Dynamic Probabilistic Risk Assessment for Cyber Security Risk Analysis in Nuclear Reactors.

Pavan Kumar Vaddi[a], Yunfei Zhao[a], and Carol Smidts[a]
[a] Department of Mechanical and Aerospace Engineering, The Ohio State University, Columbus.
vaddi.3@osu.edu, zhao.2263@osu, smidts.1@osu.edu

Abstract: The increasing adaptation of nuclear power plants to incorporate software-based components along with digital communication networks in their operation has resulted in improved control, automation, monitoring and diagnostics, while simultaneously opening those power plants to a new dimension of risk, cyber-attacks. Additionally, the attackers have become more knowledgeable about the vulnerabilities associated with such software systems and network architectures. Hence there is a need to systematically study and quantify the risks associated with cyber-attacks on NPPs and the existing cyber defenses. In this paper we present a dynamic probabilistic risk assessment (DPRA) framework for nuclear power plants in the context of cyber security. In addition to stochastic events such as component failures, the framework implements cyber-attacks along with defenders' i.e., the plant operators, and the attackers' behaviors and their interactions in a game theory-based framework.

1. INTRODUCTION

The primary objectives of probabilistic risk assessment (PRA) are identifying "*what can go wrong*," i.e., identifying the initiating events and the possible sequences of events that can result in undesirable consequences, establishing "*what are the consequences if something went wrong*" i.e., identifying and evaluating the above-mentioned potentially *risky* consequences when something actually goes wrong i.e., when the initiating events occur and evolve, and quantifying "*how likely it is for something to go wrong*," i.e., computing the likelihood of occurrence of the above-mentioned initiating events and the probabilities that those initiating events evolve into said dangerous scenarios [1], [2]. An initiating event in PRA of nuclear power plants (NPP), is defined as "*any event that creates a disturbance in the plant that has the potential to lead to core damage, depending on the successful operation of the required mitigation systems in the plant*," [3]. While component failures either hardware or digital, or human operator errors are implicitly considered as initiating events, the increasing installation of networked digital systems in nuclear power plants makes it essential to expand the definition of initiating events to consider the relevant cyber events, either intentional cyber-attacks or unintentional events because such events in industrial control systems (ICS) have implications in the physical world, and consequently it is necessary to expand NPP PRA to the field of cyber security.

Extending the classical definition that risk can be quantified as "*the product of expected frequency of occurrence of events and the damage resulting from those events*" [4], Park and Lee [5] defined the risk of a cyber-attack as the product of the following three terms: the frequency of occurrence of cyber-attacks, the conditional probability that a cyber-attack will result in an event of significance, and the damage caused by that event. Additionally, Park and Lee [5] considered cyber-attacks as basic events, integrated those into fault trees and computed the risk due to cyber-attacks in terms of increase in core damage frequency metrics. However, it is important to understand that in the context of cyber-attacks, the evolution of the system depends on the actions of both the attacker and the defender i.e., the operator. The subsequent actions of the defender and the attacker also depend on the state of the system and on each other's actions. Taking this into account, Zhao et al. [6], [7] modeled the interaction between the defender and the attacker as a stochastic game and computed the probability of reaching an undesirable state as well as the probability of discrete system states, using both analytical and Monte Carlo simulation methods. However, the state transitions in the game model were defined using classical event trees.

While classical PRA methods such as fault trees and event trees can help us understand and identify what can go wrong, these methods are lacking in establishing how something can go wrong. Classical PRA approaches are limited in the following aspects: modeling and incorporating the changes of system properties as functions of physics and time, for example failure rates of components are dependent on physical conditions, modeling the changes in the behavior of human operators with respect to system states and time, for example the operator can be under a significant amount of stress depending on the state of the system, and capturing the evolution of the system over time due to events such as random component failures or operator errors. Dynamic probabilistic risk assessment (DPRA), a set of probabilistic risk assessment techniques that uses deterministic physics based dynamic models of the system to study its evolution in the context of random events [8], [9] can overcome the limitations of classical PRA and provide more accurate estimates of risk. The field of dynamic probabilistic risk assessment is well established, taking initiating events such as failure of hardware components either due to aging or random failures [8], [10], failure of digital systems [11] and human operator errors [12]–[14] into consideration. Devooght and Smidts [8], [12] presented the continuous event tree approach, a continuous time DPRA method, and presented a single integral equation and its differential form to model the system evolution in the presence of random events such as equipment failures, operator actions and operator errors.

It is important to understand that cyber-attacks on NPPs impact the physical world and affect the evolution of physical systems over time. Additionally, the behavior and strategies of the attacker and the operator will depend on the state of the system, and assuming that attacker and the defender act rationally, their actions are directed towards maximizing long term benefit which is dependent on the evolution of the system. Hence it is imperative that physics of the system must be explicitly considered to accurately evaluate the risks associated with cyber-attacks on nuclear power plants, and thus DPRA is a valid framework for the purpose.

While Zhao et al. [7] modeled the dynamics of attacker-defender interaction in the context of cyber-attacks on nuclear power plants, the physics of the system was not explicitly modeled. In subsequent research Zhao et al. [15] used DPRA for cybersecurity risk analysis of electric grids, but game theory based attacker and defender interaction was not modeled. In this paper we present a DPRA simulation architecture for cybersecurity risk analysis that incorporates both the system model and game theory based analysis of the interaction between the operator and the attacker, expand the theory of continuous trees to the context of cyber-attacks under a Markovian assumption, and provide the corresponding mathematical formulation. We consider a procedure following operator and operator errors are not explicitly modeled separately, but our equations can be expanded to consider those cases.

2. DPRA SIMULATION ARCHITECTURE FOR CYBER SECURITY RISK ANALYSIS

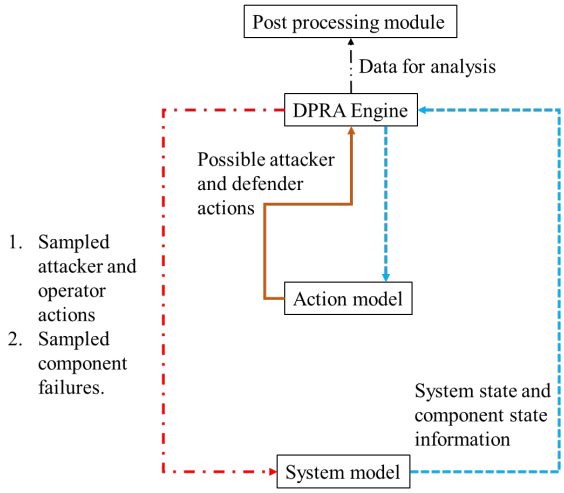
DPRA involves the use of deterministic physics based model of the system in order to study its evolution in the presence of random events such as component failures, operator errors. As such, to perform DPRA analysis, a system model is required along with and a DPRA engine that schedules and implements the above mentioned random events on the system model. In this research we expand the traditional DPRA analysis to the context of cyber-attacks i.e., we focus on incorporating the stochastic nature of the operator's as well as the attacker's actions using a game theory based framework in addition to component failures, and study their effects on the evolution of the system. Hence, the proposed DPRA simulation architecture has the following three elements:

1. the system model to emulate the evolution of the system under consideration, in this case a nuclear power plant.
2. The DPRA engine, that monitors the state of the system, and implements the sampled attacker and defender actions as well as randomly generated component failure scenarios [15].

3. The action model which generates a set of possible operator and attacker actions to be implemented on the system. In addition to the system model and the DPRA engine, we explicitly consider an action model that generates possible defender and attacker actions to be implemented on the system model using a game theory based analysis. The action model and its components are explained in this section.

Additionally, a post processing module is considered to analyse the large amounts of data generated during the simulations and compute meaningful risk metrics. Figure 1 depicts a high-level schematic of the DPRA simulation architecture used to perform cybersecurity risk analysis.

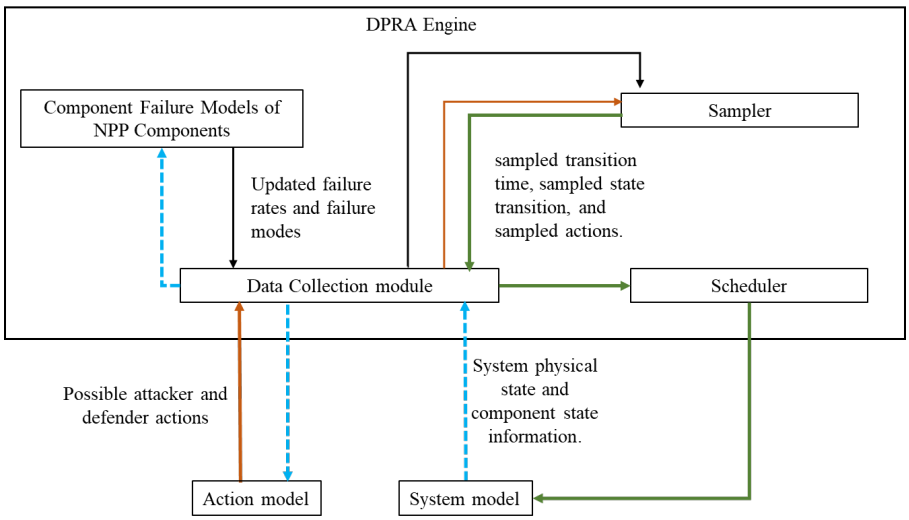
Figure 1. Schematic of the DPRA simulation architecture for cybersecurity risk analysis.



2.1. The DPRA Engine

Figure 2 depicts the elements of the DPRA engine in the proposed architecture, that generate or sample the scenarios to be implemented on the system model.

Figure 2. The DPRA Engine.



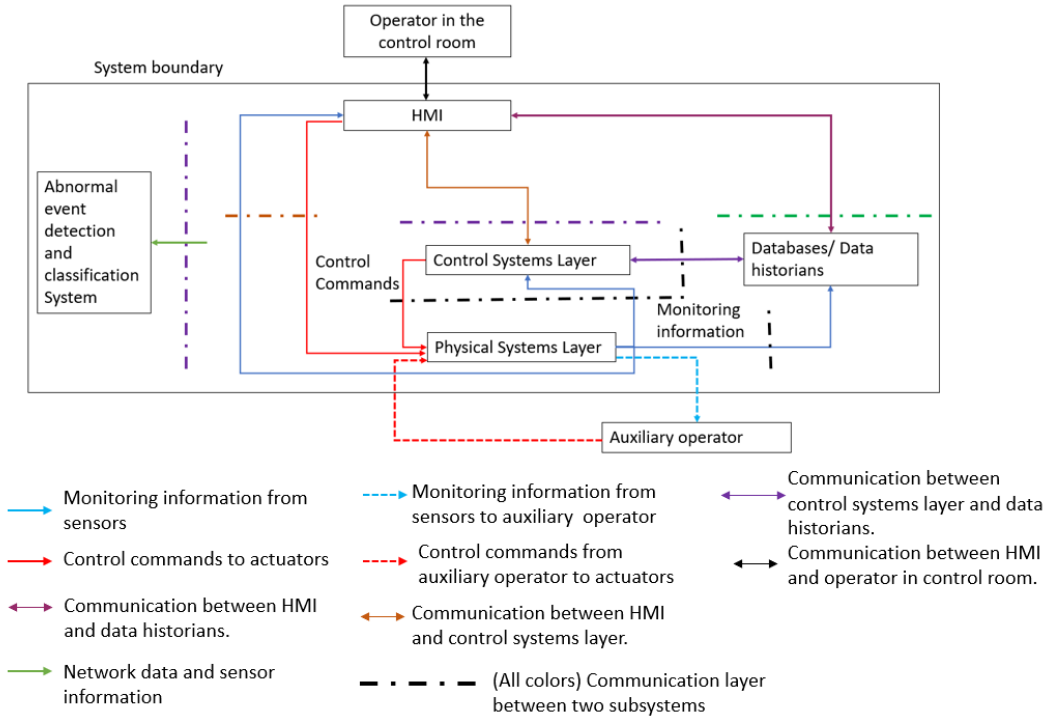
The data collection module of the DPRA engine receives the system physical state information i.e., a vector of relevant physical variables, and the current component state information from the system model. This information is disseminated to the component failure models element of the DPRA engine and the action model. Using this information as input, the component failure models element updates the failure rates and the failure modes of the NPP components and transmits the updated values back to the data collection module. Similarly, the action model returns a set of possible

attacker and defender actions to the data collection module. The output of the component failure models, and the action model received by the data collection module is transmitted to the sampler. The next state transition time, the next state transition to be implemented on the system model from the set of failure modes generated by the component failure models and the next operator and attacker actions to be enforced on the system model form the inputs received from the action model are sampled by the Sampler element of the DPRA engine and provided to the data collection module. The data collection module then shares this information with the scheduler, which then implements the sampled transitions and the sample actions on the system model. The data collection module assimilates all the data generated by all the elements of the DPRA architecture. This data is sent to the post processing module for analysis and computation of relevant risk metrics.

2.2. The System Model

Figure 3 presents a simplified structure of nuclear power plant system. The system model consists of mathematical models of the components in the physical systems layer under different states, mathematical models of the controllers, and the models of other network elements. The objective of the system model is to simulate the evolution of the physical system when subjected to stochastic events such as component failures and cyber-attacks. We consider an abnormal event detection and classification system that can detect an abnormal event and differentiate it as either a safety event caused by component failure or a cyber-attack. This is used to explore scenarios of undetected attackers and evaluate the associated risks. It is our opinion that the scenarios in which a cyber-attack is undetected, resulting in the operator taking incorrect actions should be studied from a risk perspective.

Figure 3. The System Structure in a Nuclear Power Plant.



2.3. The Action Model

Figure 4 depicts the action model. The action model receives system monitoring information i.e., information about the system state as defined by the vector of a list of physical variables and vector of component states and generates a set of possible attacker and operator actions. As presented in Figure 4, the action model has three individual models, the procedure model, the undetected attacker model and the game model. In this research we assume that the operator is procedure following and is not

prone to errors. The procedure model is used to generate possible operator actions when no cyber attack is detected by the abnormal event detection module in the system model. The undetected attacker model is used to represent and model initial launching of cyber-attacks and the scenarios in which a cyber-attack remains undiagnosed.

Figure 4. The Action Model.

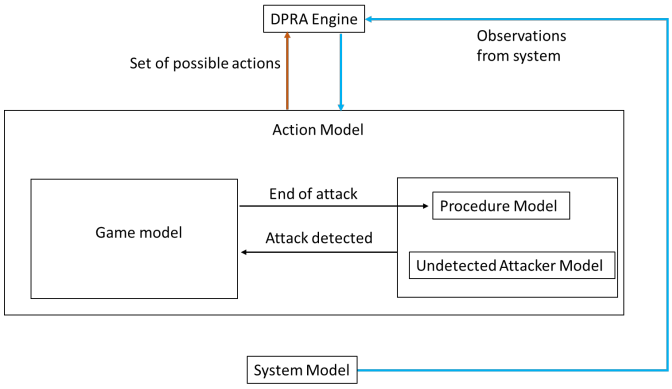
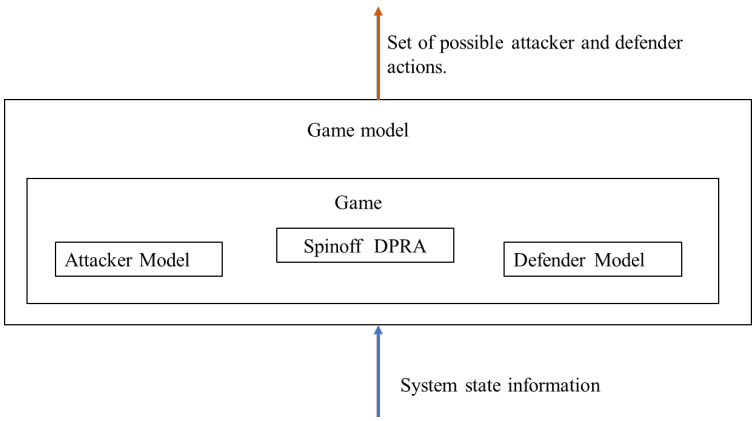


Figure 5 represents the game model. The action model switches to the game model whenever a cyber-attack is detected in the system. In the presence of a cyber-attack, the operator takes the role of a defender. The components of the game model are the game itself of which the attacker and defender(s) are the players, and a spinoff DPRA process. The optimal attacker and defender actions depend on the physics of the system. We want to consider the computation of optimal actions based on physics and implement those on the system to observe it's evolution. So, as part of the spinoff DPRA process, we simulate i.e., run a parallel model to predict of the system behaviour under different pairs of attacker and defender actions to a certain time point in the future and use that knowledge to inform the attacker and defender policies in the original DPRA process.

Figure 5. The Game Model



3. CONTINUOUS EVENT TREES FOR CYBERSECURITY RISK ANALYSIS

In this section we present the mathematical formulation of continuous event trees for cybersecurity risk analysis. With the theory of continuous event trees presented by Devooght and Smidts [8] as reference, we describe the nuclear power plant system as follows:

The physical state of a nuclear power plant is represented using a state vector, $\bar{x}$, a vector of physical variables such as pressure, flowrate, temperature etc. It is implicit that $\bar{x} \in \mathbb{R}^n$ is a point in continuous space with its boundaries determined by the physics. Let $\mathbb{X} \subset \mathbb{R}^n$ represent the space of all possible physical state vectors $\bar{x}$.

The states of the components in the NPP are represented using a vector i, a vector on a discrete space. In this research we limit ourselves to only discrete component states such as normal or failed states. Integers can be used to represent such discrete states of components. For example 0, 1 and 2 can be used to denote that a component is in normal state or failed state or compromised state respectively. Consider an example system with three components, a digital controller, a digital sensor and a mechanical valve. Then $i = [i_1, i_2, i_3]$ where i_1, i_2, and i_3 represent the states of the controller, the sensor and the valve respectively. Here, $i_1, i_2 \in \{0, 1, 2\}$ and $i_3 \in \{0, 1\}$ because the digital controller and the sensor can be compromised whereas the mechanical valve cannot be subjected to cyber-attacks. Let $\mathbb{C}$ represent the set of all possible component states.

$D = \{d_1, d_2, d_3 \dots\}$ is the defender's action space and $A = \{a_1, a_2, a_3 \dots\}$ is the attacker's action space. We assume that the defender and the attacker action spaces are discrete, with actions such as switch from main controller to backup controller or compromise the controller and shut down the pump etc. Continuous action spaces will be studied in future research. It is implicit that feasible defender and attacker actions depend on the physical state as well as the state of components. For example, we assume that a component that has been compromised by the attacker cannot be compromised again and remains in that state, until it is "*repaired*." Additionally, certain actions may not be physically possible depending on the physical state of system. For example, the speed of a pump cannot be reduced to zero instantaneously.

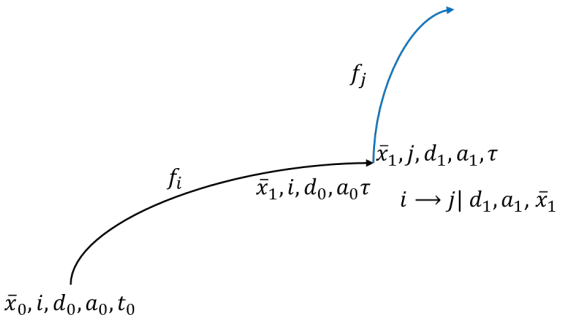
At any time t, the overall system state of the NPP is represented using the tuple $(\bar{x}, i, d, a, t)$, where the physical state vector $\bar{x}$ represents the physical system state, the component state is represented by the vector i, and the couple (d, a) represents the latest pair of actions taken by the defender and the attacker respectively. For the remainder of this paper the expressions physical state vector and physical state will be used interchangeably. The same is true for the expressions component state vector and component state.

A system of differential equations as presented by equation (1) can be used to represent the trajectory of the NPP in the physical state space [8].

$$\frac{\partial}{\partial t}\bar{x} = f_i(\bar{x}, t) \tag{1}$$

It is implicit that these differential equations are dependent on the states of the components i.e., when the states of components change, the differential equations representing the dynamics of the system will change and the system follows a different trajectory in the state space, as shown in Figure 6.

Figure 6. Example of trajectories in state space.



The component state i can change either due to random component failures or due to the actions of the defender and the attacker. Additionally, it is implicit that defender and attacker cannot directly interfere with the physical process and can only change the component state vector, which in turn will change the trajectory of system evolution i.e., the trajectory of the reactor in the physical state space is conditionally independent of the actions of the attacker and the defender given the component state vector. In the example depicted in Figure 6, initially the system is in the state $(\bar{x}_0, i, d_0, a_0, t_0)$, and

evolves along the trajectory defined by f_i until time τ, where the physical state vector is $\bar{x}_1$. The defender and the attacker then take actions (d_1, a_1) at $(\bar{x}_1, \tau)$ and the component state vector transitions from i to j as a result, following which the system evolves along the trajectory defined by f_j. In this paper we assume that the component state transitions due to attacker and defender actions if any, are instantaneous. Delayed transitions will be studied in future research.

Let equation (2) represent the solution to the system of differential equations presented in equation (1), where $\bar{x}_0$ is the initial condition [8]. It is implicit that for time $t = 0$, $\bar{x}_0 = g_i(0, \bar{x}_0)$. It is also implicit that f_i and g_i represent the same trajectories in the physical state space given the component state vector i.

$$\bar{x}(t) = g_i(t, \bar{x}_0) \tag{2}$$

Let the probability density of the overall system state $(\bar{x}, j, d, a, t)$at time t be $\pi(\bar{x}, i, d, a, t)$. Let the conditional probability density that the system is in state $(\bar{x}, j, d, a, t)$at time t, given the initial state $(\bar{x}_0,\ i, d_0, a_0, t_0)$ be denoted by $\pi(\bar{x}, j, d, a, t|\bar{x}_0, i, d_0, a_0, t_0)$ [8]. It is implicit that:

$$\pi(\bar{x}, j, d, a, t_0|\bar{x}_0, i, d_0, a_0, t_0) = \delta(\bar{x} - \bar{x}_0) \times \delta_{ij} \times \delta_{(d_0,a_0),(d,a)} \tag{3}$$

where δ is the Dirac delta function, and δ_{ij} and $\delta_{(d_0,a_0),(d,a)}$ are Kronecker delta functions. The objective of this research is to compute the value $\pi(\bar{x}, i, d, a, t)$ and to consequently estimate the probability that the physical state of the reactor is in a certain region of the state space at any given instant of time.

As discussed above, the trajectories in physical state space are determined by the component state vector. The component state vector can change either due to random failures of components or due to the actions of the attacker and the defender. In summary, the trajectories in the physical state space are dependent on the substate (i, d, a).

Let $\lambda_{i,d,a}(\bar{x})\Delta t$ be the conditional probability that there is a transition out of the substate (i, d, a) in the interval Δt, when the system is in state $(\bar{x}, j, d, a, t)$. The failure rates of the components are dependent on the physical state $\bar{x}$. Let $p_s(i \to j|\bar{x})\Delta t$ be the conditional probability that the component state transitions from i to j in the interval Δt explicitly due to random component failures when the physical state vector is $\bar{x}$ and the defender and attacker take no new actions. Additionally, the physical state $\bar{x}$ influences the actions of the defender as well as the attacker. Let $p_c(i \to j|d', a', \bar{x})\Delta t$ be the conditional probability that the component state transitions from i to j in the interval Δt when the defender and attacker take new actions d' and a' respectively at the physical state $\bar{x}$. The relation between $\lambda_{i,d,a}(\bar{x})$, $p_s(i \to j|\bar{x})$ and $p_c(i \to j|d', a', \bar{x})$ is presented in equation (4) where $p(d, a \to d', a')$ is the probability that the defender and the attacker take new actions d', a' respectively.

$$\lambda_{i,d,a}(\bar{x}) = \sum_{j \neq i} p_s(i \to j|\bar{x}) + \sum_{d\prime, a\prime \neq d,a} p(d, a \to d', a'|\bar{x}) \times \sum_{j} p_c(i \to j|d', a', \bar{x}) \tag{4}$$

If the overall system state is $(\bar{x}_0, i, d, a, t_0)$ initially, then the probability density that the system reaches the physical state $\bar{x}$ at time t while remaining in the substate (i, d, a) until time t is given by the product $\delta[\bar{x} - g_i(t - t_0, \bar{x}_0)] \times e^{-\int_{t_0}^{t} \lambda_{i,d,a}[g_i(s,\bar{x}_0)]ds}$ where the term $e^{-\int_{t_0}^{t} \lambda_{i,d,a}[g_i(s,\bar{x}_0)]ds}$ represents the probability that the system remains in the state (i, d, a) and consequently evolves along the trajectory defined by g_i during the interval $[t_0, t]$ and the term $\delta[\bar{x} - g_i(t - t_0, \bar{x}_0)]$ represents the probability density that $(\bar{x}, t)$ is the only point reachable from $(\bar{x}_0, t_0)$ along the trajectory defined by g_i [8].

3.1. The Extended Continuous Event Tree Equation

Equation (5) presents the integral form of the continuous event tree equation based on the Chapman-Kolmogorov equation [8] extended to the cyber-attack case to compute the probability density that the system is in state $(\bar{x}, i, d, a, t)$ at time t.

$$\pi(\bar{x}, i, d, a, t) \tag{5}$$
$$= \left[\int_{\mathbb{X}} \pi(\bar{u}, i, d, a, 0) \times \delta[\bar{x} - g_i(t, \bar{u})] \times \left(e^{-\int_0^t \lambda_{i,d,a}[g_i(s,\bar{u})]ds}\right) d\bar{u}\right]$$
$$+ \left[\sum_{j \neq i} \int_{\mathbb{X}} \left\{\int_0^t p(j \rightarrow i|\bar{u}) \times \pi(\bar{u}, j, d, a, \tau) \times \delta[\bar{x} - g_i(t-\tau, \bar{u})] \times \left(e^{-\int_\tau^t \lambda_{i,d,a}[g_i(s,\bar{u})]ds}\right) d\tau\right\} d\bar{u}\right]$$
$$+ \left[\sum_{d\prime, a\prime \neq d,a} \sum_j \int_{\mathbb{X}} \left\{\int_0^t \pi(\bar{u}, j, d', a', \tau) \times p(d', a' \rightarrow d, a|\bar{u}, j, \tau) \times p(j \rightarrow i|d, a, \bar{u}) \times \delta[\bar{x} - g_i(t-\tau, \bar{u})] \times \left(e^{-\int_\tau^t \lambda_{i,d,a}[g_i(s,\bar{u})]ds}\right) d\tau\right\} d\bar{u}\right]$$

The equation has the following 3 major parts (as separated by the square parantheses):

1. $\int_{\mathbb{X}} \pi(\bar{u}, i, d, a, 0) \times \delta[\bar{x} - g_i(t, \bar{u})] \times \left(e^{-\int_0^t \lambda_{i,d,a}[g_i(s,\bar{u})]ds}\right) d\bar{u}$– This integrand represents the probability density that the system is initially in the state $(\bar{u}, i, d, a, 0)$, and reaches the physical state $\bar{x}$ at time t while remaining in the substate (i, d, a) until time t, along the trajectory defined by g_i. While the integral is computed over the entire physical state space $\mathbb{X}$ is considered, the Dirac delta function $\delta[\bar{x} - g_i(t, \bar{u})]$ ensures that only a specific subset of appropriate $\bar{u}$ values are valid.

2. $\sum_{j \neq i} \int_{\mathbb{X}} \left\{\int_0^t p(j \rightarrow i|\bar{u}) \times \pi(\bar{u}, j, d, a, \tau) \times \delta[\bar{x} - g_i(t-\tau, \bar{u})] \times \left(e^{-\int_\tau^t \lambda_{i,d,a}[g_i(s,\bar{u})]ds}\right) d\tau\right\} d\bar{u}$– The inner most integrand in the second part represents the probability density that the system is in state $(\bar{u}, j, d, a, \tau)$ at some intermediate time τ between 0 and t, when the component state transitions from j to i due to a random event and not due to attacker and defender actions, and after that the system evolves along the trajectory defined by g_i while remaining in the state (i, d, a) from time τ to t, and eventually reaches the physical system state $\bar{x}$ at time t. The sum of this probability density over all possible $(\bar{u}, j, \tau)$ is computed. The second part of equation (5) is recursive in nature, similar to the Chapman-Kolmogorov equation [8].

3. $\sum_{d\prime, a\prime \neq d,a} \sum_j \int_{\mathbb{X}} \left\{\int_0^t \pi(\bar{u}, j, d', a', \tau) \times p(d', a' \rightarrow d, a|\bar{u}, j, \tau) \times p(j \rightarrow i|d, a, \bar{u}) \times \delta[\bar{x} - g_i(t-\tau, \bar{u})] \times \left(e^{-\int_\tau^t \lambda_{i,d,a}[g_i(s,\bar{u})]ds}\right) d\tau\right\} d\bar{u}$ – The inner most integrand of the third term represents the probability density that the system is in state $(\bar{u}, j, d', a', \tau)$ at some time τ between 0 and t, at which point the defender and the attacker take new actions (d, a) as a result of which the component state transitions from j to i and subsequently the system evolves along the trajectory defined by g_i, while remaining in the substate (i, d, a) from time τ to t and eventually arrives at the physical system state $\bar{x}$ at time t. The probability that the defender and the attacker take a new pair of actions $p(d', a' \rightarrow d, a|\bar{u}, j, \tau)$ i.e., the mixed equilibrium strategies of the defender and the attacker at physical state $\bar{u}$, component state j and time τ can be computed using a game theory based approach. It can also be observed that the third term of equation (5) is recursive in nature as well.

The conditional probability density $\pi(\bar{x}, i, d, a, t|\bar{x}_0, i_0, d_0, a_0, t_0)$ that the system is in the state $(\bar{x}, i, d, a, t)$ at time t given that it was initially in the state $(\bar{x}_0, i_0, d_0, a_0, t_0)$ can be computed using equation (6) (see equation (3)).

$$\pi(\bar{x}, i, d, a, t|\bar{x}_0, i_0, d_0, a_0, t_0) \tag{5}$$
$$= \left[\int_{\mathbb{X}} \delta[\bar{x}_0 - \bar{u}] \times \delta_{ii_0} \times \delta_{(d_0,a_0)(d,a)} \times \delta[\bar{x} - g_i(t - t_0, \bar{u})] \times \left(e^{-\int_0^t \lambda_{i,d,a}[g_i(s,\bar{u})]ds}\right) d\bar{u}\right]$$
$$+ \left[\sum_{j \neq i} \int_{\mathbb{X}} \left\{\int_{t_0}^{t} p(j \right.\right.$$
$$\left.\left. \rightarrow i|\bar{u}) \times \pi(\bar{u}, j, d, a, \tau|\bar{x}_0, i_0, d_0, a_0, t_0) \times \delta[\bar{x} - g_i(t - \tau, \bar{u})] \times \left(e^{-\int_\tau^t \lambda_{i,d,a}[g_i(s,\bar{u})]ds}\right) d\tau\right\} d\bar{u}\right]$$
$$+ \left[\sum_{d',a' \neq d,a} \sum_{j} \int_{\mathbb{X}} \left\{\int_{t_0}^{t} \pi(\bar{u}, j, d', a', \tau|\bar{x}_0, i_0, d_0, a_0, t_0) \times p(d', a' \rightarrow d, a|\bar{u}, j, \tau) \times p(j \right.\right.$$
$$\left.\left. \rightarrow i|d, a, \bar{u}) \times \delta[\bar{x} - g_i(t - \tau, \bar{u})] \times \left(e^{-\int_\tau^t \lambda_{i,d,a}[g_i(s,\bar{u})]ds}\right) d\tau\right\} d\bar{u}\right]$$

Equation (7) presents the expected cumulative rewards received by the players i.e., the defender and the attacker. Here α is used as an index and is not an exponent. $R^1(\bar{x}, i, d, a, t)$ and $R^2(\bar{x}, i, d, a, t)$ are the expected cumulative rewards received by the defender and the attacker respectively when the defender takes an action d and the attacker takes an action a at the physical system state $\bar{x}$, the component state i and time t. These rewards are used to compute the mixed strategies of the defender and the attacker using a game theory based approach [7]. The computation of mixed strategies is not explicitly discussed in this paper.

$$R^\alpha(\bar{x}, i, d, a, t) \tag{7}$$
$$= r^\alpha_{action}(\bar{x}, i, action^\alpha, t) + \sum_j p(i \rightarrow j|d, a, \bar{x}) \times [r^\alpha_{transition}(i, j)]$$
$$+ \sum_j p(i \rightarrow j|d, a, \bar{x}) \times \sum_k \sum_{d',a'} \int \left\{\int_t^{t_{mission}} \pi(\bar{u}, k, d', a', \tau|\bar{x}, j, d, a, t) \times R^\alpha(\bar{u}, k, d', a', \tau) d\tau\right\} du$$

It can be noticed that equation (5) is a recursive equation as well and the three terms in equation (5) are explained below:

1. $r^\alpha_{action}(\bar{x}, i, action^\alpha, t)$: $r^1_{action}(\bar{x}, i, d, t)$ is the cost incurred by the defender for taking the action d at the physical system state $\bar{x}$, the component state i and time t, while $r^2_{action}(\bar{x}, i, a, t)$ is the cost incurred by the attacker for taking the action a at the physical system state $\bar{x}$, the component state i and time t.

2. $\sum_j p(i \rightarrow j|d, a, \bar{x}) \times [r^\alpha_{transition}(i, j)]$ is the expected immediate reward received by the player α when there is a transition out of the component state i due to the pair of actions (d, a). The term $r^\alpha_{transition}(i, j)$ is the immediate reward received by the player α, when the component state transitions from i to j due to the pair of actions (d, a), where $p(i \rightarrow j|d, a, \bar{x})$ is the probability of that transition.

3. $\sum_j p(i \rightarrow j|d, a, \bar{x}) \times \sum_k \sum_{d',a'} \int \left\{\int_t^{t_{mission}} \pi(\bar{u}, k, d', a', \tau|\bar{x}, j, d, a, t) \times R^\alpha(\bar{u}, k, d', a', \tau) d\tau\right\} du$ – represents the expected future rewards received by the player α. At the physical system state $\bar{x}$, the component state i and time t, when the defender takes the action d and the attacker takes the action a there is an immediate transition in the component state from i to j, and the new system state is $(\bar{x}, j, d, a, t)$. The term $R^\alpha(\bar{u}, k, d', a', \tau)$ represents the reward received

by the player α at some future state $(\bar{u}, k, d', a', \tau)$ at time $t < \tau < t_{mission}$, physical system state $\bar{u}$ and component state k, when the defender takes action d' and the attacker takes an action a'. The term $\pi(\bar{u}, k, d', a', \tau | \bar{x}, j, d, a, t)$ represents the conditional probability density of arriving at the system state $(\bar{u}, k, d', a', \tau)$ given that the initial state is $(\bar{x}, j, d, a, t)$. The probability that the players take the pair of actions (d', a') at $(\bar{u}, k, \tau)$ is encoded in this conditional probability density.

4. CONCLUSIONS AND FUTURE WORK

The increasing digitalization of nuclear power plants and the growing prevalence of cyber-attacks on industrial control systems makes it necessary to study and quantify cybersecurity risks. The dynamic probabilistic risk assessment framework which includes a physics based model of the system and considers the timing of events such as component failures or operator errors and even cyber-attacks provides the most appropriate set of tools to quantify the risks associated with cyber-attacks on nuclear power plants.

In this paper we expanded the theory of continuous event trees to the context of cybersecurity and presented a Chapman-Kolmogorov equation based integral equation to calculate the probability density that the system is in a certain state at any instant of time. Additionally, we presented the equations to compute the expected cumulative rewards to be used in game theory based modeling of cyber-attacks. We presented an architecture to perform DPRA analysis for nuclear power plants cyber security. The proposed DPRA simulation architecture will be implemented and the continuous event trees framework for cybersecurity will be expanded to consider delayed state transitions and operator errors in future research.

Acknowledgements

This research is being performed using funding received from the DOE Office of Nuclear Energy's Nuclear Energy University Program.

References

[1] A. Mosleh, “PRA: A PERSPECTIVE ON STRENGTHS, CURRENT LIMITATIONS, AND POSSIBLE IMPROVEMENTS,” *Nucl. Eng. Technol.*, vol. 46, no. 1, pp. 1–10, Feb. 2014, doi: 10.5516/NET.03.2014.700.

[2] R. J. Breeding, T. J. Leahy, and J. Young, “Probabilistic risk assessment course documentation. Volume 1: PRA fundamentals,” Energy, Inc., Seattle, WA (USA), NUREG/CR-4350/1; SAND-85-1495/1, Aug. 1985. doi: 10.2172/6277413.

[3] International Atomic Energy Agency, “Defining initiating events for purposes of probabilistic safety assessment,” *IAEA-TECDOC-719, International Atomic Energy Agency*. 1993.

[4] N. J. McCormick, *Reliability and risk analysis: methods and nuclear power applications*. Academic Press New York, 1981.

[5] J. W. Park and S. J. Lee, “Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants,” *Nucl. Eng. Technol.*, vol. 51, no. 1, pp. 138–145, Feb. 2019, doi: 10.1016/j.net.2018.09.009.

[6] Y. Zhao, L. Huang, C. Smidts, and Q. Zhu, “A game theoretic approach for responding to cyber-attacks on nuclear power plants,” *Nucl. Sci. Eng.*, 2021.

[7] Y. Zhao, L. Huang, C. Smidts, and Q. Zhu, “Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants,” *Reliab. Eng. Syst. Saf.*, vol. 201, p. 106878, Sep. 2020, doi: 10.1016/j.ress.2020.106878.

[8] J. Devooght and C. Smidts, “Probabilistic Reactor Dynamics—I: The Theory of Continuous Event Trees,” *Nucl. Sci. Eng.*, vol. 111, no. 3, pp. 229–240, Jul. 1992, doi: 10.13182/NSE92-A23937.

[9] T. Aldemir, “A survey of dynamic methodologies for probabilistic safety assessment of nuclear power plants,” *Ann. Nucl. Energy*, vol. 52, pp. 113–124, Feb. 2013, doi: 10.1016/j.anucene.2012.08.001.
[10] C. Smidts and J. Devooght, “Probabilistic Reactor Dynamics—II: A Monte Carlo Study of a Fast Reactor Transient,” *Nucl. Sci. Eng.*, vol. 111, no. 3, pp. 241–256, Jul. 1992, doi: 10.13182/NSE92-A23938.
[11] T. Aldemir *et al.*, “NUREG/CR-6942: Dynamic Reliability Modeling of Digital Instrumentation and Control Systems for Nuclear Reactor Probabilistic Risk Assessments,” 2007.
[12] J. Devooght and C. Smidts, “Probabilistic Reactor Dynamics — III. A Framework for Time-Dependent Interaction between Operator and Reactor during a Transient Involving Human Error,” *Nucl. Sci. Eng.*, vol. 112, no. 2, pp. 101–113, Oct. 1992, doi: 10.13182/NSE92-A28407.
[13] C. Smidts, “Probabilistic Reactor Dynamics —IV. An Example of Man/Machine Interaction,” *Nucl. Sci. Eng.*, vol. 112, no. 2, pp. 114–126, Oct. 1992, doi: 10.13182/NSE92-A28408.
[14] K.-S. Hsueh and A. Mosleh, “The development and application of the accident dynamic simulator for dynamic probabilistic risk assessment of nuclear power plants,” *Reliab. Eng. Syst. Saf.*, vol. 52, no. 3, pp. 297–314, Jun. 1996, doi: 10.1016/0951-8320(95)00140-9.
[15] Y. Zhao *et al.*, “Dynamic Probabilistic Risk Assessment for Cyber Security Risk Analysis of the Electric Grid,” in *Proceedings of the 30th European Safety and Reliability Conference and 15th Probabilistic Safety Assessment and Management Conference*, 2020, pp. 2020–2027. doi: 10.3850/978-981-14-8593-0_5058-cd.