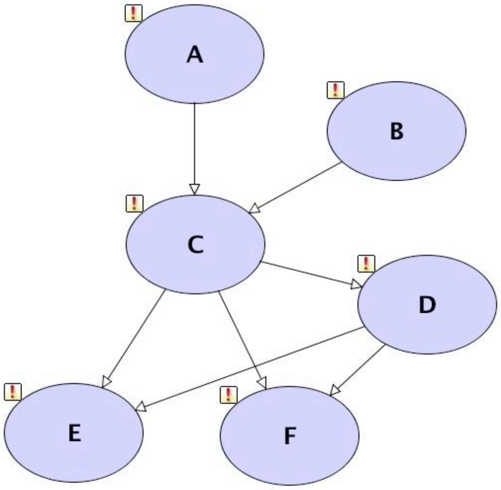


**Figure 10. An example of Bayesian network.**

## 2.2 Game Theory

Game theory is a science that uses mathematical models of conflict and cooperation between intelligent rational decision-makers where insights and solutions are offered for a general scope of domain such as economics, politics and social situations [45]. As suggested by Myerson, the name of "game theory" might be more descriptive and easy for understanding when replaced by the terms like "conflict analysis" or "interactive decision theory" [45], since it ultimately analyzes how two or more individuals influencing the other's benefit based on his or her behavior.

In view of the history, much of the early work of game theory was established by many scholars during World War II in order to deal with different kinds of controversial situations. With the progress of civilization and physical technologies, people were increasingly facing more dilemma such as nuclear power, which called for deeper and broader study on way of handling problems. The modern game theory focuses on important economics application with the arts of tackling complications and it has been brought into horizons by awarding the Nobel Prize to a group of wise game-theorists. Till now, eleven game-theorists have won the economics Nobel Prize for their remarkable contributions.

For a better understanding in the model that was built for intentional third-party damage with game theory in the fourth section of this manuscript, some of the basis and terminology will be defined here. And a classic example will later be presented to reinforce these concepts.

Game: a game encompasses a collection of decision-makers, the possible information states of each decision-maker at each decision time, the collection of possible moves, a procedure for determining how the action choices of all players determine the possible outcomes and the preferences of individual decision-maker over these outcomes.

Player: each participant (interested party) that makes decisions in a game.

Strategy: a player decides his or her course of action from the list of action during the game. There are two types of strategies, pure strategy and mixed strategy depending on the magnitude of cooperation between players. Pure strategy stands for a single course of action for each player, while mixed strategy means a course of action for each player in accordance with some particular probability of distribution. The model built in section four only take pure strategies.

Payoff: the outcome of playing the game for each player.

Saddle point: is one of the payoff combinations of players shown in the payoff matrix that has the smallest value in its row and the largest value in its column. The saddle point is considered as an equilibrium point in a zero-sum game (will be explained later of this section) that results in a solution based on Min-Max theorem [46].

Nash Equilibrium: a specific $n$-player combination feasible strategy $S*$ with each player $i$, where $S^{*} = S_1^{\ *} \times S_2^{\ *} \times \cdots \times S_n^{\ *}$ that no player perceives a way of achieving a higher payoff by switching strategies while all the other players keep theirs unchanged [47]. This current strategy set with the corresponding payoffs constitute a Nash Equilibrium. In other words, Nash Equilibrium is a solution among all the available strategy combinations of players to have a best result from each individual point of view. Basically, the choice of strategy to each player is the best response towards a comprehensive consideration of what others will decide to choose. At this point, each player makes what he thinks the optimal decision under the current circumstance without any regrets. Therefore, the status of this point where no player wants to change his mind any more is defined as Nash Equilibrium. Regarded as an alternative solution (the other solution is Min-max theorem), Nash Equilibrium can both solve zero-sum game and non-zero sum game.

Zero-sum game vs. Non-zero sum game: In a zero-sum game, the payoff for every combination strategy always adds to zero, and non-zero sum game has a net outcome greater or less than zero. The former type is more ideal, while the latter one is more dominant in today’s studies.

Simultaneous vs. Sequential game: In a simultaneous game, players make decisions simultaneously without having any prior knowledge of opponent's move. The investigation of this sort of game is analyzed by payoff matrices. Different from the static simultaneous game, a sequential game, known as dynamic game is denoted by decision trees where the later player has some information on the prior player's move.

## 2.3 Prisoner's Dilemma

To fully illustrate a game theory model in terms of its concepts and general operation mechanism, this section will address a very basic and famous example, the prisoner's dilemma. This issue was originally framed by Merrill Flood and Melvin Dresher working at RAND in 1950.

Two suspects A and B were under arrest. Each of them was in a solitary confinement with no means to communicate with the other. The police knew they were guilty but were lack of sufficient evidence. So the prosecutors then offered each the same bargain at the same time. Each prisoner had two choices, either confess the crime (betray the other) or remain silent (cooperate with the other).

As a result, there are four possible situations:

- If A and B were honest and both betray the other, each of them would serve 8 years in prison.
- If A confessed and B remained silent, A will be set free while B will have a more severe punishment with a 10-year sentence.

- Similarly, if B confessed and A remained silent, B will be set free while A will have the 10-year sentence instead.
- If A and B both took the opportunities and deny the offence, both of them will only be given 1-year sentence.

The four possible scenarios are summarized in Table 7 where the columns represent prisoner A's behavior and the rows denote prisoner B's choices. Correspondingly, the four situations are shown pairwise in parentheses and the values indicate payoff of prisoners A and B, respectively. For instance, the pair of (0, -10) implies that A will be free from jail and B will be sentenced for 10 years.

**Table 7. Payoff matrix of a standard prisoner's dilemma.**

| **A\B** | **Confess** | **Deny** |
|---|---|---|
| **Confess** | (-8, -8) | (0, -10) |
| **Deny** | (-10, 0) | (-1, -1) |

The prisoner's dilemma holistically is a non-zero sum simultaneous game where prisoners A and B are the two players got involved. Each of them have two strategies: confess or deny the crime, forming a total of four strategy combinations. Since none of them was able to know the information about how the other will respond regarding with the offer, this game is categorized as simultaneous game with the payoff indicating the number of years being sentenced.

It is apparent that the best payoff in the combination of strategies is (-1, -1) when both of the two prisoners kept silent. Interestingly, Nash equilibrium provides the solution of (-8, -8) that the rational and intelligent prisoners will tend to choose despite the plausible optimal outcome of (-1, -1). That is because no matter what action the other prisoner will decide to take, confession always seems to be a better alternative. Supposing the other player denied, A (or B) is prone to choose confession because A (or B) can be set free rather than has 1-year sentence. Likewise, supposing the other player confessed, A (or B) still would prefer to choose confession since he would only get 8-year sentence compared with 10 years. Eventually, both of them betrayed the other.

Game theory is a quantitative modeling process with strategic interaction between players. In addition to economics, the application of game theory can also be a valuable and promising tool that assists industry to sort out the messy scenarios, defend malicious activities with proper decisions, and ensure the personnel and property safety.

# 3. RISK ASSESSMENT OF UNINTENTIONAL PIPELINE THIRD-PARTY DAMAGE WITH BAYESIAN NETWORK (BN)

The statistics released by Pipeline and Hazardous Materials Safety Administration (PHMSA) under U.S. Department of Transportation (DOT) indicates that third-party disturbance is among the top three causes attributing to the pipeline failure. 15% to 18% pipeline incidents in U.S. were directly related to third-party intrusion, and this type of failure cause was responsible for approximately 50% of all pipeline incidents in Western European countries [39]. In spite of its considerable portion among the pipeline failure modes, third-party damage was far less stressed. Compared with corrosion and equipment failure which in a long time had attracted great attention from industry and had evolved with new technologies to reduce the failure rate, the pipeline failure caused by third-party damage is one of the least factors being considered during the pipeline hazard assessment stage. Therefore, this study is conducted aiming at investigating pipeline risk resulting from third-party damage, and will formulate risk assessment model to identify threats, prioritize risks and determine which integrity plan should apply to different pipeline segments given the condition of third-party interference.

The term of third-party damage refers to the interference on pipeline from activities of personnel not associated with the pipeline. In other words, a third-party is obviously neither a pipeline operator nor a contractor who serves to pipeline working properly and this failure mode is ascribed to incorrect operations and human error. On the other hand, some literature concluded third-party damage with the description of external interference or outside forces which covered the aspect of natural forces like earth movements and seismic events. In this study, the third-party damage analysis would be addressed to investigate activities from personnel not associated with pipeline while excludes natural force impact.

The third-party damage can be either accidental disturbance caused by excavating in the vicinity of buried utilities without realizing the presence of oil and gas pipeline or malicious interference caused by sabotage or pilferage. Damage in both cases can lead to severe consequences, immediately jeopardizing life and property. Even interference that appears to be minor can undermine the integrity of the pipeline under a cumulative period of time, and eventually cause the pipeline failure. Nonetheless, the risk analysis of unintentional third-party interference and malicious acts are intuitively different. While the probability of pipeline failure due to unintentional third-party interference explicitly correlates with comparatively well-defined factors in terms of pipeline characteristics and maintenance, the risk pattern of malicious acts primarily relies on less straightforward variables such as the understanding of adversarial intention, facility criticality assessment and security vulnerability assessment [48]. For this reason, the study in these two modes (unintentional interference and malicious acts) of pipeline risk assessment due to third-party damage will be elaborated in separate sections 3 and 4, and this chapter will place emphasis on the risk assessment by unintentional third-party interference model simulation.

### 3.1 Unintentional Third-Party Damage BN Model Development

One of the commonly employed practices of pipeline risk assessment is the relative risk model known as risk scoring with threats weighted and summed up to generate a comprehensive value measuring an overall risk of a specific segment of pipeline. On the other hand, a number of pipeline operators and process experts through interview investigation implied a demand for a more probabilistic model being implemented, as this type of risk presentation can be easily interpreted and visualized to all levels of an organization. Consequently, the model developed in this section will combine the ideas from the two methods targeting to clarify the cause-effect mechanism of unintentional third-party damage and quantify the failure probability under this type of failure mode without loss flexibility.

The non-malicious third-party damage BN model is devised through the following stages and will be delineated with more details later in this section:

1. Identify main components that impact the pipeline probability of failure due to unintentional third-party damage.
2. Degrade each component with more fundamental factor analysis and create a graphical representation of the chain events to show the cause-effect dependency.
3. Integrate fundamental factors by applying weighing factors and build a mathematical framework.
4. Generate third-party disturbance index by combining main components throughout the Bayesian Network (BN).

5. Estimate pipeline failure probability due to unintentional third-party damage based on available historical data and current calculated risk score given pipeline performance and evident observations.
6. Input data based on the evaluation of pipeline characteristics, expert judgements, historical failure experience and engineering modeling. Initial distributions were assigned and the assumed initial values are interchangeable once data are gleaned.

The first stage, independent hazard identification is largely seeking the main components that directly associate with pipeline risk performance specifically affected by unintentional third-damage. These main components could serve as incident leading and lagging indicators illustrating a sense of relative risk. The risk assessment of pipeline failure due to exposure to unintentional third-party intrusion is generally controlled by the following listed variables.

**Public awareness and education on third-party digging**

**Location**

**Cover**

**Presence and performance of pipeline markers and barriers**

**Patrolling**

**One-call system**

**Planning and new technologies**

### Public awareness and education on third-party digging

A third-party intrusion is predominantly composed of excavation projects conducted by personnel who are irrelevant with the oil and gas pipeline. The digging process ranging from a building or utility construction to a house-owner installing swimming pool could accidentally hit or damage the pipeline and thus result in catastrophic consequence and monetary loss. To ultimately eliminate the potential hazards and mitigate the crisis where people are ignorant about the buried oil and gas pipeline location and the indication signs, the public should continuously cultivate and improve safety awareness on the third-party digging by launching public education program. A series of actions should be taken to assure proper digging procedures within the public education program.

To reduce the pipeline failure from household individual digging, mailout and regular door-to-door contact with neighboring community are very essential in spreading oil and gas pipeline safety culture as considered the first line of defense [30]. Good community education on pipeline third-party digging will not only provide the right guidance such as calling 811 to get notified about all digging information for every digging attempt, but also makes the residents as a part of pipeline protectors or patrollers. In general, the contact or meeting should be held at least once every year.

The risk communication among pipeline company, local government, and other utility companies plays an extremely important role in preventing pipeline failure from other constructional excavation. Local government should take the responsibility to arrange meetings before any excavation construction projects and make decisions of issuing the permits in the aftermath. During the meeting, pipeline company should be committed to provide geologic information of the pipeline as precise as possible while utility companies are supposed to clearly state the processes involved in the ongoing plans.

The magnitude of public education on unintentional third-party damage reflecting governmental endeavors in coordination with pipeline companies, local community, and utility companies is divided into five levels from very low to very high and attributes 15% to the third-party disturbance index.

### Location

The likelihood that onshore pipeline being exposed to accidental third-party interference strongly relies on the location which is complicated and synthesized by a number of aspects such as population density, frequency of constructional activities, rail and road disturbance, the presence of other buried utilities, and wildlife activities, which are linked by arrows shown in the Bayesian network. In addition to determining the probability of the risk, the location is an indispensable element for failure outcome analysis as well by applying various physical consequence models.

The five aspects mentioned above measure the location impact on pipeline third-party damage from different perspectives and perform as “parent” nodes to determine the condition of the “child” node of location. Each parent event is actually not assigned by an exact score but a discrete probability density function that describes the performance state. In contrast to the traditional risk scoring assessment that evaluates each variable with one certain credit, the probability density function leaves flexibility to manage the uncertainty of the risk. As the data is available, these parent nodes can be filled with precisely known state; even though the information sometimes is incomplete or absent, soft observations and initial assumptions can be temporarily used to assess the risk.

It is apparent that more populated regions are more susceptible to the third-party interference. An example to demonstrate the tendency is that 35% of excavation damage during 1984-1987 occurred in Class 1 and 2 locations (shown in Table 10 defined by DOT pipeline regulations) as summarized in DOT gas pipeline incidents statistical report. More populated areas or regions with heavy and frequent construction activities correspond to a higher risk and lower risk score level in the "child" node of location. Locations with high volume of train and vehicle are prone to have the aboveground pipeline suffer outside force damage by car hit. In the meantime, the conditions of other buried utilities may affect the buried oil and gas pipeline integrity. An example is the Qingdao Sinopec pipeline explosion incident where sewage system intertwined the existing oil pipeline, which severely aggravated pipeline corrosion. Besides, the maintenance of other buried utilities could also introduce extra excavation equipment strike on the oil and gas pipeline. Other concerns include the wild animal disturbance in some areas. Large animals like bison can do damage to the pipeline instrumentation and pipe coatings.

In the calculation of location node, the aspects of population density, construction activities, train and vehicle, other buried utilities and wildlife damage weigh 30%, 30%, 10%, 20% and 10%, respectively. Because of the great impact on the risk of unintentional third-party damage, the node location is weighing 20%.

**Cover**

The node Cover among the main risk variables serves as a passive protection layer from third-party damage. The effectiveness of cover protection depends on the depth and nature of the cover. Firm cover with adequate depth not only can conceal the pipeline but also protect it from earth moving equipment to some extent.

Study conducted by Mather *et al*., [39] revealed the relationship between pipeline failure frequency caused by third-party and the depth of cover based on the data source from European Gas Pipeline Incident Data Group (EGIG) given by Table 8. For those pipelines that were buried with less than 31.50-inch cover only weight 10% in the overall operating experience but account for about 65% failure frequency. The pipeline failure frequency drastically decreases with increasing depth of cover, especially for the case when the depth reaches 31.50 inch and above. Nowadays, in U.S. three feet (36 in) is a standard cover depth as requested by many regulatory agencies for new buried pipeline construction [30]. The node Depth of Cover in the BN model can be assigned a point value within the score range from 0 to 100 according to the actual depth. This point value is determined by dividing the actual depth (with the unit of inch) by 45 and multiplying 100 (the score cannot exceed 100). For instance, the pipeline minimum buried depth is 36 inches and the score for the node Depth of Cover follows:

$$36 \text{ inch of cover} = 36 / 45 * 100 = 80 \text{ points}$$

The initial points distribution is assumed with an average of 80 points in the normal distribution. Observations can be inserted into the model whenever the information is available.

**Table 8. Third-party damage failure frequency per depth of cover**

| Depth of cover (in) | Number of failures | Operating experience (mile-year) | Total failure frequency (1000 mile-year)$^{-1}$ |
|---|---|---|---|
| 0 - 31.50 | 103 | 86,140 | 1.196 |
| 31.50 - 39.37 | 248 | 664,512 | 0.373 |
| 39.37+ | 120 | 479,925 | 0.250 |

The nature of cover is another criterion in assessing cover protection effectiveness. Enhanced materials such as concrete or asphalt in the surface layer and rock or slab in the soil layer can create an additional level of protection. Hence, an advance cover nature and deeper cover depth formulates a safer condition as presented in the node of Cover shown in the BN model.

**Presence and performance of pipeline markers and barriers**

Oil and gas pipelines exist everywhere and are generally buried underground. Easily recognized markers and aboveground warning signs play a critical role in helping people to identify the location of pipeline corridor so that can successfully prevent accident third-party intrusion. Barriers like fence, tree and valve lockout are able to exempt an aboveground pipeline facility and instrument from third-party interference. Another best practice is to bury a warning tape which is commercially available along with the pipeline corridor. The highlighted strip reminds people who are digging in the right-of-way (ROW) area the presence of pipeline, and hopefully they will cease the excavation action when discover the warning tape. The node of Markers and Barriers attributes 10% to the third-party disturbance index.

**Patrolling**

Regular pipeline patrolling is intended to detect the abnormal pipeline condition ranging from more evident phenomenon such as pinhole or rupture on the surface of the pipeline to subtle indications like dead vegetation and the construction activities near the ROW. This visible inspection method is able to proactively spot imminent threats and terminate the third-party intrusions by periodic observations and becomes the only means to examine unreported pipeline digging when an official excavation notification system is absent.

Pipeline patrol is proved to be an effective way to directly fight with the third-party damage, whose value is assessed by frequency and thoroughness. The number of ground and air patrol in a certain period of time increases the detection opportunity and the possibility of discovering potential hazards. Usually a cost-benefit analysis is performed to determine the optimal interval of patrol. The node of Frequency in the BN model is therefore derived with five kinds of schedules from less than once per month to daily. As to the patrol thoroughness, checklist is often utilized by patrol technician or observer to ensure various facets have been inspected. Apart from regular failure detection, involved aspects in relation to third-party intrusions include missing markers or warning signs, construction activities near the pipeline, indication of heavy traffic through the ROW, ROW encroachments, unauthorized acts, and third-party changes to slope or drainage. It is reasonable to assume that the average value of patrol thoroughness score is 80 out of 100 based on the patrolling mitigation study [30]. Again, an initial probability density function is assigned, and an evaluator can input a real number in the Thoroughness node when applying this BN model.

**One-call system**

The invention of one-call system offers an interactive platform for risk communications between the third-party ready to excavate and the pipeline protection agencies. This formal service requires landowner or excavation contractor to call to locate the exact pipeline buried site prior to the construction as well as to immediately notify any disturbance made to the pipeline. The one-call system successfully helped to avoid third-party intrusions and reduced the related incidents by 20% - 70% in the investigated sixteen one-call centers [49]. Key elements to evaluate the effectiveness of one-call system as the nodes presented in the BN model are Widely Advertised, Standard Establishment and Enforcement, and Appropriate Reactions to Calls.

Sufficient advertisement on one-call system ensures this service got fully utilized and the degree of community engagement largely affects the number of unreported excavations. In most states of the United State, participation to one-call is a law and obligatory. Therefore, industry standards and noncompliance penalty should be clearly addressed to guarantee the system working properly. For those countries lacking such formal notification system, it is urgent to develop similar program especially in the case where the number of oil and gas pipeline is tremendous. Finally, as the backbone of one-call system, appropriate reactions to calls from general public or excavation contractors mean to arrange a sequence of actions in an efficient manner. Timely efforts should be made to recordkeeping and documentation, pre-job contact and communication, dispatching personnel to mark pipeline location, guidance with accurate mapping, and site inspection during and after the excavation activities [30]. The above three aspects cooperatively reflect the overall one-call system performance and are illustrated in the graphical BN model shown in Figure 11.

**Planning and new technologies**

As new sophisticated technologies emerging for safer excavation, the probability of pipeline being punctured by heavy equipment no doubt will be reduced with that application. Appropriately utilizing inherently safer techniques like hydro-vac excavator could avoid strikes on pipeline containing natural gas and petrochemical products at early stage. Beyond that, good planning and job safety analysis (JSA) are also conducive for third-party operators to realize the pipeline hazards so that risky events will be done with greater carefulness.

## 3.2 Unintentional Third-Party Damage BN Model Algorithms

The Bayesian Network calculations are computed by the simulation software Agenarisk 7.0. A hybrid model was constructed through object-oriented interface containing discrete and continuous uncertain variables. The defined algorithms for unintentional third-party damage BN model is given be Table 9.

**Table 9. Define algorithms for unintentional third-party damage BN model**

| Node Name | Unique Identifier | Type | Defined Equation |
|---|---|---|---|
| Depth of Cover | DofCover | Fundamental Factor | Continuous interval; TNorm (80, 25) |
| Nature of Cover | NofCover | Fundamental Factor | Ranked (Normal, Enhanced, Excellent); TNorm (0.50, 0.1) |
| Population Density | Pop_Density | Fundamental Factor | Ranked (Very High, High, Medium, Low, Very Low); TNorm (0.8, 0.07) |
| Construction Activities | Cstr_Act | Fundamental Factor | Ranked (Very Frequent, Frequent, Medium, Rare, Very Rare); TNorm (0.75, 0.08) |
| Train and Vehicle | Train_Vehicle | Fundamental Factor | Ranked (Very High, High, Medium, Low, Very Low); TNorm (0.70, 0.05) |
| Other Buried Utilities | Other_B_U | Fundamental Factor | Ranked (Intensive, Moderate, None); TNorm (0.80, 0.04) |
| Wildlife Damage | Wild_Damage | Fundamental Factor | Ranked (High, Medium, Low); TNorm (0.70, 0.03) |
| Frequency | Freq | Fundamental Factor | Ranked (Less than once per month = 0.08, Less than four times per month = 0.12, One or two days per week = 0.30, Three or four days per week = 0.30, Daily = 0.20) |
| Thoroughness | Thoro | Fundamental Factor | Continuous interval; TNorm (80, 50) |
| Widely Advertised | Wide_Ad | Fundamental Factor | Ranked (Low = 0.05, Medium = 0.55, High = 0.40) |
| Standard Establishment & Enforcement | SEE | Fundamental Factor | Ranked (Poor, Below Average, Average, Good, Excellent); TNorm (0.88, 0.20) |

| Node Name | Unique Identifier | Type | Defined Equation |
|---|---|---|---|
| Appropriate Reactions | App_Rxn | Fundamental Factor | Ranked (Poor, Below Average, Average, Good, Excellent); TNorm (0.85, 0.10) |
| Level of Public Education | LofPub_Edu | Background Factors | Ranked (Very Low, Low, Medium, High, Very High); TNorm (0.70, 0.05) |
| Cover | Cover | Indicators | Cover = (DofCover + NofCover *100*0.3)/1.3 |
| Location | Location | Indicators | Location = (Pop_Density*3 + Cstr_Act*3 + Train_Vehicle + Other_B_U*2 + Wild_Damage)*100/10 |
| Plans and Technologies | P_T | Indicators | Ranked (None = 0.10, Prepared = 0.70, Well-prepared = 0.20) |
| Markers and Barriers | M_B | Indicators | Ranked (Poor, Below Average, Average, Good, Excellent); TNorm (0.90, 0.09) |
| Patrol | Patrol | Indicators | Patrol = (Freq*100 + Thoro)/2 |
| One-Call System | One_Call | Indicators | Icdt_Rep = (Wide_Ad*0.15 + SEE*0.30 + App_Rxn*0.55)*100 |
| 3rd Party Disturbance Index | TParty | Indexing Score | TParty = Cover*0.20 + Location*0.20 + Patrol*0.15 + One_Call*0.15 + M_B*100*0.1 + LofPub_Edu*100*0.15 + P_T*100*0.05 |
| Estimated Pipeline Failure Probability | Esti_Prob | Estimated Probability | Esti_Prob = 0.0362*/(1-TParty/100)/0.32 |

## 3.3 Unintentional Third-Party Damage BN Model Application

### Risk modeling

The purpose of this model is to analyze the pipeline risk posed by unintentional third-party interference, thereby forming an optimal risk management for control and mitigation. Having developed the framework of BN model on unintentional pipeline third-party damage analysis as described in previous sections, we can now focus on the actual steps for model application. The integration of relative risk scoring approach and quantitative risk assessment in this model makes it possible to estimate not only the relative risk, but a quantified probability of failure. The seven main risk variables (displayed as pink nodes in Figure 11) explained earlier in the chapter each contains various sub-factors (exhibited as blue nodes) that determine the magnitude of pipeline risk susceptibility from unintentional third-party intrusions. These main risk attributes then formed a holistic third-party disturbance index (shown in the yellow node) and built a network that coordinates cause-effect relationships as demonstrated in Figure 11. Moreover, this third-party disturbance index can be further converted to an absolute risk value by incorporating reliable historical data to obtain an estimated pipeline failure probability (presented in the green node).

**Data collection and preparation**

An accurate and meaningful pipeline risk assessment in large part depends on the quality and availability of data. Gathering the data means to achieve everything that relates to the pipeline. In this case, information includes origin construction data, environmental conditions, pipeline geological conditions, patrolling schedule and so on. If data is less straightforward or hard to access, expert judgement, empirical modeling and historical experience are alternatives to seek for solutions. Initial probability density functions were assumed and applied for the risk nodes in the model, which is shown in Table 9. The overall third-party disturbance risk score has an average value about 68 out of 100 (given by Figure 12) and the first quartile and third quartile are 64 and 72, respectively. Accordingly, the average of oil and gas pipeline failure probability due to third-party damage in the period of 2011-2015 is *0.0362 per 1000 mile-year*. Thus, a quantitative correlation between the risk index and estimated failure probability can be obtained and is listed in the last cell of Table 9.

**Segmentation**

Because risks are rarely constant along a pipeline, in industrial practice, pipeline is designed to be divided into segments that hold concurrent characteristics such as material, function and terrain. Each classified segment will be examined through such a risk model presented in this work with a series of relevant data being input (Figures 11 and 12) and will be ended up with a relative risk score based on their performance.

**Assessing risks**

In real case, with updated information in hand, we can input data to the nodes in this third-party risk model and generate a relative risk score as well as estimated probability of failure for that investigated pipeline segment. An example is given in Figure 13 when data is available on public education and one-call system nodes assuming local government had done excellent job in advertising public pipeline safety culture and establishing a sound one-call system. As inserting the observation into the sub-factor nodes of Level of Publication Education, Widely Advertised, Standard Establishment and Enforcement, and Appropriate Reactions, a higher performance scenario is formed with the mean value of 75 for third-party disturbance index and an estimated failure rate of *0.028 per 1000 mile-year*. This improvement in community excavation education and one-call system indeed has considerably reduced the risk from third-party interference. Similar risk assessing can be conducted following the same procedures.

**Managing risks**

A series of pipeline segments will undergo this type of risk model and create unique risk scores. In view of these scores, one can easily obtain the risk ranking based on the calculated results. The score order has huge significance that can benefit risk management when deciding how to allocate resource in the pipeline integrity program. In other words, knowing the different level of risks for each pipeline segment, we can prioritize the segments for patrolling and inspection, therefore, tailor a more suitable plan to control and mitigate the risks.

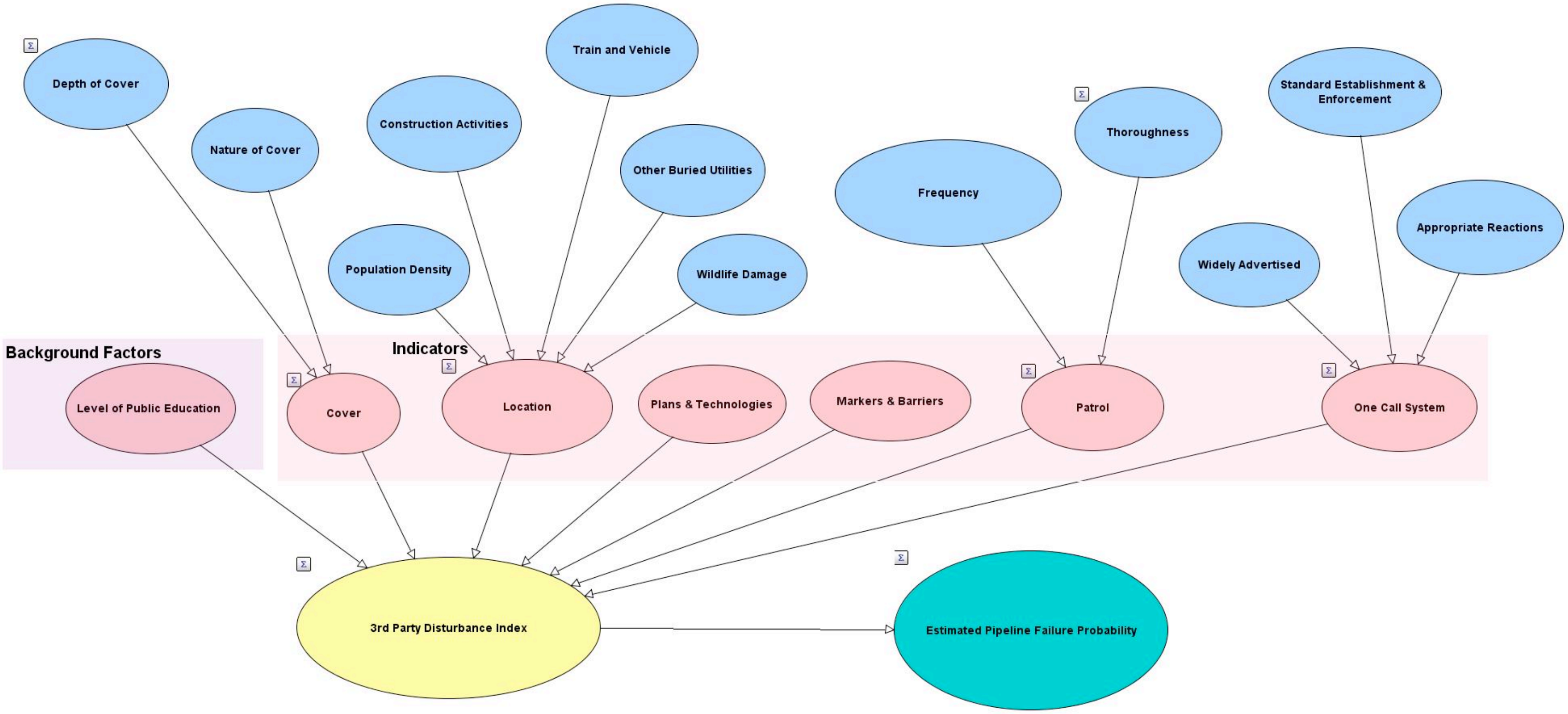
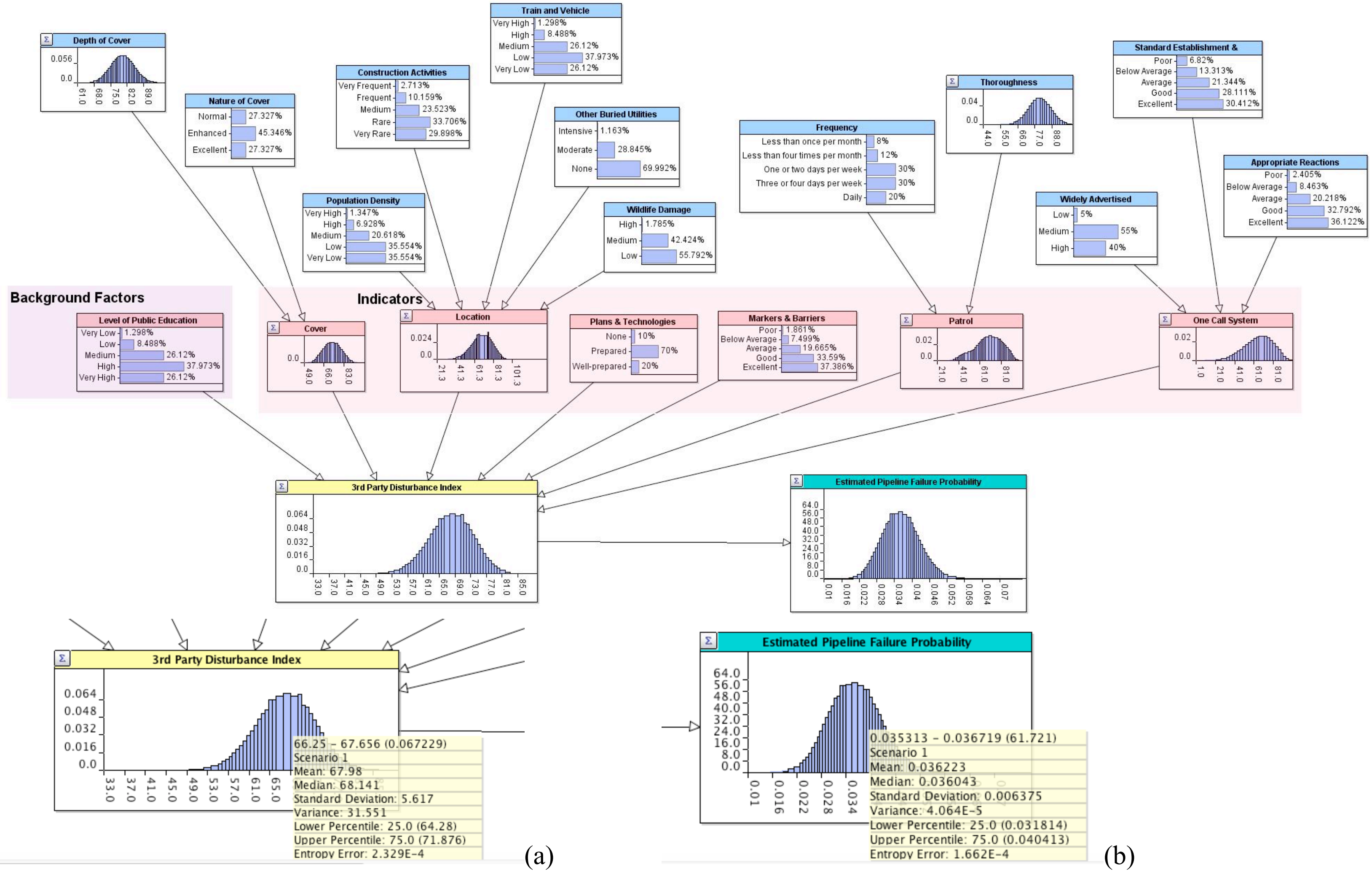


**Figure 11. Overview of unintentional third-party damage BN model**



(a)

```
66.25 - 67.656 (0.067229)
Scenario 1
Mean: 67.98
Median: 68.141
Standard Deviation: 5.617
Variance: 31.551
Lower Percentile: 25.0 (64.28)
Upper Percentile: 75.0 (71.876)
Entropy Error: 2.329E-4
```

(b)

```
0.035313 - 0.036719 (61.721)
Scenario 1
Mean: 0.036223
Median: 0.036043
Standard Deviation: 0.006375
Variance: 4.064E-5
Lower Percentile: 25.0 (0.031814)
Upper Percentile: 75.0 (0.040413)
Entropy Error: 1.662E-4
```

**Figure 12. Unintentional third-party damage BN model with initial data assumptions. (a) Statistics of 3$^{rd}$ Party Disturbance Index node. (b) Statistics of Estimated Pipeline Failure Probability node.**

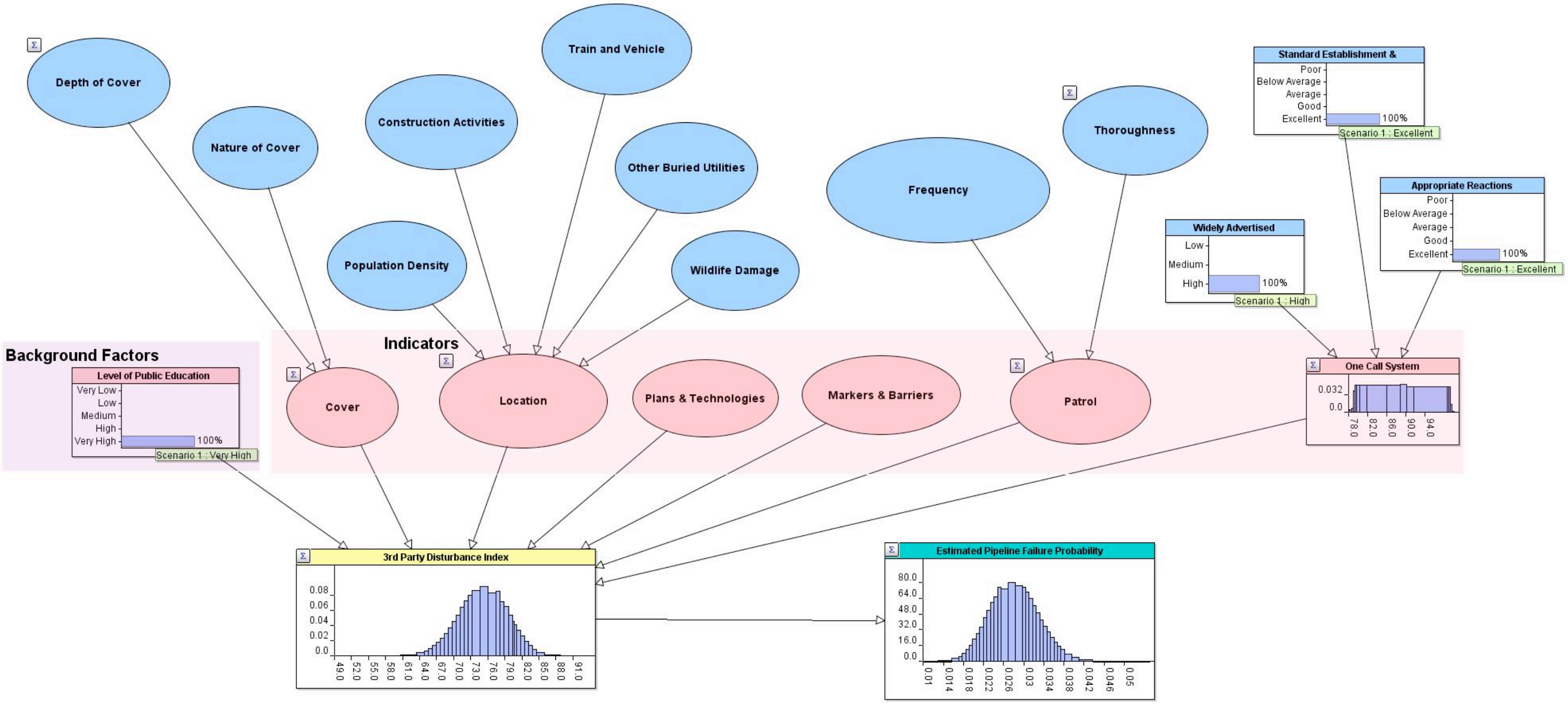


**Figure 13. Unintentional third-party damage BN model results given partial information of public education**

# 4. PIPELINE SECURITY ASSESSMENT WITH GAME THEORY

In the United States, the Office of Pipeline Safety (OPS) under the Department of Transportation (DOT) oversees the pipeline safety with regards to aspects such as corrosion, equipment failure and accidental third-party damage. The fact that numerous amount of oil and gas were carried over the U.S. by pipeline attracted the attention of pipeline industry and government who had made substantial investments each year to protect these systems against terror attacks or pilferage. At the same time, due to its economic status and inherent vulnerability of pipeline, the Transportation Security Administration (TSA) under the Department of Homeland Security (DHS) is continuously working on all fashions of transportation security including pipelines [50]. Though the two agencies have distinct missions on pipeline, some of the responsibilities are overlapping and have the same ultimate goal.

Similar to the allocation of government agencies, the traditional safety analysis together with a security related pipeline risk assessment should both be involved which are indispensable elements in a complete risk investigation. Since the malicious third-party interferences at most time are highly unpredictable and usually lead to very extreme consequences, the uncertainty and the risk generated by this pattern are gigantic. It should be noted that the threats from intentional third-party interferences differ from the accidental ones because of the intrinsic challenge from forecasting, and the complexation of chaotic psychology-based scenarios. On the contrary, the unintentional threats relying on tangible factors are able to formulate a model to characterize probabilities of failure and risks qualitatively and quantitatively. Thus, the conventional probabilistic risk assessment like previously elaborated in section three with Bayesian network evaluating accidental third-party damage on pipeline no longer applies here and, other alternative methods that can support decision-making for preventing or mitigating malicious interferences with security related heuristic algorithms are required.

### 4.1 Using Game-Theoretic Model for Pipeline Security Measurement

Industrial safety specialists and stakeholders are always struggling to yield a best trade-off between investment on protection systems of the infrastructure and the production costs. Questions like how to balance the finite recourses, how to allocate adequate safety and security investment have been raised frequently.

To deal with these problems on pipeline security, a security related game theory model is developed to sort out potentially messy scenarios and to support decisions for preventing or mitigating the adversarial acts throughout the administration and risk management in the government or industrial companies. This section will present this game-theoretic model for pipeline security measurement on intentional third-party damage to the property considering different levels of pipeline security risk and its own features.

To begin with, we need full knowledge on ourselves (pipeline security risk) and the enemies (targets of the terrorist) as the oldest version of game theory book, *the Art of War* by the Chinese Sun-Tzu goes that *if you know the enemy and know yourself, you need not fear the result of a hundred battles; if you know yourself but not the enemy, for* *every victory gained you will also suffer a defect; if you know neither the enemy nor yourself, you will succumb in every battle* [51].

**Clarify the aims and ideology for terrorists**

Terrorists tend to intentionally destroy pipelines resulting in release, fire and explosion and try to maximize the casualty, social chaos, disruptions and economic losses to grab attention of local or global authorities and to other political purposes.

**Define security risk level of pipeline based on location classification**

The pipeline security risk level is summarized in Table 10. Initially, the concept of location class (1, 2, 3 and 4) elaborated by 49 CFR Part 192 [52] (shown in the last two columns in Table 10) is aiming at identifying the pipeline characteristics as a basis for applying corresponding construction codes or standards, being able to decide how the integrity management program (IM) should be implemented and what will be the magnitude being implemented. In practice, during the design stage, one of the design factors (F) that provides a coefficient in the formula for steel pipe pressure design relies on the location classification and equals to 0.72 for Class 1 location, 0.60 for Class 2 location, 0.50 for Class 3 location and 0.40 for Class 4 location. The four classes actually depict the urbanization from more rural areas (class 1 or 2) to more urban regions (class 3 or 4).

**Table 10. Pipeline security risk level classification.**

| *i* | Security Level | Location | Description (49 CFR Part 192) [52] |
|---|---|---|---|
| **1** | Less vulnerable | Class1 | A Class 1 location is any 1-mile section of pipeline that has 10 or fewer buildings intended for human occupancy. This includes areas such as: Wastelands, Deserts, Rugged mountains, Grazing land, Farmland and Sparsely populated areas. |
| **2** | Moderately vulnerable | Class2 | This is any 1-mile section of pipeline that has more than 10 but fewer than 46 buildings intended for human occupancy. This includes fringe areas around cities and towns, industrial areas, and ranch or country estates. |
| **3** | Vulnerable | Class3 | This is any 1-mile section of pipeline that has 46 or more buildings intended for human occupancy except when a Class 4 Location prevails. This includes: Suburban housing developments, Shopping centers, Residential areas, Industrial areas and Other populated areas not meeting Class 4 Location requirements. |
| **4** | Highly vulnerable | Class4 | This is any 1-mile section of pipeline where multistory buildings are prevalent, traffic is heavy or dense, and where there may be numerous other utilities underground. Multistory means four or more floors above ground including the first, or ground, floor. The depth of basements or number of basement floors is immaterial. |

The pipeline security risk level is also highly correlated with the pipeline geography in view of both attackers and defenders. In fact, the philosophy of attackers is to maximize the total expected damage, which is inclined to have more people and facilities get involved. There is a higher probability for attackers to choose an area that multistory buildings are prevalent, traffic is dense and population is concentrated over a sparsely populated location. Therefore, it is reasonable to assign the same pipeline location class to the pipeline security risk level denoted by $i$ where $i = 1, 2, 3$ or 4. In this model, the pipeline security risk level is similarly divided into four categories in accordance with the four location classes: less vulnerable ($i = 1$), moderately vulnerable ($i = 2$), vulnerable ($i = 3$) and highly vulnerable ($i = 4$) as listed in the first two columns of Table 10. The increasing numeric value $i$ indicates the increasing intrinsic potential of pipeline being attacked and the degree of urbanization.

Although in this case, the pipeline security risk level is directly associated with geological factors in order to reduce the complexation, the pipeline security level should not be limited to only considering this aspect. It should be noted that additional factors such as the possible consequence of a pipeline incident occurred in the area, the real concentration of population and the facility used frequency cannot be ignored when comprehensively determining the risk level in the real-world. This criticality assessment is a part of security related risk analysis. Besides, the security risk level of a specific pipeline segment could not be taken for granted as a constant value in most cases. Derived from Gas Transmission and Distribution Pipeline Systems initial pipeline safety regulation (ASME B31.8 Location Class), the pipeline security risk level will change as the population grows or people moving out from the area that close to pipeline facilities, which updates the risk level $i$.

**Define players and possible strategy scales in the game-theoretic model**

Generally, in the game theoretic model players are strategic decision makers within the context of the game where a diametrically opposed conflict exists. It is clear that we have two players/sides within the game, defenders and attackers.

Player1 Defenders (D): government, public or private pipeline institution and industrial companies that ensure the safety and security of pipelines and make great efforts to mitigate incident consequences.

Player2 Attackers (A): vandal or/and terrorist that attack the pipeline to arise social panic for some political purposes.

The strategy is a complete plan of action that a player will take given a set of circumstances according to the game theory. We assert that for each pipeline security risk level, *i* where *i* = 1, 2, 3 or 4, both defenders and attackers have five levels of strategies marked as $D_{S1}$, $D_{S2}$, $D_{S3}$, $D_{S4}$, $D_{S5}$ and $A_{S1}$, $A_{S2}$, $A_{S3}$, $A_{S4}$, $A_{S5}$, respectively. The five-level scaled strategy system are inspired by the U.S. Homeland Security Advisory System which classified five-level alarms in response to a terrorist attack. The five colors (green, blue, yellow, orange and red) from the bottom to the top show an increasing terrorism alert from low risk to severe risk, which is demonstrated by Figure 14. Once released the alarm code, the U.S. government would take the corresponding action against the impending or occurred terrorist attack. In the same way, each strategy in this model for defenders ($D_{S1}$ to $D_{S5}$) and attackers ($A_{S1}$ to $A_{S5}$) triggers a series of countermeasures to confront the opponent, taking advantages of various resources including human resources, technologies, and industrial capability. The degree of allocating resources is no doubt associated with the specific scale in the serial strategies. Moreover, the detailed criteria and boundary conditions for the strategy levels should be defined case by case depending on the current scenario.

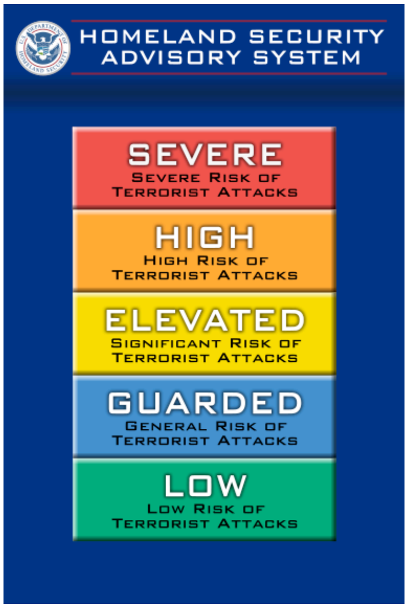

HOMELAND SECURITY
ADVISORY SYSTEM
SEVERE
Severe Risk of Terrorist Attacks
HIGH
High Risk of Terrorist Attacks
ELEVATED
Significant Risk of Terrorist Attacks
GUARDED
General Risk of Terrorist Attacks
LOW
Low Risk of Terrorist Attacks

**Figure 14. United States Department of Homeland Security Advisory System to terrorist attacks [53].**

**Apply the common ratio from contest success function** [54]:

$$P_i(A_i, D_i) = \frac{A_i}{A_i + \beta_i D_i} \quad (5)$$

$P_i$: probability of pipeline being successfully attacked by intentional damage (implying the chance that attackers win the game) given by specific pipeline security risk level *i*.

A$_i$ : strategies that an attacker may take under the condition of security risk level *i*.

D$_i$ : strategies that a defender may take under the condition of security risk level *i*.

$\beta_i$ : the relative defense/attack effectiveness ratio for pipeline security risk level $i$.

We can assume that $\beta_i$ follow the order: $\beta_1 > \beta_2 > \beta_3 > \beta_4$, which means that defense/attack effectiveness remain lowest in the case where pipeline located in densely populated areas and is very vulnerable according to the security risk level (*i*=4) while the less vulnerable security risk level (*i*=1) tends to be the easiest to defend. Symmetrically, $R_i$ is the resistance of the pipeline that survived through the damage under defender's protection (implying the chance that defenders win the game). The relationship between $R_i$ and $P_i$ is summarized by the below equation:

$$R_i = 1 - P_i \tag{6}$$

Thus, it's not hard to derive:

$$\partial P_i / \partial D_i \le 0 \tag{7}$$

$$\partial P_i / \partial A_i \ge 0 \tag{8}$$

or

$$\partial R_i / \partial D_i \ge 0 \tag{9}$$

$$\partial R_i / \partial A_i \le 0 \tag{10}$$

Ideally, supposing that the relative defense/attack effectiveness ratio $\beta_i$ equals to 1 and the attacker as well as the defender adopt the same level of strategies to contest, the outcome of $P_i$ or $R_i$ is 50%, which becomes a fair game. In other words, every action taking to attack or defend is sufficiently (100 %) effective while both parties have the same scale of countermeasures, so the chance to win (or lose) the game for each side is fifty-fifty. Unfortunately, in the real world, the pipeline protection game cannot have a 100% defense effectiveness.

**Utility function** [55]

$$\mathrm{v}_i = f_i + e_i + c \cdot h_i \tag{11}$$

where $\mathrm{v}_i$ is the expected loss index given by a successful attack composed of financial loss $f_i$, environmental damage $e_i$ and the human loss term $c \cdot h_i$. $h_i$ represents the accumulative human loss such as trauma, severe burns, respiratory impairment and fatality during an attack, and the coefficient c convert the overall human loss to the monetary index.

**Maximize the utility functions**

$$u(A, D) = \sum_{i}^{4} \{v_i \cdot [1 - P_i(A_i, D_i)]\text{-}\, b \cdot D_i\} \tag{12}$$

$$U(A, D) = \sum_{i}^{4} [v_i \cdot P_i(A_i, D_i)\text{-}B \cdot A_i] \tag{13}$$

In general, both players in the game are eager to maximizing the payoff as their ultimate goal. The attackers are apt to maximize the total expected damage while minimizing the costs of the action. Similarly, defenders are willing to maximize the assets that they have preserved from an attack subtracting the protection costs. The utility functions with regards to payoffs are illustrated in the above equations, and u(A, D) as well as U(A, D) represent the payoffs for defenders and attackers, respectively. b and B in these equations are the unit costs for defense and attack, respectively. Concerning the fact that the costs of protection are always much higher than the costs of an attack, we conclude that b >> B. How cheap is the cost of B? The Joint Improvised Explosive Device Defect Organization, a Pentagon organization has released an estimation of terrorist attack costs that provide us some monetary sense. An attack made by using a remote-controlled bomb is only about $400; a suicide bombing vest is $1200 and a suicide car bomb can vary between $13,000 and $20,000 depending on the car model [55]. Compared with the much lower cost of attack, the expenditures for blocking and fighting terrorism are no doubt many times over the attack costs.

**Data assumption and processing**

In principle, the main idea of developing this game theoretic model for defending malicious pipeline damage is to help tide up conditions with an array of factors and make decisions based on computed payoff values. In order to elaborate the model, some initial values are needed but may not be available from this standpoint. Therefore, a few data assumptions will be performed for further processing. Those piece of data can be replaced once the real data are available in practical cases.

Five sets of strategies are available for defender and attacker under various pipeline security risk level $i$, where $i = 1, 2, 3$ or 4. The scales regarding different sets of strategies are from 1 (low defending/attacking level) to 5 (severe defending/attacking level) shown in Table 11 while the level of countermeasures is expanded as the scale-point increasing. The assuming strategy scales are identical for both defender and attacker under the same security level of $i$. With five possible strategies in hand for each party, there are 25 pairs of strategy in total towards all pipeline security levels as indicated in Table 12.

**Table 11. Five sets of strategies for defender or attacker under various pipeline security risk levels.**

| Strategy | Security risk level | | | |
|---|---|---|---|---|
| | *i* = 1 | *i* = 2 | *i* = 3 | *i* = 4 |
| $D_{S1}/A_{S1}$ | 1 | 2 | 2 | 3 |
| $D_{S2}/A_{S2}$ | 1 | 2 | 3 | 4 |
| $D_{S3}/A_{S3}$ | 2 | 3 | 3 | 4 |
| $D_{S4}/A_{S4}$ | 2 | 3 | 4 | 5 |
| $D_{S5}/A_{S5}$ | 3 | 4 | 4 | 5 |

Having collected the levels of strategies, the probability of a successful malicious damage to pipeline $P_i(A_i, D_i)$ can be determined by plugging the defense/attack effectiveness $\beta_i$ . We suppose the defense/attack effectiveness $\beta_1$= 80% , $\beta_2$= 70% , $\beta_3$= 60% and $\beta_4$= 50% based on the nature of the four pipeline security levels as mentioned earlier in this section. Accordingly, the estimated probabilities of pipeline being successfully attacked by malicious damage are computed based on different strategy planning and are summarized in Table 13.

Furthermore, in the utility function, asserted values of financial loss $f_i$ , environmental damage $e_i$ and accumulative human loss $h_i$ are also listed in Table 14 for each pipeline security level *i*.

In our example, we also set c = 200 to transfer human loss to monetary index, b = 50 and B = 5 where b = 10B to express a sense of that the costs by defenders are always much higher than the costs by attackers. The exact values of above assumptions are subject to more discussion when approaching to the real scenarios, yet are beyond the scope of this research.

**Table 12. 25 pairs of strategy towards all pipeline security levels.**

| Obs | Strategy | D(*i*=1) | D(*i*=2) | D(*i*=3) | D(*i*=4) | A(*i*=1) | A(*i*=2) | A(*i*=3) | A(*i*=4) |
|---|---|---|---|---|---|---|---|---|---|
| **1** | $D_{S1}$ $A_{S1}$ | 1 | 2 | 2 | 3 | 1 | 2 | 2 | 3 |
| **2** | $D_{S1}$ $A_{S2}$ | 1 | 2 | 2 | 3 | 1 | 2 | 3 | 4 |
| **3** | $D_{S1}$ $A_{S3}$ | 1 | 2 | 2 | 3 | 2 | 3 | 3 | 4 |
| **4** | $D_{S1}$ $A_{S4}$ | 1 | 2 | 2 | 3 | 2 | 3 | 4 | 5 |
| **5** | $D_{S1}$ $A_{S5}$ | 1 | 2 | 2 | 3 | 3 | 4 | 4 | 5 |
| **6** | $D_{S2}$ $A_{S1}$ | 1 | 2 | 3 | 4 | 1 | 2 | 2 | 3 |
| **7** | $D_{S2}$ $A_{S2}$ | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| **8** | $D_{S2}$ $A_{S3}$ | 1 | 2 | 3 | 4 | 2 | 3 | 3 | 4 |
| **9** | $D_{S2}$ $A_{S4}$ | 1 | 2 | 3 | 4 | 2 | 3 | 4 | 5 |
| **10** | $D_{S2}$ $A_{S5}$ | 1 | 2 | 3 | 4 | 3 | 4 | 4 | 5 |
| **11** | $D_{S3}$ $A_{S1}$ | 2 | 3 | 3 | 4 | 1 | 2 | 2 | 3 |
| **12** | $D_{S3}$ $A_{S2}$ | 2 | 3 | 3 | 4 | 1 | 2 | 3 | 4 |
| **13** | $D_{S3}$ $A_{S3}$ | 2 | 3 | 3 | 4 | 2 | 3 | 3 | 4 |
| **14** | $D_{S3}$ $A_{S4}$ | 2 | 3 | 3 | 4 | 2 | 3 | 4 | 5 |
| **15** | $D_{S3}$ $A_{S5}$ | 2 | 3 | 3 | 4 | 3 | 4 | 4 | 5 |
| **16** | $D_{S4}$ $A_{S1}$ | 2 | 3 | 4 | 5 | 1 | 2 | 2 | 3 |
| **17** | $D_{S4}$ $A_{S2}$ | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 |
| **18** | $D_{S4}$ $A_{S3}$ | 2 | 3 | 4 | 5 | 2 | 3 | 3 | 4 |
| **19** | $D_{S4}$ $A_{S4}$ | 2 | 3 | 4 | 5 | 2 | 3 | 4 | 5 |
| **20** | $D_{S4}$ $A_{S5}$ | 2 | 3 | 4 | 5 | 3 | 4 | 4 | 5 |
| **21** | $D_{S5}$ $A_{S1}$ | 3 | 4 | 4 | 5 | 1 | 2 | 2 | 3 |
| **22** | $D_{S5}$ $A_{S2}$ | 3 | 4 | 4 | 5 | 1 | 2 | 3 | 4 |
| **23** | $D_{S5}$ $A_{S3}$ | 3 | 4 | 4 | 5 | 2 | 3 | 3 | 4 |
| **24** | $D_{S5}$ $A_{S4}$ | 3 | 4 | 4 | 5 | 2 | 3 | 4 | 5 |
| **25** | $D_{S5}$ $A_{S5}$ | 3 | 4 | 4 | 5 | 3 | 4 | 4 | 5 |

**Table 13. Estimated probability of pipeline failure due to malicious damage based on different strategy planning for all pipeline security levels.**

| Obs | Strategy | P(*i*=1) | P(*i*=2) | P(*i*=3) | P(*i*=4) |
|---|---|---|---|---|---|
| 1 | $D_{S1}$ $A_{S1}$ | 0.55556 | 0.58824 | 0.62500 | 0.66667 |
| 2 | $D_{S1}$ $A_{S2}$ | 0.55556 | 0.58824 | 0.71429 | 0.72727 |
| 3 | $D_{S1}$ $A_{S3}$ | 0.71429 | 0.68182 | 0.71429 | 0.72727 |
| 4 | $D_{S1}$ $A_{S4}$ | 0.71429 | 0.68182 | 0.76923 | 0.76923 |
| 5 | $D_{S1}$ $A_{S5}$ | 0.78947 | 0.74074 | 0.76923 | 0.76923 |
| 6 | $D_{S2}$ $A_{S1}$ | 0.55556 | 0.58824 | 0.52632 | 0.60000 |
| 7 | $D_{S2}$ $A_{S2}$ | 0.55556 | 0.58824 | 0.62500 | 0.66667 |
| 8 | $D_{S2}$ $A_{S3}$ | 0.71429 | 0.68182 | 0.62500 | 0.66667 |
| 9 | $D_{S2}$ $A_{S4}$ | 0.71429 | 0.68182 | 0.68966 | 0.71429 |
| 10 | $D_{S2}$ $A_{S5}$ | 0.78947 | 0.74074 | 0.68966 | 0.71429 |
| 11 | $D_{S3}$ $A_{S1}$ | 0.38462 | 0.48780 | 0.52632 | 0.60000 |
| 12 | $D_{S3}$ $A_{S2}$ | 0.38462 | 0.48780 | 0.62500 | 0.66667 |
| 13 | $D_{S3}$ $A_{S3}$ | 0.55556 | 0.58824 | 0.62500 | 0.66667 |
| 14 | $D_{S3}$ $A_{S4}$ | 0.55556 | 0.58824 | 0.68966 | 0.71429 |
| 15 | $D_{S3}$ $A_{S5}$ | 0.65217 | 0.65574 | 0.68966 | 0.71429 |
| 16 | $D_{S4}$ $A_{S1}$ | 0.38462 | 0.48780 | 0.45455 | 0.54545 |
| 17 | $D_{S4}$ $A_{S2}$ | 0.38462 | 0.48780 | 0.55556 | 0.61538 |
| 18 | $D_{S4}$ $A_{S3}$ | 0.55556 | 0.58824 | 0.55556 | 0.61538 |
| 19 | $D_{S4}$ $A_{S4}$ | 0.55556 | 0.58824 | 0.62500 | 0.66667 |
| 20 | $D_{S4}$ $A_{S5}$ | 0.65217 | 0.65574 | 0.62500 | 0.66667 |
| 21 | $D_{S5}$ $A_{S1}$ | 0.29412 | 0.41667 | 0.45455 | 0.54545 |
| 22 | $D_{S5}$ $A_{S2}$ | 0.29412 | 0.41667 | 0.55556 | 0.61538 |
| 23 | $D_{S5}$ $A_{S3}$ | 0.45455 | 0.51724 | 0.55556 | 0.61538 |
| 24 | $D_{S5}$ $A_{S4}$ | 0.45455 | 0.51724 | 0.62500 | 0.66667 |
| 25 | $D_{S5}$ $A_{S5}$ | 0.55556 | 0.58824 | 0.62500 | 0.66667 |

**Table 14. Associated values of financial loss, environmental damage and accumulative human loss under various pipeline security risk levels.**

| Parameters | Security risk level | | | |
|---|---|---|---|---|
| | $i = 1$ | $i = 2$ | $i = 3$ | $i = 4$ |
| $\boldsymbol{f_i}$ | 100 | 200 | 300 | 400 |
| $\boldsymbol{e_i}$ | 120 | 90 | 60 | 30 |
| $\boldsymbol{h_i}$ | 5 | 15 | 25 | 35 |

With the associated values in Table 14 and equation 11, the utility functions in terms of each pipeline security risk level can be easily calculated. The holistic payoffs for defender and attacker can then be obtained via equations 12 and 13, respectively and the results are demonstrated in Table 15.

All the computations of the model were conducted by SAS (Statistical Analysis Solution) software which can conveniently manage vast quantity of data and perform predictive analysis. In more practical cases, the amount of data might increase exponentially when putting additional factors into the calculation. Because of this, it is overwhelmingly essential to use external data manipulating software to help efficiently accomplish the task. SAS (r) Proprietary Software 9.4 (TS1M3) licensed to TEXAS A&M UNIVERSITY - SFA T&R, Site 70080787 is executed on the X64_8PRO platform with V9 Engine. The code and data log of this model programming will be attached in the appendix at the end of this thesis.

**Table 15. Summarized utility function based on different pairs of strategies for all pipeline security levels.**

| Obs | Strategy | u(i=1) | u(i=2) | u(i=3) | u(i=4) | U(i=1) | U(i=2) | U(i=3) | U(i=4) | u(A,D) | U(A,D) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **1** | $D_{S1}$ $A_{S1}$ | 492 | 1255 | 1910 | 2327 | 673 | 1925 | 3340 | 4938 | 5984 | 10876 |
| **2** | $D_{S1}$ $A_{S2}$ | 492 | 1255 | 1431 | 1876 | 673 | 1925 | 3814 | 5384 | 5055 | 11795 |
| **3** | $D_{S1}$ $A_{S3}$ | 299 | 947 | 1431 | 1876 | 861 | 2228 | 3814 | 5384 | 4553 | 12287 |
| **4** | $D_{S1}$ $A_{S4}$ | 299 | 947 | 1137 | 1565 | 861 | 2228 | 4103 | 5690 | 3947 | 12883 |
| **5** | $D_{S1}$ $A_{S5}$ | 207 | 753 | 1137 | 1565 | 948 | 2417 | 4103 | 5690 | 3661 | 13159 |
| **6** | $D_{S2}$ $A_{S1}$ | 492 | 1255 | 2389 | 2772 | 673 | 1925 | 2811 | 4443 | 6908 | 9852 |
| **7** | $D_{S2}$ $A_{S2}$ | 492 | 1255 | 1860 | 2277 | 673 | 1925 | 3335 | 4933 | 5884 | 10866 |
| **8** | $D_{S2}$ $A_{S3}$ | 299 | 947 | 1860 | 2277 | 861 | 2228 | 3335 | 4933 | 5382 | 11358 |
| **9** | $D_{S2}$ $A_{S4}$ | 299 | 947 | 1513 | 1923 | 861 | 2228 | 3677 | 5282 | 4682 | 12048 |
| **10** | $D_{S2}$ $A_{S5}$ | 207 | 753 | 1513 | 1923 | 948 | 2417 | 3677 | 5282 | 4396 | 12324 |
| **11** | $D_{S3}$ $A_{S1}$ | 651 | 1535 | 2389 | 2772 | 464 | 1595 | 2811 | 4443 | 7347 | 9313 |
| **12** | $D_{S3}$ $A_{S2}$ | 651 | 1535 | 1860 | 2277 | 464 | 1595 | 3335 | 4933 | 6323 | 10327 |
| **13** | $D_{S3}$ $A_{S3}$ | 442 | 1205 | 1860 | 2277 | 668 | 1920 | 3335 | 4933 | 5784 | 10856 |
| **14** | $D_{S3}$ $A_{S4}$ | 442 | 1205 | 1513 | 1923 | 668 | 1920 | 3677 | 5282 | 5083 | 11547 |
| **15** | $D_{S3}$ $A_{S5}$ | 324 | 983 | 1513 | 1923 | 781 | 2137 | 3677 | 5282 | 4743 | 11877 |
| **16** | $D_{S4}$ $A_{S1}$ | 651 | 1535 | 2724 | 3127 | 464 | 1595 | 2426 | 4038 | 8037 | 8523 |
| **17** | $D_{S4}$ $A_{S2}$ | 651 | 1535 | 2182 | 2608 | 464 | 1595 | 2963 | 4552 | 6976 | 9574 |
| **18** | $D_{S4}$ $A_{S3}$ | 442 | 1205 | 2182 | 2608 | 668 | 1920 | 2963 | 4552 | 6437 | 10103 |
| **19** | $D_{S4}$ $A_{S4}$ | 442 | 1205 | 1810 | 2227 | 668 | 1920 | 3330 | 4928 | 5684 | 10846 |
| **20** | $D_{S4}$ $A_{S5}$ | 324 | 983 | 1810 | 2227 | 781 | 2137 | 3330 | 4928 | 5344 | 11176 |
| **21** | $D_{S5}$ $A_{S1}$ | 711 | 1719 | 2724 | 3127 | 354 | 1361 | 2426 | 4038 | 8281 | 8179 |
| **22** | $D_{S5}$ $A_{S2}$ | 711 | 1719 | 2182 | 2608 | 354 | 1361 | 2963 | 4552 | 7220 | 9230 |
| **23** | $D_{S5}$ $A_{S3}$ | 515 | 1388 | 2182 | 2608 | 545 | 1687 | 2963 | 4552 | 6694 | 9746 |
| **24** | $D_{S5}$ $A_{S4}$ | 515 | 1388 | 1810 | 2227 | 545 | 1687 | 3330 | 4928 | 5940 | 10490 |
| **25** | $D_{S5}$ $A_{S5}$ | 392 | 1155 | 1810 | 2227 | 663 | 1915 | 3330 | 4928 | 5584 | 10836 |

**Model Outcome: Simultaneous Manner (Payoff matrix)**

One way to examine the game is inspecting it in a simultaneous fashion supposing both involved players have no clue to the other's strategy choice. In other words, government or pipeline companies have no indication about what attack scale will be, at the same time, the pipeline attackers lack the suggestive information on how the countermeasures the opponent will take. Typically, the payoff matrix is a predominant way to study this game mode.

Once gained the computed utility functions for defender [u(A, D)] and attacker [U(A, D)] under different combinations of strategies (implied in the last two columns of Table 15), the payoff matrix can be framed as a handy understanding representation shown in Table 16. Similar to the payoff matrix in the Prisoner's Dilemma example, the row exhibited the five possible strategies for one party: attacker, while the column presented the five possible strategies for the other party: defender. Each cell in the matrix shown pair-wisely in parentheses reports the payoffs of the defender and the attacker, respectively. By performing Nash Equilibrium that no player has a reason to choose a better action given that the other component adheres to a strategic profile of the game, a steady state can be reached as a solution for the game assuming both players are rational and intelligent to choose a correct action. After the application of the theory, the payoff result of $D_{S5}$ $A_{S5}$ with the value of (5584, 10836) indicates the equilibrium for this game and is displayed in bold in Table 16.

Despite the idealized setting that all players are rational and logical, the outcome from Nash Equilibrium under this setting still provides us insights to solve the problem and make decisions by giving a stady state solution. In a simultaneous game, each player formulates independent thinking without extra information on the tendency of the other's choice. In general, a good first step is to figure out the payoffs of all the players in the game, and then put yourself in the opponent's shoes, to attempt to predict what they will do. In the game of secure pipeline, attackers are aiming at maximizing their utilities to generate chaos as much as they can by setting attack level to the highest scale. From the perspective of pipeline defenders, they are able to recognize the opponents' philosophy and escalate the scale of prevention and mitigation to the highest level in response to the proposed attackers' behavior. Thus, under the isolated planning, attacker will tend to choose the highest level of strategy $A_{S5}$ while defender will tend to adopt the most intensive level of strategy $D_{S5}$, which is in line with the results of Nash Equilibrium.

**Table 16. Payoff matrix based on different pairs of strategies.**

| u \ U | $A_{S1}$ | $A_{S2}$ | $A_{S3}$ | $A_{S4}$ | $A_{S5}$ |
|---|---|---|---|---|---|
| $D_{S1}$ | (5984, 10876) | (5055, 11795) | (4553, 12287) | (3947, 12883) | (3661, 13159) |
| $D_{S2}$ | (6908, 9852) | (5884, 10866) | (5382, 11358) | (4682, 12048) | (4396, 12324) |
| $D_{S3}$ | (7347, 9313) | (6323, 10327) | (5784, 10856) | (5083, 11547) | (4743, 11877) |
| $D_{S4}$ | (8037, 8523) | (6976, 9574) | (6437, 10103) | (5684, 10846) | (5344, 11176) |
| $D_{S5}$ | (8281, 8179) | (7220, 9230) | (6694, 9746) | (5940, 10490) | **(5584, 10836)** |

The payoff pairs are then plotted in Figure 15 where the utility functions of attacker shown in orange line are mostly upwards and defender's payoffs shown in blue line are mostly downwards. This distribution of payoffs is mostly in good accordance with the real-world situations where pipeline defenders invest tons of resources in fighting against attackers and taking accountability to prevent the occurrence of incidents. However, perhaps at some point when attackers take a relatively lower level of strategy and defenders adopt a higher protection level, defenders can defect over attackers and abort the vandalism. In fact, there are some exemplary cases that defenders effectively ceased the deliberate damage with the right strategy combinations just like the cross point in figure 15.

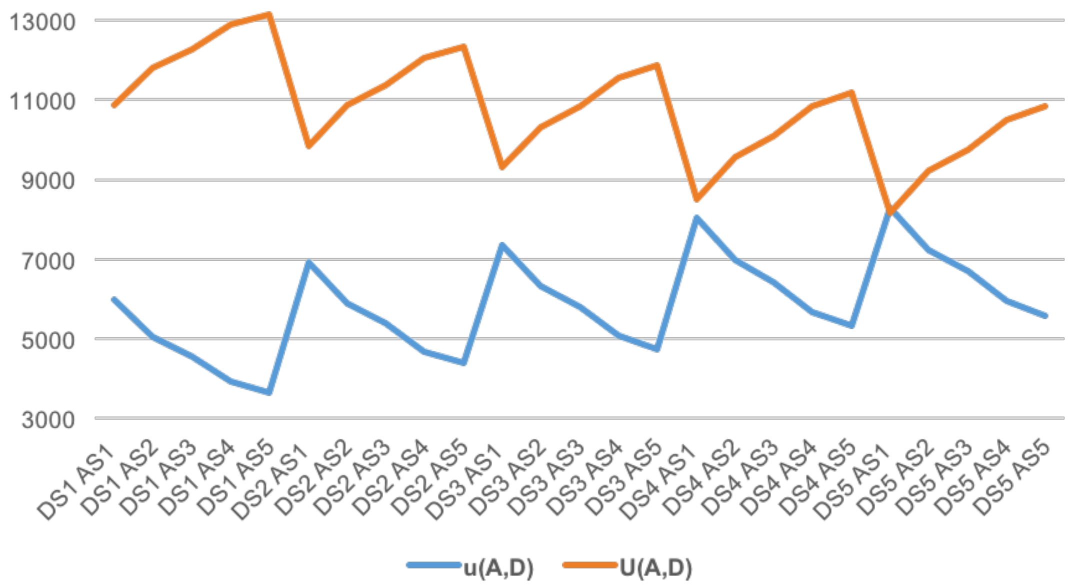


**Figure 15. Defender's [u(A,D)] vs. attacker's [U(A,D)] payoff summary.**

**Model Outcome: Sequential Manner (Extensive decision tree)**

In addition to simultaneous game mode, sequential mode is commonly used in an investigation where one player first made a strategy. To explicitly express the scenarios and solve the game, the backward induction method [56] is used by analyzing the extensive representation which is exhibited in Figure 16. Let's assume the government or pipeline company starts to play strategy first, and the pairwise of payoffs are listed at the bottom of the decision tree in Figure 16. With the application of backward induction, it is credible for the latter player, attackers to select $A_{S5}$ under each of tree branch of $D_{S1}$, $D_{S2}$, $D_{S3}$, $D_{S4}$ and $D_{S5}$ since the payoff of $A_{S5}$ has the highest value. With that noted, the passive player, defenders at the starting stage would, therefore, prefer to choose $D_{S5}$ to react to attackers' "future" decision and to minimize his disutility and the consequence [55]. The credible sequential route is highlighted in bold shown in Figure 16.

## 4.2 Game-Theoretic Model Discussion

The probability and consequence scale of intentional damage to pipelines are difficult to predict and evaluate, largely because of the uncertainty of human psychology, making it almost inaccessible via conventional risk assessment tools like fault tree analysis. However, the game-theoretic model can clarify the ambiguity by computing payoffs, sorting out possible scenarios and applying theory to reach equilibrium and provide credible action. Knowing the nature of all the players in the game can forecast potential behaviors and thus help us to select the best strategy in different situations.

In the pipeline secure game or other similar infrastructure protection game, regardless of budget limitation, attackers or defenders without context are anticipated to choose the highest level of strategy to maximize their utility functions expanding (from the views of attackers) or diminishing (from the views of defenders) the damage as much as possible no matter it's a simultaneous mode or sequential mode. This imitative manner that players are copying the strategy level from their opponent is in agreement with the reality. For instance, the way that U.S. Security Advisory System against a terrorist attack is to address a similar level of countermeasures to combat the terrorism.

This game-theoretic model for intentional damage on pipeline aims to establish a framework that considers a number of facets including the nature of pipeline infrastructure, attack/protection effectiveness, possible levels of strategies, overall losses and gaming philosophy. The payoff values based on assumptions are changeable once being applied in a real case. It should be stressed that other essential elements such as economic factor will also have an impact on the final strategy decisions. With all the information in hand, equilibrium points will be very suggestive in assigning credible pathway of the game and people can refer the model basis to take appropriate action.

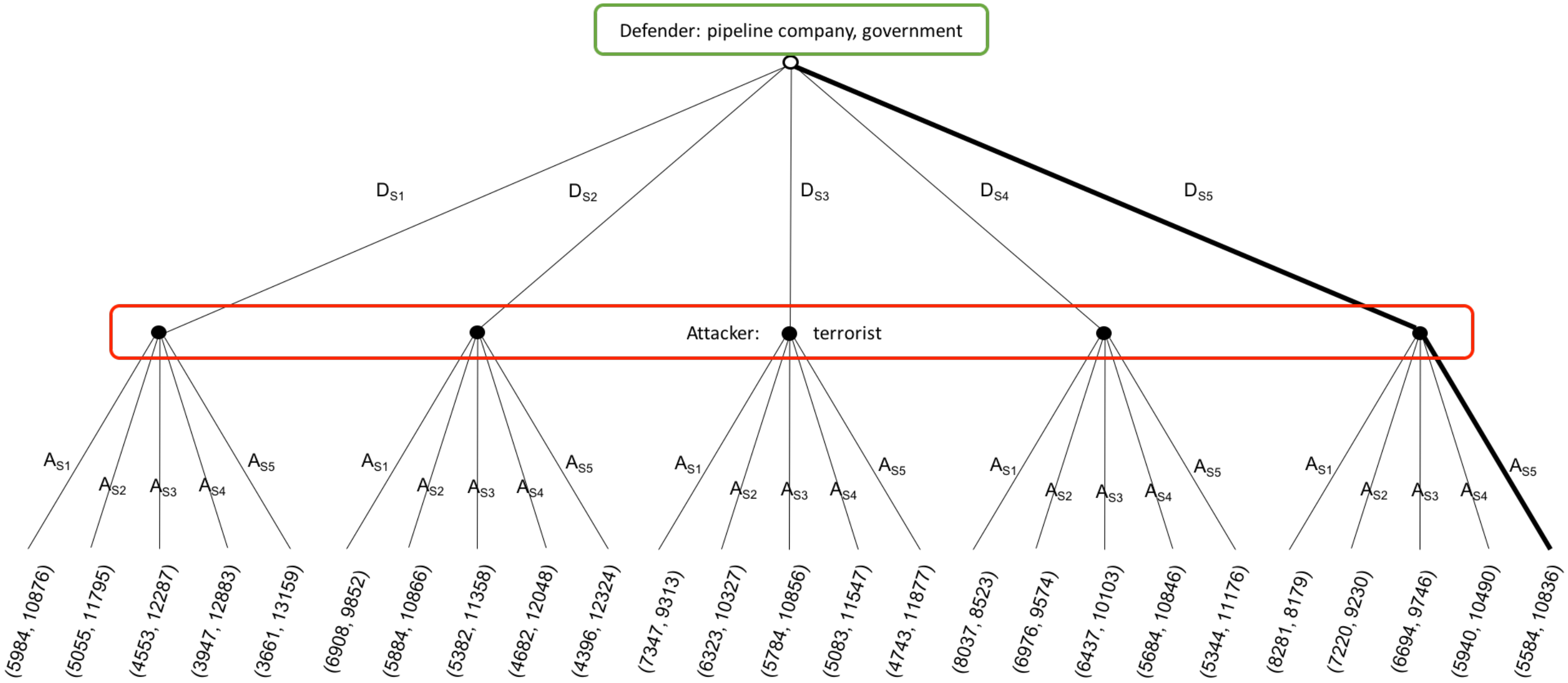


**Figure 16. Extensive form of game-theoretic model for intentional third-party damage on pipeline.**

# 5. CONCLUSIONS AND FUTURE WORKS

The pipeline third-party interference can be divided into unintentional disturbance and malicious sabotage. This failure mode is usually one of the least factors being considered during the pipeline hazard assessment stage despite the substantial portion contributing to the total number of oil and gas pipeline incident. This is because of the intrinsic risk assessment challenge. A probabilistic risk analysis is hard to model human actions and cannot be applied to intentional acts. Due to the distinctive motivation of third-party damage, an unintentional third-party damage BN model and a game-theoretic model were therefore built to examine the mechanism of pipeline failure caused by third-party damage.

The unintentional third-party damage BN model coupled the methods of relative risk scoring and quantitative risk assessment targeting to clarify the cause-effect relationship of unintentional third-party damage and quantify the failure probability simultaneously under this type of failure mode without loss flexibility. Set of assumptions are made for prior probabilities to allow initial computation and analysis of the study. Real data once available, can be inserted as observations to obtain more practical results that can reveal the risk ranking among pipeline segments and be suggestive for future risk mitigation resource allocation.

In order to get good insights into adversarial acts to pipeline third-party damage, a game-theoretic model is developed by understanding attack ideology, defining risk security level, and sorting out possible strategies and scenarios for each party.

In conclusion, this work provides a better understanding in pipeline third-party intrusion mechanism and developed two practical risk assessment models for industry to perform associated risk analysis based on different motivations.

Though third-party damage plays a critical role in pipeline failure modes, probabilistic studies on other aspects such as corrosion, equipment failure and incorrect operations out of the seven major causes are recommended to be investigated by Bayesian Network model in the future. The incorporation of the corresponding models can develop a more holistic pipeline failure analysis network for industrial use.

In addition to the probabilistic study, risk-based consequence analysis is also suggested to be a continuation study with a number of physical modeling being integrated (Gaussian plume, Thermal radiation flux model and Overpressure model) to compute and estimate the outcome in a pipeline incident, giving rise to fulfill an overall risk assessment of pipeline.

Another possible future work on this topic can be assigned to use the game-theoretic model to simulate malicious attacks by pilferage while improving the evaluation of countermeasures against terrorism or pilferage since measures that prevent a specific event from occurring can simply make terrorists or stealers shift their tactics from more resistant targets to more vulnerable ones. The existing model in this work hence can be modified to apply to the case of pilferage as well as implement more complicated strategies to meet scenarios in a more realistic world.

# REFERENCES

[1] "Safety Study: Integrity Management of Gas Transmission Pipelines in High Consequence Areas," National Transportation Safety Board 2015.

[2] "Basic petroelum data book, petroleum industry statistics " American Petroleum Institute 2015, vol. 35.

[3] U.S. Energy Information Administration (2017). *Weekly Petroleum Status Report*.

[4] U.S. Energy Information Administration (2017). *Monthly crude oil and natural gas production*.

[5] Pipeline and Hazardous Materials Safety Administration (2017). *Pipeline incident 20 year trends*.

[6] Y. Zhu, X.-m. Qian, Z.-y. Liu, P. Huang, and M.-q. Yuan, "Analysis and assessment of the Qingdao crude oil vapor explosion accident: Lessons learnt," *Journal of Loss Prevention in the Process Industries,* vol. 33, pp. 289-303, 2015.

[7] U.S. Department of Transporation Pipeline and Hazardous Materials Safety Administration, *Gas Transmission Integrity Management: Fact Sheet* (2004).

[8] M. S. Mannan, R. A. Mentzer, and J. Zhang, "Framework for creating a Best-in-Class safety culture," *Journal of Loss Prevention in the Process Industries,* vol. 26, no. 6, pp. 1423-1432, 2013.

[9] U.S. Department of Transporation Pipeline and Hazardous Materials Safety Administration*, Incident Report Form, FormF7100.2*.

[10] A. S. Markowski and M. S. Mannan, "Fuzzy risk matrix," *Journal of hazardous materials,* vol. 159, no. 1, pp. 152-157, 2008.

[11] S. Mannan, *Lees' loss prevention in the process industries*. Butterworth-Heinemann, 2005.

[12] B. Ruge, "Risk matrix as tool for risk assessment in the chemical process industries," in *Probabilistic Safety Assessment and Management*, 2004, pp. 2693-2698: Springer.

[13] H. Ni, A. Chen, and N. Chen, "Some extensions on risk matrix approach," *Safety Science,* vol. 48, no. 10, pp. 1269-1278, 2010.

[14] L. Xing and S. V. Amari, "Fault tree analysis," in *Handbook of performability engineering*: Springer, 2008, pp. 595-620.

[15] W.-S. Lee, D. L. Grosh, F. A. Tillman, and C. H. Lie, "Fault Tree Analysis, Methods, and Applications A Review," *IEEE transactions on reliability,* vol. 34, no. 3, pp. 194-203, 1985.

[16] G. E. Apostolakis, "How useful is quantitative risk assessment?," *Risk analysis,* vol. 24, no. 3, pp. 515-520, 2004.

[17] M. F. D'Atri, D. Rodriguez, and R. García-Martínez, "Improving pipeline risk models by using data mining techniques," in *24th World Gas Conference Proceedings CD. Paper*, 2009, vol. 663.

[18] R. Palmer-Jones, S. Turner, and P. Hopkins, "A new approach to risk based pipeline integrity management," in *2006 International Pipeline Conference*, 2006, pp. 811-823: American Society of Mechanical Engineers.

[19] Y.-D. Jo and B. J. Ahn, "A method of quantitative risk assessment for transmission pipeline carrying natural gas," *Journal of hazardous materials,* vol. 123, no. 1, pp. 1-12, 2005.

[20] Z. Han and W. Weng, "An integrated quantitative risk analysis method for natural gas pipeline network," *Journal of Loss Prevention in the Process Industries,* vol. 23, no. 3, pp. 428-436, 2010.

[21] Z. Han and W. Weng, "Comparison study on qualitative and quantitative risk assessment methods for urban natural gas pipeline network," *Journal of Hazardous Materials,* vol. 189, no. 1, pp. 509-518, 2011.

[22] M. J. Gharabagh, H. Asilian, S. Mortasavi, A. Z. Mogaddam, E. Hajizadeh, and A. Khavanin, "Comprehensive risk assessment and management of petrochemical feed and product transportation pipelines," *Journal of Loss Prevention in the Process Industries,* vol. 22, no. 4, pp. 533-539, 2009.

[23] M. Dziubiński, M. Frątczak, and A. Markowski, "Aspects of risk analysis associated with major failures of fuel pipelines," *Journal of Loss Prevention in the Process Industries,* vol. 19, no. 5, pp. 399-408, 2006.

[24] D. Yuhua and Y. Datao, "Estimation of failure probability of oil and gas transmission pipelines by fuzzy fault tree analysis," *Journal of loss prevention in the process industries,* vol. 18, no. 2, pp. 83-88, 2005.

[25] P. K. Dey, "Analytic hierarchy process analyzes risk of operating cross-country petroleum pipelines in India," *Natural Hazards Review,* vol. 4, no. 4, pp. 213-221, 2003.

[26] E. Cagno, F. Caron, M. Mancini, and F. Ruggeri, "Using AHP in determining the prior distributions on gas pipeline failures in a robust Bayesian approach," *Reliability Engineering & System Safety,* vol. 67, no. 3, pp. 275-284, 2000.

[27] P. K. Dey, "An integrated assessment model for cross-country pipelines," *Environmental Impact Assessment Review,* vol. 22, no. 6, pp. 703-721, 2002.

[28] A. Jamshidi, A. Yazdani-Chamzini, S. H. Yakhchali, and S. Khaleghi, "Developing a new fuzzy inference system for pipeline risk assessment," *Journal of loss prevention in the process industries,* vol. 26, no. 1, pp. 197-208, 2013.

[29] A. S. Markowski and M. S. Mannan, "Fuzzy logic for piping risk assessment (pfLOPA)," *Journal of loss prevention in the process industries,* vol. 22, no. 6, pp. 921-927, 2009.

[30] W. K. Muhlbauer, *Pipeline risk management manual: ideas, techniques, and resources*. Gulf Professional Publishing, 2004.

[31] O. Shabarchin and S. Tesfamariam, "Internal corrosion hazard assessment of oil & gas pipelines using Bayesian belief network model," *Journal of Loss Prevention in the Process Industries,* vol. 40, pp. 479-495, 2016.

[32] F. Ayello, S. Jain, N. Sridhar, and G. Koch, "Quantitive Assessment of Corrosion Probability-A Bayesian Network Approach," *Corrosion,* vol. 70, no. 11, pp. 1128-1147, 2014.

[33] I. Dmytrakh, "Corrosion fatigue cracking and failure risk assessment of pipelines," in *Safety, Reliability and Risks Associated with Water, Oil and Gas Pipelines*: Springer, 2008, pp. 99-113.

[34] J. ZENG, J.-c. XU, G.-h. CHEN, and J.-b. YUAN, "Applicability of Risk Assessment Method for Urban Buried Gas Pipeline [J]," *Gas & Heat,* vol. 5, pp. 55-61, 2007.

[35] K. Lawson, "Pipeline corrosion risk analysis-an assessment of deterministic and probabilistic methods," *Anti-Corrosion Methods and Materials,* vol. 52, no. 1, pp. 3-10, 2005.

[36] F. Caleyo, J. Gonzalez, and J. Hallen, "A study on the reliability assessment methodology for pipelines with active corrosion defects," *International Journal of Pressure Vessels and Piping,* vol. 79, no. 1, pp. 77-86, 2002.

[37] Y. Cao, X. Sun, S. Zhang, and S. Xue, "Field experiments and FEM analysis of third-party damaged oil transmission pipeline," *Engineering Failure Analysis,* vol. 17, no. 1, pp. 344-352, 2010.

[38] A. Adebayo and A. Dada, "An Evaluation of the causes of oil pipeline incidents In Oil and Gas Industries in Niger Delta Region of Nigeria," *J. Eng. Applied Sci,* vol. 3, no. 3, pp. 279-281, 2008.

[39] J. Mather, C. Blackmore, A. Petrie, and C. Treves, "An assessment of measures in use for gas pipelines to mitigate against damage caused by third party activity," *HSE Contract Research Report,* 2001.

[40] W. Liang, J. Hu, L. Zhang, C. Guo, and W. Lin, "Assessing and classifying risk of pipeline third-party interference based on fault tree and SOM," *Engineering Applications of Artificial Intelligence,* vol. 25, no. 3, pp. 594-608, 2012.

[41] N. Fenton and M. Neil, *Risk assessment and decision analysis with Bayesian networks*. CRC Press, 2012.

[42] J. V. Stone, *Bayes' rule: a tutorial introduction to Bayesian analysis*. Sebtel Press, 2013.

[43] H. Pasman and W. Rogers, "How can we use the information provided by process safety performance indicators? Possibilities and limitations," *Journal of Loss Prevention in the Process Industries,* vol. 30, pp. 197-206, 2014.

[44] N. Khakzad, F. Khan, and P. Amyotte, "Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network," *Process Safety and Environmental Protection,* vol. 91, no. 1, pp. 46-53, 2013.

[45] R. B. Myerson, *Game theory*. Harvard university press, 2013.

[46] J. Von Neumann and O. Morgenstern, *Theory of games and economic behavior*. Princeton university press, 2007.

[47] A. K. Dixit and S. Skeath, *Games of Strategy: Fourth International Student Edition*. WW Norton & Company, 2015.

[48] "Pipeline Security Guidelines," Transportation Security Administration2011.

[49] "One-Call Systems," *Pipeline Digest,* March 1991.

[50] P. W. Parfomak, "Pipeline security: An overview of federal activities and current policy issues," 2004: DTIC Document.

[51] Sun-Tzu, *The Art of War*. Simon & Brown, 2014.

[52] U. DOT, "CFR Part 192, Transportation of Natural and Other Gas by Pipeline: Minimum Federal Safety Standards. 2004," *Washington, DC: US Dept. of Transportation*.

[53] P. (talk). (2008). *United States Department of Homeland Security - Hsas-chart.jpg, Public Domain*.

[54] S. Skaperdas, "Contest success functions," *Economic theory,* vol. 7, no. 2, pp. 283-290, 1996.

[55] L. Talarico, G. Reniers, K. Sörensen, and J. Springael, "MISTRAL: A game-theoretic model to allocate security measures in a multi-modal chemical transportation network with adaptive adversaries," *Reliability Engineering & System Safety,* vol. 138, pp. 105-114, 2015.

[56] J. N. Webb, *Game theory: decisions, interaction and Evolution*. Springer Science & Business Media, 2007.

# APPENDIX A

```
NOTE: SAS (r) Proprietary Software 9.4 (TS1M3)
     Licensed to TEXAS A&M UNIVERSITY - SFA T&R, Site 70080787.
NOTE: This session is executing on the X64_8PRO  platform.



NOTE: Updated analytical products:

     SAS/STAT 14.1
     SAS/ETS 14.1
     SAS/OR 14.1
     SAS/IML 14.1
     SAS/QC 14.1

NOTE: Additional host information:

 X64_8PRO WIN 6.2.9200  Workstation

NOTE: SAS initialization used:
     real time           2.43 seconds
     cpu time            1.79 seconds

1    libname model1 'C:\Users\Yan\Documents\my SAS folders\game theory model\payoff.xlsx';
NOTE: Libref MODEL1 was successfully assigned as follows:
     Engine:        EXCEL
     Physical Name: C:\Users\Yan\Documents\my SAS folders\game theory model\payoff.xlsx
2    libname cyemotiu 'C:\Users\Yan\Documents\my SAS folders\game theory model';
NOTE: Libref CYEMOTIU was successfully assigned as follows:
     Engine:        V9
     Physical Name: C:\Users\Yan\Documents\my SAS folders\game theory model
3
4    data cyemotiu.sim(drop=i beta_1-beta_4 v1-v4);
5       set model1.'simultaneous$'n;
6       array D{4} D1-D4;
7       array A{4} A1-A4;
8       array beta{4} beta_1-beta_4;
9       array prob{4} prob1-prob4;
10      array v{4} v1-v4;
11      array ud{4} ud1-ud4;
12      array ua{4} ua1-ua4;
13         do i=1 to 4;
14            prob{i}=A{i}/(A{i}+beta{i}*D{i});
15            ud{i}=v{i}*(1-prob{i})-50*D{i};
16            ua{i}=v{i}*prob{i}-5*A{i};
17         end;
18      udtotal=sum(ud1,ud2,ud3,ud4);
19      uatotal=sum(ua1,ua2,ua3,ua4);
20      label D1='D(i=1)'
21           D2='D(i=2)'
22           D3='D(i=3)'
23           D4='D(i=4)'
24           A1='A(i=1)'
25           A2='A(i=2)'
```

```
26          A3='A(i=3)'
27          A4='A(i=4)'
28          udtotal='u(A,D)'
29          uatotal='U(A,D)';
30   run;

NOTE: There were 25 observations read from the data set MODEL1.'simultaneous$'n.
NOTE: The data set CYEMOTIU.SIM has 25 observations and 23 variables.
NOTE: DATA statement used (Total process time):
     real time          0.09 seconds
     cpu time           0.09 seconds


31
32   ods pdf file='C:\Users\Yan\Documents\my SAS folders\game theory model\gameoutput.pdf';
NOTE: Writing ODS PDF output to DISK destination
     "C:\Users\Yan\Documents\my SAS folders\game theory model\gameoutput.pdf", printer "PDF".
33   title;
34   option nodate nonumber;
35   proc contents data=cyemotiu.sim;
NOTE: Writing HTML Body file: sashtml.htm
36   run;

NOTE: PROCEDURE CONTENTS used (Total process time):
     real time          0.67 seconds
     cpu time           0.40 seconds


37
38   title 'Possible strategy combinations of defenders vs. attackers based on five defense/attack
38 ! level';
39   proc print data=cyemotiu.sim(keep=strategy D1-D4 A1-A4) label;
40   run;

NOTE: There were 25 observations read from the data set CYEMOTIU.SIM.
NOTE: PROCEDURE PRINT used (Total process time):
     real time          0.24 seconds
     cpu time           0.09 seconds


41
42   title 'List of probability of pipeline failure due to intentional damage under diffferent
43   security risk levels given by available strategies (defender vs. attacker)';
44   proc print data=cyemotiu.sim(keep=strategy prob1-prob4) label;
45      label prob1='P(1=1)'
46          prob2='P(i=2)'
47          prob3='P(i=3)'
48          prob4='P(i=4)';
49   run;

NOTE: There were 25 observations read from the data set CYEMOTIU.SIM.
NOTE: PROCEDURE PRINT used (Total process time):
     real time          0.13 seconds
     cpu time           0.03 seconds
```

```

title 'List of calculated utility function under diffferent security risk levels
given by available defender vs. attacker strategies';
proc print data=cyemotiu.sim(drop=prob1-prob4 D1-D4 A1-A4) label;
   format udtotal uatotal ua1-ua4 ud1-ud4 6.;
   label ud1='u(i=1)'
        ud2='u(i=2)'
        ud3='u(i=3)'
        ud4='u(i=4)'
        ua1='U(i=1)'
        ua2='U(i=2)'
        ua3='U(i=3)'
        ua4='U(i=4)';
run;

NOTE: There were 25 observations read from the data set CYEMOTIU.SIM.
NOTE: PROCEDURE PRINT used (Total process time):
      real time           0.28 seconds
      cpu time            0.12 seconds


title;
ods pdf close;
NOTE: ODS PDF printed 5 pages to C:\Users\Yan\Documents\my SAS folders\game theory
      model\gameoutput.pdf.
```