Achieving Cyber-Informed Engineering Through Bayesian Belief Network and Sensitivity Analysis

Chidi Agbo, and Hoda Mehrpouyan*
Boise State University, Boise, Idaho, USA
chidiagbo@u.boisestate.edu, hodamehrpouyan@boisestate.edu
*corresponding author

Abstract—The security of critical infrastructures is a challenge facing nations and states today as a result of the increased complexity and interconnectivity of these systems and their control from remote locations. Ensuring the security of critical systems requires engineering cybersecurity-related risks that attackers can exploit to cause severe consequences, such as equipment damage, environmental/water pollution, monetary loss, or even loss of life. It is important to identify and prioritize actions or attacks that can lead to high-consequence events (HCEs) capable of crippling critical functions of any organization. In this work, we proposed a new approach to cybersecurity risk assessment by proposing the Consequence-Driven Cyber-Informed Engineering (CCE) approach and the Bayesian Belief Network (BBN) with Sensitivity Analysis (SA). For proof of concept, we tested the proposed approach at the Tennessee Eastman chemical plant and were able to uncover and prioritize ripple effects caused by disturbance or noise-induced attacks on critical infrastructure.

Keywords–Critical infrastructures security; cyber-informed engineering; cybersecurity risk assessment; Bayesian belief network; Sensitivity analysis; High-consequence events

1. Introduction

In order to ensure the security of critical infrastructures, it is important to consider the operating technology environment [1] (OT) and its complexity and interconnectivity. Initially, critical infrastructures were built to be controlled on site, but today these systems are managed and controlled from remote locations, exposing them to cyberattacks. To ensure the protection of critical assets, it is critical to analyze and understand cybersecurity-related risks and threats and their impact on processes and systems. Cyber threats are increasing, and attackers are equipped with sophisticated cybersecurity tools and resources to bypass security mechanisms and cause cyber sabotage. Unfortunately, most organizations assume that their systems and industrial software packages are mostly protected, and they are hesitant to allocate proper budget and resources to embrace the necessary cybersecurity practices that address today's security challenges. However, it is not feasible to eliminate all possible cyber risks associated with critical infrastructure, and it is important to identify actions or attacks that can lead to high-consequence events (HCE).

In information technology (IT), HCEs are events that affect critical functions of an organization by crippling its day-to-day business operations [1]. In critical systems, HCEs impact critical infrastructures such as power, energy, nuclear, or water treatment plants, leading to equipment/plant damage or shutdown, environmental pollution, monetary loss, injuries, or even death. HCEs represent events that have the most severe impact on the system. According to the China State Administration of Work Safety accident record, more than 125 chemical plant safety accidents occurred in China between 2006 and 2015, resulting in the deaths of 524 people and 438 injured [2]. The effects of HCE are overwhelmingly disastrous and should not be allowed to occur.

Several tools and approaches have been developed for cyber risk analysis and prevention [3], [4]. Examples of the most popular techniques are fault tree analysis (FTA) to analyze system-level failures [5], attack trees for threats or cyber risk modeling [6], NIST Cyber Security Framework to manage cybersecurity risks within critical infrastructure [7] and many others. However, these techniques help uncover the vulnerabilities and threats found within the system, but lack the ability to find HCEs during the early stages of system design and development. Finding HCE early in critical infrastructure is essential to prevent cybersecurity risks that threaten national security. To this end, the cyber-informed consequence-driven engineering approach (CCE) [8] is introduced to address this weakness. The US Department of Energy (DOE) adopts the CCE approach as an improved cyber risk assessment method to counter cyber sabotage against the energy infrastructure [9]. CCE is a framework to promote the participation of cybersecurity engineering staff in understanding and mitigating high-consequence cyber threats that continually evolve in critical safety systems [10]. CCE is a top-down approach that focuses mainly on finding HCE that affects critical infrastructure, how a malicious actor can exploit the system to cause HCE, and creating mitigation strategies.

Over the years, organizations have witnessed HCE caused by phishing, ransomware, DDoS, spyware, SQL injection, DNS attacks, or disturbance/noise-induced attacks. For example, in 2017, Russian hackers targeted the Wolf Creek nuclear power plant in Burlington, Kansas, to learn the inner workings of the plant relevant to launch a precise attack on the plant [11].

[1] Operation Technology(OT) describes hardware and software systems employed to manage, monitor, and control industrial equipment and operations.

2767-6684/23/$31.00 ©2023 IEEE
DOI 10.1109/DSA59317.2023.00039

The attack on the California Water and Waste System (WWS) facility that targeted the SCADA system in 2021 [12], and a sophisticated cyberattack that targeted the industrial control systems of a German Steel Mill blast furnace, causing the furnace to shut down improperly, leading to massive damage to the furnace [13].

In their research article, Ahmed, Zhou, and Mathur [14] and Yadav, Kannan, and Mansor [15] highlight the fact that disturbance- or noise-induced HCE remains an understudied area in cyberphysical systems (CPS). In this study, we propose an approach inspired by the work of Bochman [9] and Freeman [8]. Bochman [9] and Freeman [8] adopt the CCE approach to identify and prioritize HCE based on expert knowledge. However, our proposed approach combines the CCE approach and the Bayesian belief network (BBN) with a sensitivity analysis (SA) to analyze, identify and prioritize HCE caused by disturbance- or noise-induced attacks. Our approach addresses the main weaknesses found in [9], [8], [16] by eliminating a high dependence on human or expert knowledge during HCE prioritization using BBN with SA analysis to provide a measurable result and evaluations based on system simulation data as described in Section 4. Our approach is twofold; First, the analysis, identification, and prioritization of HCEs are part of the consequence prioritization phase. Then, the analysis of security threats and the demonstration of how cyber adversaries can cause the identified HCEs against the target system are done under the consequence-based targeting phase. At its core, our methodology focuses on uncovering the cascade effects caused by a disruption in critical infrastructure. Furthermore, the BBN-SA phase will describe the impact of the failure caused by a certain disturbance, which will reveal how critical certain components / processes are to the whole system. For proof of concept, we tested our approach on the Tennessee Eastman (TE) plant to analyze the impact of disturbances on the plant during chemical production necessary for the identification and prioritization of disturbance-induced HCE. On the basis of the CCE-BBN result, we conducted an integrity attack on the TE plant to cause disturbance-induced HCE to cripple the plant's critical processes and functions. Our CCE-BBN approach will allow cybersecurity engineers and / or experts in governments and industries to build enhanced protection and mitigation mechanisms for safety-critical systems. However, the implementation of protection and mitigation strategies is beyond the scope of this work. To our knowledge, our work is the first to integrate CCE and BBN with SA for cybersecurity risk assessment to analyze, identify, and prioritize HCE induced by disturbance-related cyber attacks. The codes and results of our work are found in the DSA-2023 git repository[2]. The repository contains the C codes, Matlab files, and Python script for our implementation. The remainder of this paper is organized as follows. Section II discusses related work. Our proposed methodology is presented in Section III. We apply our methodology to the Tennessee Eastman Plant Process in Section IV, where we identified possible attack scenarios and performed an integrity attack in C to demonstrate how a malicious actor can cause HCE in real-world plants. The conclusions and future work are discussed in Section V.

2. Related Work

Several cybersecurity risk assessment methodologies and threat modeling tools have evolved over the years. Bottom-up cyber-risk approaches, such as failure modes and effects analysis (FMEA), failure modes, vulnerabilities, and effects analysis (FMVEA), and failure modes, effects, and criticality analysis (FMECA), are good at identifying and classifying system-level risks. Subriadi and Najwa [17] expanded the FMEA to include the assessment of IT risk. They explored the difficulties in finding the root causes of potential risks using traditional FMEA, thus proposing the use of an improved FMEA. As identified in [18], both FMEA and FMVEA cannot identify complex attack modes. Hyder and Govindarasu [19] proposed the use of attack defense trees and game theory for the analysis of cyber attack paths in smart grids and possible mitigation strategies. Agbo and Mehrpouyan [20] proposed an STPA-SafeSec-CDCL approach that combines System Theoretic Process Analysis for Safety and Security (STPA-SafeSec) and Conflict-Driven Clause Learning (CDCL) technique for the analysis and resolution of safety and security conflicts. Turner, Wheeler, and Gibson [21] proposed the cyber-hazard analysis risk method (CHARM) for nuclear power plants that use STPA to create cyber-informed fault trees. One of the major challenges of attack or fault trees is that the leaves of the tree can grow exponentially, leading to error-prone results. Alanen et al. [22] conducted a review of cybersecurity risk analysis methods and tools for safety-critical industrial control systems such as Security Threat Analysis (STA) for instrumentation and control cybersecurity risk assessments [23], Cyber Process Hazard Analysis (Cyber PHA) for industrial process automation risk assessment [24], Event Tree Analysis (ETA) to trace events that lead to accidents. Singh, Kumar and Pusti [25] proposed an ETA for the analysis of the consequences of the most hazardous events in electrical energy storage systems, but their work did not provide an accurate probabilistic estimate of the results based on real-time failure. In ETA, all events are independent and the analysis is limited to one initiating event, making it difficult for cases where many events occur in combination to cause HCE. Our proposed methodology addresses these weaknesses by taking into consideration cases where different initiating events, actions, or attacks can cause HCE using a Bayesian belief network (BBN) with sensitivity analysis (SA) to handle such probabilistic modeling.

Although there are some approaches for cybersecurity risk assessment based on probabilistic modeling such as (CyberSAGE) [26], the Cyber Security Modeling Language (CySeMoL) [27], and the Adversary View Security Evaluation (ADVISE) [28] and their limitations have been identified in [29], [30], [31] such as state space explosion, the potential for attack graphs or workflows to grow significantly in complexity, rendering them impractical for use in certain

[2] https://github.com/Chidi93/DSA-2023.git

scenarios, etc. The limitations mentioned above are effectively mitigated through the use of Bayesian belief networks (BBN) in conjunction with Sensitivity Analysis (SA) as a means of constructing feasible models for complex systems [32], [33]. The CPS Security Framework (FAST-CPS) [34] only models the system to identify vulnerabilities, and as a result, no attack goals or threats are described or modeled. Furthermore, to our knowledge, there is no existing work on probabilistic modeling of disturbance-induced HCE against safety-critical systems based on CCE with BBN and SA models.

BBN and SA have been used in the risk analysis of industrial and chemical plants or power grids. According to Kabir, Balek, and Tesfamariam [35], BBN is a probabilistic graphical network that represents the main cause-and-effect relationships in the system. The authors proposed a consequence-based model to prioritize buried infrastructure based on health and safety, environmental, social, economic, and organizational impacts using BBN. Zerrouki and Smadi [36] proposed the use of BBN in the chemical and process industry to assess the risk of events that can affect the safety of processes, humans, and the environment. "One of the major advantages of BBN is the ability to model dependencies between variables, manage nonlinear interaction, such as low probability (and high consequence) events, and integrate different kinds of information about the system such as measurement data, feedback experience, and information regarding the system behavior" [37]. Brutica and Tesfamariam proposed the application of BBN and SA for the probabilistic analysis of HCE in electric power systems [38]. They expand their approach to Canadian power systems. BBN and SA have also been used to model the risk of chemical plant explosion accidents [39].

However, the consequence-driven cyber-informed engineering approach (CCE) is an improved cybersecurity risk assessment method that has been applied to identify, prioritize, and mitigate HCEs. Bochman and Freeman in their work applied the CCE approach to counter cyber sabotage [9]. Freeman [16] adopted the CCE approach in which the author proposed an HCE severity score calculated using the equation:

HCE Severity Score = α(Area Impacted) + β(Duration) + γ(Attack Breadth) + δ(System Integrity) + ϵ(Safety) + ζ(Cost) where α, β, γ, δ, ϵ, and ζ are weighting coefficient values determined by domain experts. The main challenge with the proposed approach to prioritize HCE [16] is that domain experts can make errors in severity scoring due to incomplete or imperfect data in the target system. The authors proposed going back and forth to adjust the severity score when more information or data is obtained. To address this weakness, we proposed the use of a Bayesian belief network (BBN) with a sensitivity analysis (SA) modeling approach that works well in predicting probabilistic events even in areas with sparse or incomplete data, thus reducing the dependency on human or expert knowledge through probabilistic modeling. Our approach also focuses on analyzing and identifying HCE associated with critical assets of an organization and explores actions or attack scenarios that can impact the system to cause such HCE.

3. Methodology

In this work, we propose a CCE-BBN approach that integrates a consequence-driven cyber-informed engineering approach (CCE) [9] and the Bayesian Belief Network (BBN) with sensitivity analysis (SA) [38] for the analysis, identification and prioritization of HCEs capable of crippling critical national or state infrastructures such as power / energy, nuclear or water treatment plants, etc.

CCE is an enhanced methodology developed by Idaho National Laboratory [3] (INL) that seeks to identify HCE with worse-case functional impacts on critical infrastructure [9]. The CCE approach provides organizations with the important phases needed to ensure the protection of assets that perform the most critical functions. CCE also enables organizations to adequately identify and calculate cybersecurity risks caused by specific cyber adversaries and groups, and to develop an understanding of the potential impact (both cyber and physical) of a cyber event to provide improved security within critical infrastructure [8]. On the other hand, BBN is a graphical model that captures a probabilistic relationship among a set of variables. Bayesian network modeling is an artificial intelligence tool that is used to model uncertainty in a domain or system [40]. BBN is a dependency graph (directed acyclic graph) where nodes represent variables and arcs (arrows) denote causal relationships among them. Models the probabilistic occurrence of events given the uncertainty in the system. An important feature of BBN modeling is the identification of critical variables, taking into account other influencing factors. To this end, SA is used to validate the BBN model by identifying the most critical parameters that have a significant impact on the overall BBN result when adjusted. In this work, we employ the capabilities of our CCE-BBN approach for the analysis, identification, and prioritization of HCE, identification of possible security threats within the target system that an attacker can exploit to disrupt critical assets that the organization relies on to function, and a demonstration of how a malicious actor can paralyze the target system to cause HCE.

Figure 1 shows our proposed framework, which is discussed in detail in the next section.

Our proposed framework consists of two main phases. In phase 1 HCE analysis, identification and prioritization are performed using the BBN and SA models. Security threats and how a cyber adversary can exploit the system to cause the identified HCEs are discussed in phase two.

3.1. Consequence Prioritization

The consequence prioritization phase is an essential phase of the CCE-BBN approach based on the fact that the rest of the phases depend on the result of this phase. During this phase, worst-case scenarios, events, or attacks that can lead to HCE are identified by defining the boundary conditions and

[3] Idaho National Lab (INL) is a US Lab leading a high-impact, national security-level initiative to re-prioritize the way the nation looks at high-consequence risk within the industrial control systems (ICS) environment of the country's most critical infrastructure and other national assets [8]

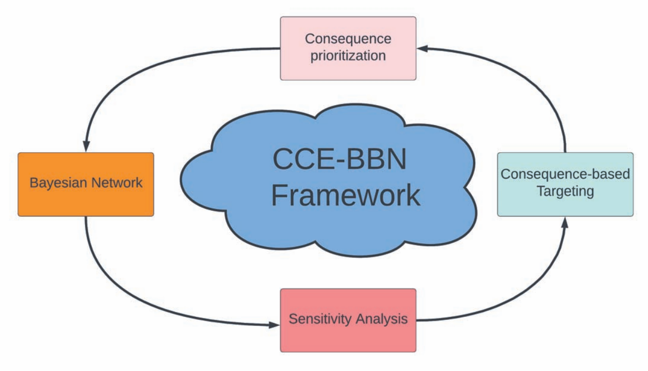


Figure 1. Proposed Framework

severity criteria necessary to assess acceptable or unacceptable risks. For HCE identification and prioritization, we proposed the use of a Bayesian belief network (BBN) with a sensitivity analysis (SA) approach to model the occurrence of events or attacks and their effects on the target system. In this work, we adopt the functional taxonomy of CCE proposed by [41] for the identification of critical components and functions such as the production of the entity or the business functions that an adversary would have to disrupt to cause HCE, as seen in Section 4. Next, we will discuss the concept of BBN and SA in detail below;

a) ***Bayesian Belief Network (BBN) and Sensitivity Analysis (SA):*** BBN and SA are essential modeling frameworks used for risk-based analysis. The BBN network is based on the Bayes theorem, which has been shown to be a coherent method for managing uncertainty by explicitly representing conditional probability dependencies (CPD) between variables [42]. Furthermore, the BBN consists of two parts: a network graph for qualitative analysis and a conditional probability table (CPT) for quantitative analysis. The network graph also known as the directed acyclic graph (DAG) represents the dependencies among variables (often referred to as nodes), and the CPT represents the conditional probabilities of a single node or variable with respect to the others in a BBN network. A node represents a random variable in a BBN model. Each node is associated with a probability distribution that describes the interdependencies between the node and its parents within the network. The CPT is derived from one of the following: (i) Expert knowledge, (ii) data, and (iii) a combination of both. BBN can also be used to compute posterior probabilities for a set of nodes given any set of evidence. To reduce the overreliance on expert knowledge, our CPT is built on the basis of system simulation data.

In addition, determining the sensitive nodes is essential for BBN modeling, and, as a result, we apply the SA approach to identify the sensitivity of each node towards the target node[4]. SA measures how changes in input variables affect the output variable of a BBN network. Identifying critical input variables in a model is crucial for decision-making purposes. SA helps validate the BBN model by increasing its correctness and reliability, as seen in section 4. SA has been used in conjunction with BBN for consequence-based analysis, medical diagnosis, predictions, and classifications.

The proposed BBN and SA approach is implemented using the GeNIe Bayesian Modeler. The GeNIe modeler is an interactive development environment to build graphical decision-theoretic models or qualitative causal models of uncertain domains by implementing SMILE (Structural Modeling, Inference, and Learning Engine), a fully platform independent library of functions for graphical probabilistic and decision-theoretic models, such as Bayesian networks, influence diagrams, dynamic Bayesian networks, and structural equation models [43]. GeNIe implements a sensitivity analysis algorithm proposed by Kjaerulff and van der Gaag [44] that efficiently and effectively calculates a complete set of derivatives of posterior probability distributions at the target nodes and at each of the numerical parameters of the Bayesian network [43]. This set of derivatives determines the magnitude of precision of the network parameters to compute the posterior probabilities of the target nodes. It implies that the larger the derivatives of a parameter, the larger the change in the posteriors of the targets, given a small change in that parameter, and vice versa. GeNIe modeler has been used for probabilistic modeling in [45], [46], [47] and many others. Furthermore, our analysis is based on four cybersecurity risk factors, which include Safety, Integrity, Availability, and Cost (SIAC), also known as the SIAC criteria. The choice of our selected criteria is based on the fact that the goal of cyber adversaries in critical infrastructures is mainly to cause the impact of SIAC. It is important to note that the impact on SIA can lead to equipment damage or shutdown, environmental/water pollution, or even death. In this work, we treat actions, events, or attacks that have a high impact on the SIAC criteria as HCEs. For example, if the introduction of disturbances/noise into the system has a severe impact on the SIAC criteria, we treat it as an HCE. Furthermore, the impact of events or attacks on these factors is used to calculate the overall severity necessary to classify HCEs. The four cybersecurity risk factors are explained in detail as follows:

b) ***Safety:*** Safety is an essential property of any critical system. Safety is freedom from conditions that can cause death, injury, occupational illness, damage, loss of equipment, or property [48]. Safety conditions are defined to ensure safe operations of the system and deviations can be catastrophic. Unfortunately, cyber adversaries target safety-critical systems to cause safety violations. For example, Lanotte, Merro, Munteanu, and Vigano [49] carried out a man-in-the-middle (MITM) attack that can manipulate sensor readings or control commands to drive a CPS into an unsafe state. In this work, we treat actions, events, or attacks that can violate the system's safety conditions and drag the system into an undesired state as an HCE.

c) ***Integrity:*** System integrity describes the protection of system data and resources from unauthorized modifications. The consequences of system integrity attacks on critical infras-

[4] A target node in the BBN model represents a predicted node whose values are determined based on the values of other nodes in the network

tructures are disastrous and can lead to death. For example, the attack on the Florida water treatment plant on 5 February 2021, in which an unidentified hacker gained access to the SCADA system and increased the amount of sodium from 100 parts per million to 11,100 parts per million, to poison drinking water [50]. System integrity-related risks refer to actions, events, or attacks that can lead to modifications or manipulations of system codes, control data, sensor values, process variables, and levels to cause HCE.

d) ***Availability:*** System availability ensures that the system is readily available for use when needed. Entails protecting the system from actions or attacks that can lead to a shutdown. For example, the BlackEnergy cyber attack on the Ukrainian power grid that comprised the SCADA system and caused the interruption of power supply to more than 225,000 customers [51] and the DarkSide Russian hackers group that led to the complete shutdown of all Colonial pipelines crippling fuel deliveries to the East Coast of the United States [52]. The availability of the system is essential for the day-to-day business operations of any organization. Risks associated with availability include actions, events, or attacks that can impact system availability, making the system unavailable for use.

e) ***Cost:*** Cost-related risks refer to actions, events, or attacks with a financial impact on the system. It includes actions or attacks that can lead to an increase in production cost, system maintenance, and the cost of restoring confidence or trust in the system after a successful attack.

We encode this reasoning in our BBN network starting with the network graph as seen in Figure 2.

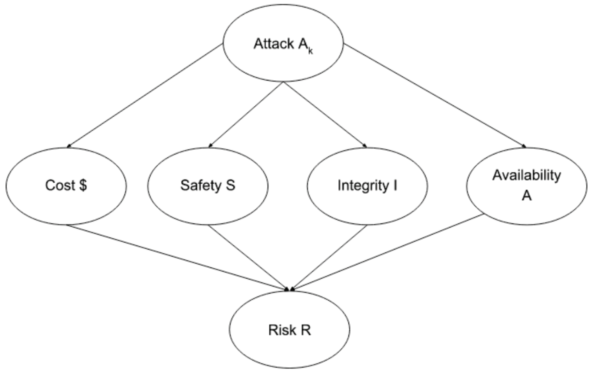


Figure 2. Network graph of our BBN model

The direct connection (arc) from A_k to SIAC shows the causal effect between the nodes. This implies that SIAC is conditionally dependent on A_k and marginally independent given their child node R. The child node R is conditionally independent of its ancestor node A_k. The concept of conditional independence is important for the compact computation of the joint probability distribution (JPD) in a Bayesian network. It states that a node is independent of its ancestors, given its parents. For example, if the parent nodes of R (i.e. $, SIA nodes) are known, the information about node A_k becomes irrelevant to the prediction of the risk node R. It is imperative to note that the attack node A_k represents a set of attacks or events that can impact the system to cause HCE with A_k ranging from $Attack_1$, $Attack_2$, $\ldots$, $Attack_n$ or $Event_1$, $Event_2$, $\ldots$, $Event_n$. Furthermore, every node in a BBN has CPD/CPT and can be calculated using the Bayes theorem. Assuming that we want to calculate the impact on the integrity of the system (I) given that an action, event, or attack A_1 has occurred, we can express the conditional probability based on the Bayesian formula given thus:

$$P(I|A_1) = \frac{P(A_1|I)P(I)}{P(A_1)} \tag{1}$$

where $P(A_1) \neq 0$, $P(I|A_1)$ is an unknown probability (posterior probability) interpreted as the probability of impact on the integrity of the system given that an attack has occurred. $P(A_1|I)$ represents the probability that an attack occurs and its impact on the integrity of the system. $P(I)$ and $P(A_1)$ are the probabilities of observing I and A_1, respectively. They are also called prior probability. Equation 1 can be expressed as:

$$P(I|A_1) = \frac{P(A_1|I)P(I)}{P(A_1|I)P(I) + P(A_1|\neg I)P(\neg I)} \tag{2}$$

However, if two or more events or attacks impact the integrity of the system, we can apply the equation 3 for this computation.

$$P(I|A_k) = \frac{P(A_k|I)P(I)}{P(A_k|I)P(I) + P(A_k|\neg I)P(\neg I)} \tag{3}$$

The JPD of all the nodes in the network graph can be computed based on the conditional independence relationships using the equation expressed thus:

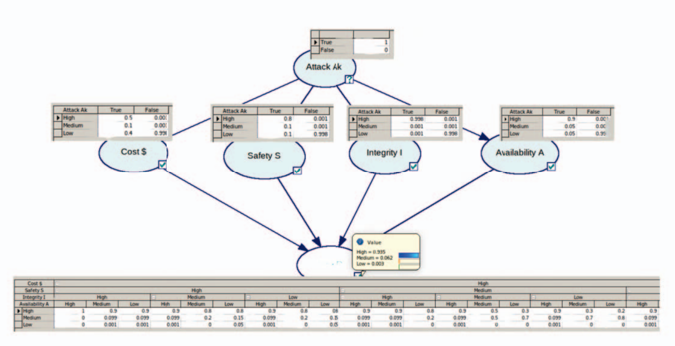
$$P(A_k, \$, S, I, A, R) = \tag{4}$$
$$P(A_k)P(\$|A_k)P(C|A_k)P(I|A_k)P(A|A_k)P(R|\$, S, I, A)$$

Calculating the probability of the overall impact or risk (R) given that an attack has occurred is given as:

$$P(R|A_k) = \sum P(R, \dot{\$}, \dot{S}, \dot{I}, \dot{A}|A_k) =$$
$$\sum [P(R|\dot{\$}, \dot{S}, \dot{I}, \dot{A})P(\dot{\$}|A_k)P(\dot{S}|A_k)P(\dot{I}|A_k)P(\dot{A}|A_k)] \tag{5}$$

where $\dot{\$}$, $\dot{S}$, $\dot{I}$, or $\dot{A}$ denotes the possible conditions of the nodes. For example, $\dot{\$}$ means impact on cost = True (denoted by $) and impact on cost = False (denoted by ¬$).

In BBN modeling, the qualitative part uses the CPT to specify probabilistic relationships. For example, consider an attack that has the following impact on a safety-critical system A, as represented by the CPT shown in Figure 3. In this work, the impact on safety, integrity, and availability (SIA) has higher CPT values. The reason is that the violation of SIA in critical infrastructures can lead to severe consequences, such as loss of life. For example, an attack A_1 directed at a water treatment plant that poisons drinking water distributed to homes by increasing the number of chemicals beyond the acceptable threshold can wipe out an entire community, or an attack that shuts down a life-supporting medical device in use, leading to the death of the patient. Furthermore, it is important to note that the GeNIe modeler implements equations 2 and 5 given the CPT for each node. In our case, we used GeNIe to calculate the overall impact given that an attack has occurred. For example, the result shows that the attack has an impact of 93. 5% in system A (that is, risk R = 93. 5%).



True	1
False	0

Attack Ak	True	False
High	0.5	0.001
Medium	0.1	0.001
Low	0.4	0.998

Attack Ak	True	False
High	0.8	0.001
Medium	0.1	0.001
Low	0.1	0.998

Attack Ak	True	False
High	0.998	0.001
Medium	0.001	0.001
Low	0.001	0.998

Attack Ak	True	False
High	0.9	0.00
Medium	0.05	0.00
Low	0.05	0.99

Value
High = 0.935
Medium = 0.062
Low = 0.003

Cost $	High																		
Safety S	High									Medium									
Integrity I	High			Medium			Low			High			Medium			Low			
Availability A	High	Medium	Low	Hijh	Medium	Low	High	Medium	Low	High	Medium	Low	High	Medium	Low	High	Medium	Low	High
High	1	0.9	0.9	0.9	0.8	0.8	0.9	0.8	08	0.9	0.9	0.8	0.9	0.5	0.3	0.9	0.3	0.2	0.9
Medium	0	0.099	0.099	0.099	0.2	0.15	0.099	0.2	0.15	0.099	0.099	0.2	0.099	0.5	0.7	0.099	0.7	0.8	0.099
Low	0	0.001	0.001	0.001	0	0.05	0.001	0	0.05	0.001	0.001	0	0.001	0	0	0.001	0	0	0.001

Figure 3. Conditional Probability Table of attack A_1 on System A

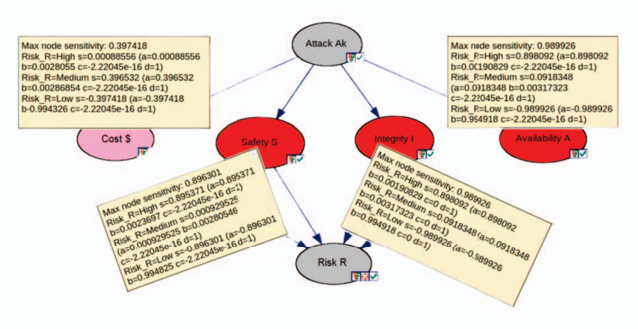
The robustness of the output probabilities of a BBN can be determined by SA [53]. The GeNIe Modeler computes the sensitivity of all possible parameters given a target node or a set of target nodes. The SA algorithm implemented by GeNIe computes a set of derivatives. These sets of derivatives are based on the evidence set in the network and are essential to measuring the precision of network numerical parameters to calculate posterior probabilities of the target nodes. The sensitivity of each node in the BBN network can be calculated as the real values of the derivative and as a set of coefficients using the equation 6. The set of coefficients defines the dependency between the target posterior node and the specific CPT parameter.

$$P = \frac{(au + b)}{(cu + d)^2} \tag{6}$$

Where P is the posterior target and a, b, c, d are coefficients calculated by SMILE and u denotes the value of the specific CPT parameter. The derivative D is calculated using the following:

$$D = \frac{(ad - bc)}{(cu + d)} \tag{7}$$

With Equation 6, we can calculate how much the posterior target will change when the CPT values (u) are modified. The degree of change is defined by $u_1 = b/d$, $u_2 = (a+b)/(c+d)$. Note that ad-bc determines which value of u_1 and u_2 is lower or greater. During sensitivity analysis, the GeNIe Modeler differentiates sensitive nodes in a network from less sensitive or nonsensitive nodes with colors. For example, gray for non-sensitive nodes, ross or light red for low-sensitive nodes, and red for high-sensitive nodes, as seen in Figure 4.



Max node sensitivity: 0.397418
Risk_R=High s=0.00088556 (a=0.00088556 b=0.0028055 c=-2.22045e-16 d=1)
Risk_R=Medium s=0.396532 (a=0.396532 b=0.00286854 c=-2.22045e-16 d=1)
Risk_R=Low s=-0.397418 (a=-0.397418 b-0.994326 c=-2.22045e-16 d=1)

Max node sensitivity: 0.989926
Risk_R=High s=0.898092 (a=0.898092 b=0.00190829 c=-2.22045e-16 d=1)
Risk_R=Medium s=0.0918348 (a=0.0918348 b=0.00317323 c=-2.22045e-16 d=1)
Risk_R=Low s=-0.989926 (a=-0.989926 b=0.994918 c=-2.22045e-16 d=1)

Max node sensitivity: 0.896301
Risk_R=High s=0.895371 (a=0.895371 b=0.0023697 c=-2.22045e-16 d=1)
Risk_R=Medium s=0.000929525 (a=0.000929525 b=0.00280546 c=-2.22045e-16 d=1)
Risk_R=Low s=-0.896301 (a=-0.896301 b=0.994825 c=-2.22045e-16 d=1)

Max node sensitivity: 0.989926
Risk_R=High s=0.898092 (a=0.898092 b=0.00190829 c=0 d=1)
Risk_R=Medium s=0.0918348 (a=0.0918348 b=0.00317323 c=0 d=1)
Risk_R=Low s=-0.989926 (a=-0.989926 b=0.994918 c=0 d=1)

Figure 4. Sensitivity Analysis of attack A_1 on System A

The SA analysis result shows that the safety, integrity and availability nodes have a sensitivity of 90%, 99%, and 99%, respectively, while the cost node has a sensitivity of 40%, with their corresponding coefficients determined by SMILE. This information is relevant during decision making, where limited resources are directed toward mitigating attacks or actions that can affect high-sensitivity nodes.

3.2. Consequence-based Targeting

The Consequence-based targeting phase enables domain experts to think like an attacker by exploring how a malicious actor can disrupt the system to cause HCE. All weak points in the system are analyzed, including all gateways, data centers, network components, and people (workers and customers). This phase can help identify the type of information or access an attacker may need to execute his payload. Humans are the weakest link in the security chain. An attacker can choose to exploit people to carry out high-impact attacks. For example, the Stuxnet attack launched to destroy Iranian centrifuges was executed on a USB drive [54]. This phase involves a detailed examination of all critical assets or components of the system that may appear attractive to the attacker. The benefit of this phase is that those who have a good understanding of the system are looking for ways to attack the system to cause HCE but with a defensive mindset. Bochman and Freeman [9] proposed adversarial operations (CONOPS), while Lawrence [55] proposed the use of the CCE kill chain[5] for consequence-based targeting analysis. We adopt the CCE kill chain approach in our work to cause HCE, as seen in section 4.

4. CASE STUDY

The Tennessee Eastman (TE) plant process [56] is the simulation of a real chemical process plant model developed for the study of industrial control processes. The main reasons for our choice of plant include (i) The TE plant is a widely used plant process model for the study of CPS [57], [58]. (ii) The plant comprises various components, levels and process variables found in real-world chemical plants such as reactor, compressor, stripper, condenser, separator, analyzers, sensors, actuators (valves), feed components, pressure, temperature,

[5] The CCE kill chain helps illustrate the specific information requirements the adversary needs to develop and deploy a payload to cause an HCE [55]

etc. and (iii) The TE plant has been extensively used in the study of CPS security and attack detection [59], [60], [61], [62], [63], etc.

First, we apply the CCE functional taxonomy proposed by [41] to identify critical functions of the TE plant by differentiating the enabling functions (EF) and critical functions (CFs). In critical infrastructure, enable functions are functions that support the delivery of critical functions and services. They include information technology, communications, safety, security, procurement, regulatory compliance, etc. Critical functions are functions whose disruption or failure would have destructive effects on the system such as environmental/water poisoning, equipment abrasion, loss of property, personal injury, or even loss of life. They include activities like production, waste management, water treatment and supplies, electricity generation and distribution, etc. In this work, we present a high-level representation of the critical and enabling functions of the TE plant with a focus on the critical functions (production) part of the functional taxonomy of the CCE as shown in Figure 5.

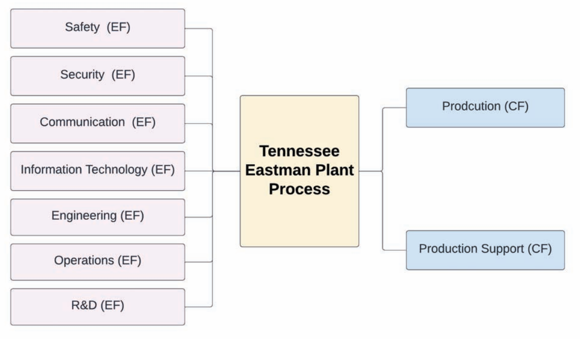


Figure 5. The TE Plant CCE Functional Taxonomy Mappings with a high-level representation of EFs and CFs

The TE plant is used in the production of two liquid products, G and H, one by-product, and one inert component, from four chemical reactants (A, C, D, and E), as shown below. Production takes place in the reactor, and as a result, we treat the reactor unit as a critical component of the TE plant. The flow of the chemical reactants (feeds) is controlled by the feed valves (FI) to allow the correct amount of feeds to pass through the reactor per hour during production.

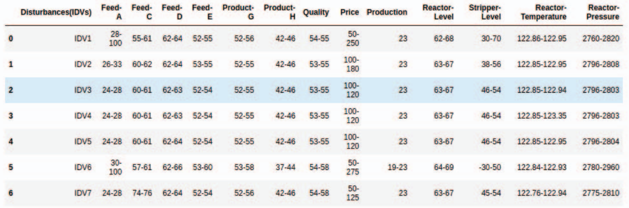
$$A(\mathrm{g}) + C(\mathrm{g}) + D(\mathrm{g}) \to G(\mathrm{liq}) \Rightarrow Product1 \tag{i}$$

$$A(\mathrm{g}) + C(\mathrm{g}) + E(\mathrm{g}) \to H(\mathrm{liq}) \Rightarrow Product2 \tag{ii}$$

The reactor contains measurement sensors that monitor reactor level, temperature, pressure, and other process variables. Analyzers measure the quality of the products being produced. If the quality of the product is satisfied, the product is sent through the discharge valve; otherwise, the product is recycled back to the reactor for reprocessing. The by-products are purged from the plant through the purge valve. Second, we applied our CCE-BBN approach to the reactor unit during the production of chemicals G and H to demonstrate how our approach can be used in real-world chemical plants. HCE in our study represents actions, events, or attacks that can impact the SIAC criteria and lead to catastrophic consequences. It can be through Denial of Service (DoS) attacks, integrity/code injection attacks, man-in-the-middle (MITM), phishing, or insider attacks, as discussed in section 4-A.

4.1. Simulation Setup

The TE chemical plant process model consists of 28 disturbances that can be activated during chemical production. However, the TE control system, as described by Downs and Vogel [56], ensures the following control objectives (i) maintaining the process variables within the desired values. (ii) ensure that the processes operate within equipment constraints. (iii) reduce variations in product rate and process variables during disturbances, (iv) reduce valve movement that affects other processes, and (v) recover quickly and smoothly from disturbances, product mix, or production rate changes. In the simulation setup, we used the TE plant code developed by Bathelt and Ricker [64] and ran the code in Matlab R2021b. We set the simulation time T to 100 hours. We used a 64-bit Dell system made up of an Intel (R) Core (TM) i7-7700HQ CPU @ 2.80GHz with 20GB of memory. Firstly, we run the simulation without disturbances using the base case values specified by Downs and Vogel [56] and observe the normal behavior of the plant in real time (see Figure 13). Second, we ran the simulation using the same setup under disturbances and recorded the effect on the plant. The real-time data obtained when the plant is operated under disturbances were fed into our BBN model to identify the overall impact of each disturbance on the SIAC criteria, thus eliminating any biases that can impact the identification of actual HCEs due to the considerable dependence on domain experts or knowledge. To understand the type of data used for our analysis, we displayed part of the data in Figure 6. The data show the impact of each disturbance on feed rates, price, process variables, production rate, quality, etc. during production.



	Disturbances(IDVs)	Feed-A	Feed-C	Feed-D	Feed-E	Product-G	Product-H	Quality	Price	Production	Reactor-Level	Stripper-Level	Reactor-Temperature	Reactor-Pressure
0	IDV1	28-100	55-61	62-64	52-55	52-56	42-46	54-55	50-250	23	62-68	30-70	122.86-122.95	2760-2820
1	IDV2	26-33	60-62	62-64	53-55	52-55	42-46	53-55	100-180	23	63-67	38-56	122.85-122.95	2796-2808
2	IDV3	24-28	60-61	62-63	52-54	52-55	42-46	53-55	100-120	23	63-67	46-54	122.85-122.94	2796-2803
3	IDV4	24-28	60-61	62-63	52-54	52-55	42-46	53-55	100-120	23	63-67	46-54	122.85-123.35	2796-2803
4	IDV5	24-28	60-61	62-64	52-54	52-55	42-46	53-55	100-120	23	63-67	46-54	122.85-122.95	2796-2804
5	IDV6	30-100	57-61	62-66	53-60	53-58	37-44	54-58	50-275	19-23	64-69	-30-50	122.84-122.93	2780-2960
6	IDV7	24-28	74-76	62-64	52-54	52-56	42-46	54-58	50-125	23	63-67	45-54	122.76-122.94	2775-2810

Figure 6. Real-time Simulation Data of the plant under Disturbances

As noted in section 3.1, the first phase of our proposed approach is consequence prioritization using BBN with SA analysis. In BBN modeling, the first part is to build a network graph or DAG to capture casual relationships between variables (i.e., the SIAC criteria).

Figure 7 represents the directed acyclic graph (DAG) of our BBN. The disturbance activation node represents a probabilistic action or event that can impact the SIAC criteria to cause HCE. Our BBN model in Figure 10 (i.e., Figures 8 and 9) is modeled using the GeNIe modeler explained in section 3.1. It

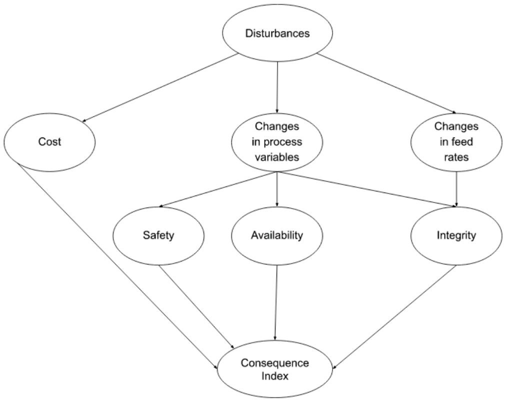


Figure 7. DAG of our Bayesian Belief Network (BBN)

depicts the consequence index of disturbance activation. The

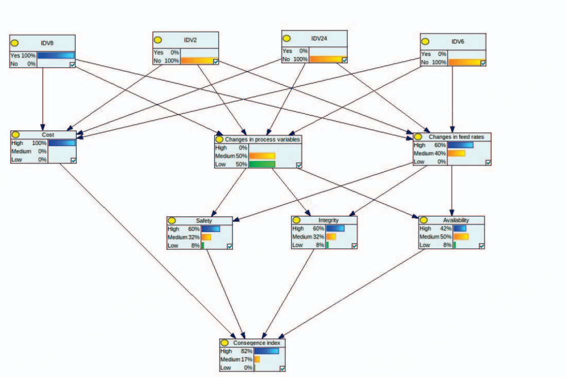


Figure 8. BBN model (Scenario 1)

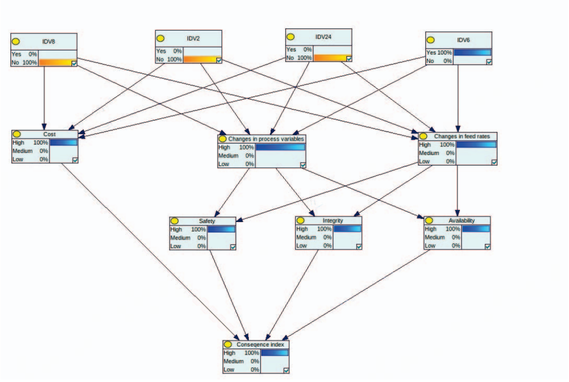


Figure 9. BBN model (Scenario 2)

Figure 10. BBN model to determine the consequence index of disturbance activation

CPT for each node was constructed based on real-time data generated during plant simulation under disturbances. In other words, the CPT is built based on the degree of impact of each disturbance on the feed rates, price, process variables, production rate, quality, etc. (see Figure 6). The assignment of values for our CPT is between 0 and 1 where 0 denotes no impact and 1 denotes the highest impact. During production, the amount of A feed component released into the reactor under normal working conditions is between 24% and 30% per hour. However, an attack or event can cause an increase in the feed components and underlying processes, forcing the rate of flow outside the defined setpoints or boundaries. For example, the activation of disturbances 1 and 3 has varying degrees of impact on the feed component A, that is, 28% - 100% and 24% - 28%, respectively, during production. Therefore, their CPT values vary accordingly. We applied this type of reasoning for the construction of our CPT where the assignment of values depends on the level of impact on the independent variables as shown in the simulation data. Based on our CPT for each node, we calculated the impact of each disturbance using the equations 2 and 5 implemented by the GeNIe modeler. The result of our BBN model shows that the TE plant reacts differently to each disturbance and the consequence index varies considerably depending on the disturbance introduced. As shown in Figures 8 and 9, disturbance 6 (IDV6) has a greater impact on the system than disturbance 7 (IDV7). To verify the accuracy and reliability of our model, we introduce the concept of sensitivity analysis (SA) implemented using the GeNIe modeler. The result of our SA model (see Figure 11) shows that the "changes in process variable" and "changes in feed rates" nodes are critical nodes, which implies that any slight changes in these nodes will greatly impact the target node. The concept of sensitivity analysis is useful in helping security experts and engineers clearly identify nodes that need maximum protection, as impacts on these nodes would have devastating effects on the system. Therefore, any attacks, events, or actions that will impact the identified sensitive nodes (i.e. changes in process variables and changes in feed rates) must be mitigated. Furthermore, to facilitate the identification ofHCE based on our BBN and SA results, we represent the overall impact of each disturbance on the TE plant in the graph shown in Figure 12.

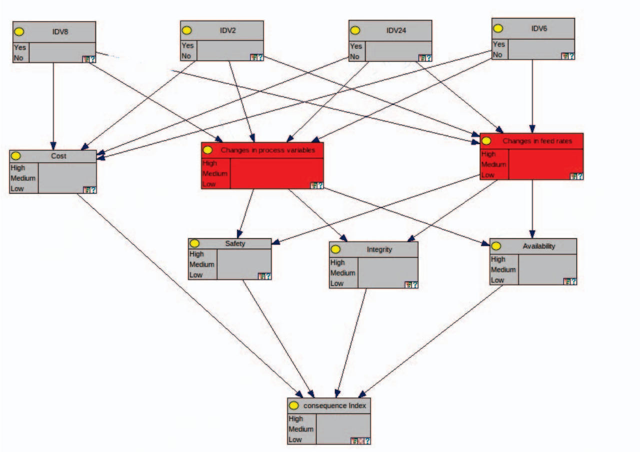


Figure 11. Sensitivity analysis of our BBN network

From the graph we see disturbances that have high, medium,

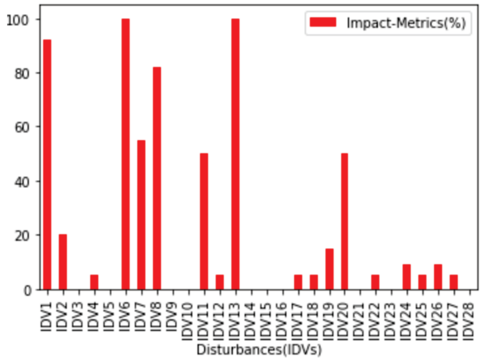


Figure 12. Consequence Index of disturbance activation

and low impacts on the plant. Having identified the events or actions that can lead to HCE, we can investigate possible attack scenarios to cause disturbance-induced HCE.

4.2. Consequence-based Targeting

In this phase, we will discuss in detail how a malicious actor can exploit the system by introducing a disturbance (s) that can disrupt the system. In our study, we define HCE as events, actions, or attacks that can affect the SIAC criteria. Therefore, we discuss possible attack scenarios that can exploit SIAC cyber risk factors.

i. **Safety threats**

- Advanced-Persistent Attacks (APTs)
  Attack Scenarios: A sophisticated group of attackers gains access to critical components and plant processes through the backdoor to cripple the plant.
- Insider threats.
  Attack Scenarios: A disgruntled employee gains control of the system by increasing privileges to cause safety violations.
- Zero-day Exploits
  Attack Scenarios: The attacker exploits an unknown weakness in the system to impact plant safety

ii. **Integrity threats**

- Code injection or modification
  Attack Scenarios: Injection or modification of plant codes through remote connection or phishing to disrupt the normal operation of the plant essential to cause HCE.
- Command Manipulation
  Attack Scenarios: Remote connection to the controller to modify control commands to cause HCE.
- Measurement Manipulation
  Attack Scenarios: Man in the middle attack (MITM) that intercepts and introduces noise into sensor measurement.

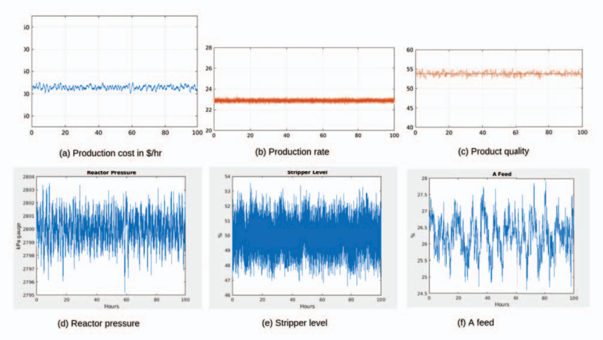
iii. **Availability threats**

- Infrastructure Failure
  Attack Scenarios: An attack that determines the best time to introduce disturbance or noise into the plant leading to the plant's shutdown.
- Infrastructure Overload
  Attack Scenarios: A DOS attack that overloads the plant with noisy data, keeping the plant too busy and unavailable.

iv. **Cost threats**

- Ransomware
  Attack Scenarios: An attacker who gains unauthorized access to encrypt the proprietary data of the plant and demands a ransom in exchange for the decryption key.
- Man-in-the-middle (MITM)
  Attack Scenarios: A MITM attack that modifies critical processes and levels of a plant to cause an increase in production cost.

Based on the identified possible security threats, we performed a code injection integrity attack to cause HCE that can impact the SIAC criteria by adding a function block in C to introduce IDV6 during production. We maintain the same simulation setup with simulation time = 100 h, where the payload is set to run at T = 50 h.



(a) Production cost in $/hr

(b) Production rate

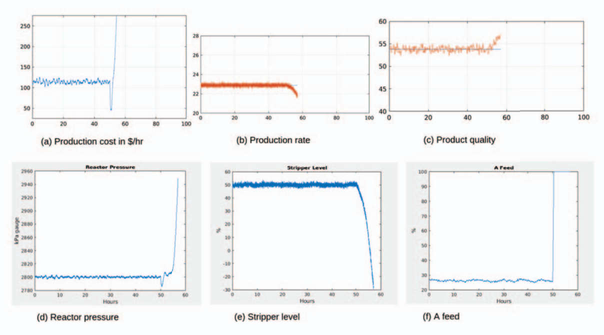
(c) Product quality

(d) Reactor pressure

(e) Stripper level

(f) A feed

Figure 13. Plant simulation result under normal operations



(a) Production cost in $/hr

(b) Production rate

(c) Product quality

(d) Reactor pressure

(e) Stripper level

(f) A feed

Figure 14. Plant simulation result under integrity attack

We compared the result of the plant under normal operation and under attack and found that there were notable impacts on production cost, process variables, feed rates, production rates, and final products, and in a short period of time, the plant was completely shut down due to a low stripper level as seen in Figure 14. For example, the cost of production increased to over $275 against $120 under normal operation. The highest amount of feed A released into the reactor per hour increased from 30% to 100%. In the real world, such impacts on chemical, nuclear or water treatment plants can lead to disasters such as equipment damage, environmental or water pollution, or even loss of life. Furthermore, we noticed that the result is consistent with our BBN and SA models. The attack result shows that changes in feed rates and process variables, such as stripper level, reactor pressure, and temperature, have the highest effects on the plant, making these nodes the most critical nodes in our model. The proposed CCE-BBN approach offers several advantages over alternative cybersecurity risk assessment techniques. One key advantage is the use of probabilistic analysis to identify and prioritize HCEs to improve protection and mitigation strategies for safety-critical systems.

5. Conclusion and Future work

The complexity and progress of Industry 4.0 pose a serious challenge to the security and protection of critical infrastructures. All previous efforts to eliminate cybersecurity risks and threats yielded little or no results, with organizations playing catch-up game or hoping never to be attacked. In this paper, we explore the strengths and weaknesses of well-known cybersecurity risk assessment approaches and therefore proposed a new enhanced framework capable of addressing these weaknesses and the risks and threats related to cybersecurity today. The CCE-BBN methodology combines the concept of Consequence-Driven, Cyber-Informed Engineering and the Bayesian belief network with a sensitivity analysis (SA) for the analysis, identification, and prioritization of high-consequence events (HCE) by identifying and classifying HCE, security threats within the target system with possible attack scenarios, and a demonstration of how an attacker can exploit the system to cause the identified HCE. In this work, we treat events, actions, or attacks that have a severe impact on system safety, integrity, availability, and cost (SIAC) as HCEs. We built our BBN and SA models based on the system's simulation real-time data using the GeNIe modeler to eliminate the high dependence on human or expert knowledge during HCE prioritization. The approach we propose demonstrates effectiveness in assessing risks both at the system / component level and during the initial phases of system design and development. The CCE-BBN enables security experts to think and act like attackers with a protective and defensive mindset. It should be noted that our approach begins where many cybersecurity risk assessment methods end. Specifically, while other approaches may prioritize identifying threats that could potentially result in severe consequences, which can be both time-intensive and may fail to detect genuine HCEs, our framework prioritizes identifying HCEs that could cripple critical assets or functions. Once we have identified the HCE, we then analyze the threats that could trigger those events. We elevate our proposed approach to the Tennessee Eastman Chemical Plant Process Model to demonstrate how our proposed approach can be applied to real-world chemical plants or safety-critical systems. We conducted an integrity attack to disrupt the system to cause HCE. The overall result of our approach will allow cybersecurity experts and engineers to build effective and efficient protection and mitigation strategies for safety critical systems.

In future work, we plan to build improved protection and mitigation measures against identified security threats within the target system. The emphasis is on detecting attacks and ensuring that the system can carry out its critical mission while under attack, as well as recovering the system in real time during an attack.

Acknowledgment

The authors would like to thank the National Science Foundation Computer and Information Science and Engineering (CISE), award number 1846493 of the Secure and Trustworthy Cyberspace (SaTC) program: Formal TOols foR SafEty aNd. Security of Industrial Control Systems (FORENSICS).

References

[1] D. Ackerman and H. Mehrpouyan, "Modeling human behavior to anticipate insider attacks via system dynamics," in *2016 Symposium on Theory of Modeling and Simulation (TMS-DEVS)*, pp. 1–6, 2016.

[2] L. Zhao, Y. Qian, Q.-M. Hu, R. Jiang, M. Li, and X. Wang, "An analysis of hazardous chemical accidents in china between 2006 and 2017," *Sustainability*, vol. 10, no. 8, p. 2935, 2018.

[3] *A Model-Based Failure Identification and Propagation Framework for Conceptual Design of Complex Systems*, vol. Volume 2: 32nd Computers and Information in Engineering Conference, Parts A and B of *International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*, 08 2012.

[4] T. Phillips, H. Mehrpouyan, J. Gardner, and S. Reese, "A covert system identification attack on constant setpoint control systems," in *2019 Seventh International Symposium on Computing and Networking Workshops (CANDARW)*, pp. 367–373, IEEE, 2019.

[5] M. Jishkariani, "Fault tree analysis (fta) for energy enterprises," *Retrievedfrom https://www. researchgate. net/publication/341494947_Fault_Tree_Analysis_FTA_For _Energy_Enterprises*, 2020.

[6] W. Depamelaere, L. Lemaire, J. Vossaert, and V. Naessens, "Cps security assessment using automatically generated attack trees," in *Proceedings of the 5th international symposium for ICS & SCADA cyber security research 2018*, British Computer Society (BCS), 2018.

[7] B. Krumay, E. W. Bernroider, and R. Walser, "Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the nist cybersecurity framework," in *Nordic Conference on Secure IT Systems*, pp. 369–384, Springer, 2018.

[8] S. G. Freeman, C. St Michel, R. Smith, and M. Assante, "Consequence-driven cyber-informed engineering (cce)," tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2016.

[9] A. A. Bochman and S. Freeman, *Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE).* CRC Press, 2021.

[10] R. S. Anderson, J. Benjamin, V. L. Wright, L. Quinones, and J. Paz, "Cyber-informed engineering," tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2017.

[11] L. Maglaras, M. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, and S. Rallis, "Threats, countermeasures and attribution of cyber attacks on critical infrastructures," *EAI Endorsed Transactions on Security and Safety*, vol. 5, no. 16, 2018.

[12] N. Tuptuk, P. Hazell, J. Watson, and S. Hailes, "A systematic review of the state of cyber-security in water systems," *Water*, vol. 13, no. 1, p. 81, 2021.

[13] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, 2015.

[14] C. M. Ahmed, J. Zhou, and A. P. Mathur, "Noise matters: Using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in cps," in *Proceedings of the 34th Annual Computer Security Applications Conference*, pp. 566–581, 2018.

[15] D. K. Yadav, P. Kannan, and S. Mansor, "Evaluating an aircraft response to disturbances caused by vibration frequency of wind forces during landing," *Journal of aerospace technology and management*, vol. 14, 2022.

[16] S. G. Freeman, "Consequence prioritization process for potential high consequence events (hce)," tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2016.

[17] A. P. Subriadi and N. F. Najwa, "The consistency analysis of failure mode and effect analysis (fmea) in information technology risk assessment," *Heliyon*, vol. 6, no. 1, p. e03161, 2020.

[18] S. Verma, T. Gruber, C. Schmittner, and P. Puschner, "Security risk assessment via attack tree,"

[19] B. Hyder and M. Govindarasu, "A novel methodology for cybersecurity investment optimization in smart grids using attack-defense trees and game theory," in *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pp. 1–5, IEEE, 2022.

[20] C. Agbo and H. Mehrpouyan, "Conflict analysis and resolution of safety and security boundary conditions for industrial control systems," in *2022 6th International Conference on System Reliability and Safety (ICSRS)*, pp. 145–156, IEEE, 2022.

[21] P. L. Turner, T. A. Wheeler, and M. Gibson, "Risk informed cyber security for nuclear power plants.," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2017.

[22] J. Alanen, J. Linnosmaa, J. Pärssinen, A. Kotelba, and E. Heikkilä, "Review of cybersecurity risk analysis methods and tools for safety critical industrial control systems," 2022.

[23] H. L. Hassani, A. Bahnasse, E. Martin, C. Roland, O. Bouattane, and M. E. M. Diouri, "Vulnerability and security risk assessment in a iiot environment in compliance with standard iec 62443," *Procedia Computer Science*, vol. 191, pp. 33–40, 2021.

[24] A. Clark, "Cyber process hazard analysis and risk management.," tech. rep., Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), 2021.

[25] A. K. Singh, R. S. Kumar, and A. Pusti, "Consequence analysis of most hazardous initiating event in electrical energy storage systems using event tree analysis," *Journal of Failure Analysis and Prevention*, pp. 1–11, 2022.

[26] S. Jauhar, B. Chen, W. G. Temple, X. Dong, Z. Kalbarczyk, W. H. Sanders, and D. M. Nicol, "Model-based cybersecurity assessment with nescor smart grid failure scenarios," in *2015 IEEE 21st Pacific Rim international symposium on dependable computing (PRDC)*, pp. 319–324, IEEE, 2015.

[27] T. Sommestad, M. Ekstedt, and H. Holm, "The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures," *IEEE Systems Journal*, vol. 7, no. 3, pp. 363–373, 2012.

[28] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke, "Model-based security metrics using adversary view security evaluation (advise)," in *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, pp. 191–200, IEEE, 2011.

[29] A. A. Abdulhameed, R. J. Al-Azawi, and B. M. Al-Mahdawi, "Modeling web security analysis attacks with cysemol tool," *Al-Mustansiriyah Journal of Science*, vol. 31, no. 3, pp. 101–109, 2020.

[30] L. Lemaire, J. Vossaert, B. De Decker, and V. Naessens, "An assessment of security analysis tools for cyber-physical systems," in *Risk Assessment and Risk-Driven Quality Assurance: 4th International Workshop, RISK 2016, Held in Conjunction with ICTSS 2016, Graz, Austria, October 18, 2016, Revised Selected Papers 4*, pp. 66–81, Springer, 2017.

[31] M. Barrère and E. C. Lupu, "Naggen: A network attack graph generation tool—ieee cns 17 poster," in *2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 378–379, IEEE, 2017.

[32] J. G. Torres-Toledano and L. E. Sucar, "Bayesian networks for reliability analysis of complex systems," in *Progress in Artificial Intelligence—IBERAMIA 98: 6th Ibero-American Conference on AI Lisbon, Portugal, October 5–9, 1998 Proceedings 6*, pp. 195–206, Springer, 1998.

[33] M. Neil, N. Fenton, and L. Nielson, "Building large-scale bayesian networks," *The Knowledge Engineering Review*, vol. 15, no. 3, pp. 257–284, 2000.

[34] L. Lemaire, J. Vossaert, J. Jansen, and V. Naessens, "Extracting vulnerabilities in industrial control systems using a knowledge-based system," in *3rd International Symposium for ICS & SCADA Cyber Security Research 2015*, pp. 1–10, BCS Learning & Development Ltd.; North Star House, North Star Avenue . . . , 2015.

[35] G. Kabir, S. Tesfamariam, A. Francisque, and R. Sadiq, "Evaluating risk of water mains failure using a bayesian

belief network model," *European Journal of Operational Research*, vol. 240, no. 1, pp. 220–234, 2015.

[36] H. Zerrouki and H. Smadi, "Bayesian belief network used in the chemical and process industry: a review and application," *Journal of Failure Analysis and Prevention*, vol. 17, no. 1, pp. 159–165, 2017.

[37] G. Kabir, N. B. C. Balek, and S. Tesfamariam, "Consequence-based framework for buried infrastructure systems: A bayesian belief network model," *Reliability Engineering & System Safety*, vol. 180, pp. 290–301, 2018.

[38] J. A. Buriticá and S. Tesfamariam, "Consequence-based framework for electric power providers using bayesian belief network," *International Journal of Electrical Power & Energy Systems*, vol. 64, pp. 233–241, 2015.

[39] R. Zhu, X. Li, X. Hu, and D. Hu, "Risk analysis of chemical plant explosion accidents based on bayesian network," *Sustainability*, vol. 12, no. 1, p. 137, 2019.

[40] G. F. Cooper and E. Herskovits, "A bayesian method for the induction of probabilistic networks from data," *Machine learning*, vol. 9, no. 4, pp. 309–347, 1992.

[41] M. Reif, J. R. Gellner, C. P. St Michel, and D. G. Kuipers, "Cce case study: Stinky cheese company," tech. rep., Idaho National Lab.(INL), Idaho Falls, ID (United States), 2020.

[42] K.-R. Liu, C.-W. Chen, and Y.-S. Shen, "Using bayesian belief networks to support health risk assessment for sewer workers," *International Journal of Environmental Science and Technology*, vol. 10, no. 2, pp. 385–394, 2013.

[43] L. BayesFusion, "Genie modeler—user manual," *BayesFusion, LLC*, vol. 524, 2017.

[44] U. Kjærulff and L. C. Van Der Gaag, "Making sensitivity analysis computationally efficient," *arXiv preprint arXiv:1301.3868*, 2013.

[45] Y. Wan, C. Liu, and W. Qiao, "An safety assessment model of ship collision based on bayesian network," in *2019 European Navigation Conference (ENC)*, pp. 1–4, IEEE, 2019.

[46] L. Li and Z. Fang, "Cause analysis of coal mine gas explosion based on bayesian network," *Shock and Vibration*, vol. 2022, 2022.

[47] P. Gao, W. Li, Y. Sun, and S. Liu, "Risk assessment for gas transmission station based on cloud model based multilevel bayesian network from the perspective of multi-flow intersecting theory," *Process Safety and Environmental Protection*, vol. 159, pp. 887–898, 2022.

[48] B. Békési, "System safety program requirements," *REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK 2000/1: pp. 41-50.(2000)*, 2000.

[49] R. Lanotte, M. Merro, A. Munteanu, and L. Vigano, "A formal approach to physics-based attacks in cyber-physical systems," *ACM Transactions on Privacy and Security (TOPS)*, vol. 23, no. 1, pp. 1–41, 2020.

[50] CISA, "Compromise of u.s water treatment plant," 2021.

[51] CISA, "Cyber-attack against ukrainian critical infrastructure," 2016.

[52] J. R. Reeder and C. T. Hall, "Cybersecurity's pearl harbor moment: Lessons learned from the colonial pipeline ransomware attack," 2021.

[53] U. Kjærulff and L. C. van der Gaag, "Making sensitivity analysis computationally efficient," in *Proceedings of the Sixteenth conference on Uncertainty in artificial intelligence*, UAI'00, (San Francisco, CA, USA), pp. 317–325, Morgan Kaufmann Publishers Inc., June 2000.

[54] D. Kushner, "The real story of stuxnet," *ieee Spectrum*, vol. 50, no. 3, pp. 48–53, 2013.

[55] J. Lawrence, J. Hollern, B. Geddes, B. Geddes, S. Freeman, M. Reif, and C. Reiger, "Fossil power plant cyber security life-cycle risk reduction, a practical framework for implementation," tech. rep., Electric Power Research Institute, Palo Alto, CA (United States); Idaho ..., 2020.

[56] J. J. Downs and E. F. Vogel, "A plant-wide industrial process control problem," *Computers & chemical engineering*, vol. 17, no. 3, pp. 245–255, 1993.

[57] G. Chen and T. J. McAvoy, "Predictive on-line monitoring of continuous processes," *Journal of Process Control*, vol. 8, no. 5-6, pp. 409–420, 1998.

[58] F. Capaci, E. Vanhatalo, M. Kulahci, and B. Bergquist, "The revised tennessee eastman process simulator as testbed for spc and doe methods," *Quality Engineering*, vol. 31, no. 2, pp. 212–229, 2019.

[59] M. Krotofil, A. A. Cárdenas, B. Manning, and J. Larsen, "Cps: Driving cyber-physical systems to unsafe operating conditions by timing dos attacks on sensor signals," in *Proceedings of the 30th Annual Computer Security Applications Conference*, pp. 146–155, 2014.

[60] J. Liu, W. Zhang, T. Ma, Z. Tang, Y. Xie, W. Gui, and J. P. Niyoyita, "Toward security monitoring of industrial cyber-physical systems via hierarchically distributed intrusion detection," *Expert Systems with Applications*, vol. 158, p. 113578, 2020.

[61] M. Segovia, J. Rubio-Hernan, A. R. Cavalli, and J. Garcia-Alfaro, "Cyber-resilience evaluation of cyber-physical systems," in *2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, pp. 1–8, IEEE, 2020.

[62] C. Gao, H. Park, and A. Easwaran, "An anomaly detection framework for digital twin driven cyber-physical systems," in *Proceedings of the ACM/IEEE 12th International Conference on Cyber-Physical Systems*, pp. 44–54, 2021.

[63] A. Ghafouri, Y. Vorobeychik, and X. Koutsoukos, "Adversarial regression for detecting attacks in cyber-physical systems," *arXiv preprint arXiv:1804.11022*, 2018.

[64] A. Bathelt, N. L. Ricker, and M. Jelali, "Revision of the tennessee eastman process model," *IFAC-PapersOnLine*, vol. 48, no. 8, pp. 309–314, 2015.