Journal of Communication Engineering (JCE)

P- ISSN: 2322-4088 Vol. 11, No. 1, Jan.-Jun. 2022 E- ISSN: 2322-3936

Security Evaluation of Cyber-physical Systems by Modeling Attacks Against Control Loops

H. Sepehrzadeh*

[Corresponding Author] Department of Computer Engineering; Technical and Vocational University (TVU); Tehran, Iran;
Email: h.sepehrzadeh@tvu.ac.ir

Received: *06 Feb. 2022* ***Revised:*** *18 May 2022* ***Accepted:*** *10 Jun. 2022*

Abstract: Cyber-physical systems (CPSs) are deeply intertwining and integrating the physical processes with cyber components. In these intelligent systems, a process is monitored and controlled by cyber systems and different types of sensitive information is exchanged in a real-time manner. Nowadays, the security of these systems has been considered increasingly. Connecting physical devices to the cyber network makes the critical infrastructures more vulnerable to the adversarial activities. The primary target of attacks against CPSs is often disrupting physical processes under control. Since, improving the security of CPSs has gained considerable importance nowadays. This paper presents a method for modeling the security of CPSs using stochastic Petri nets (SPNs). The proposed method models the system control loop associated with anomaly detection systems (ADSs) in normal behavior and under security attacks. By using this model, we can investigate the consequences of the integrity and denial of service attacks against CPSs and perform probabilistic and temporal analysis of the system under security attacks. By solving the proposed model, the security of CPSs is estimated in terms of metrics, such as mean-time-to-failure and availability. Finally, the security of a chemical plant is investigated as an illustrative example to represent the effectiveness of the proposed modeling method.

Index Terms: Cyber-physical Systems (CPSs), Security, Modeling, Quantitative Evaluation, Stochastic Petri Nets (SPNs).

Citation: H. Sepehrzadeh, “Security Evaluation of Cyber-Physical Systems by Modeling Attacks Against Control Loops,” *Journal of Communication Engineering*, vol. 11, no. 1, pp. 41-58, Jan.-Jun. 2024.

http://dx.doi.org/10.32598/Immunoregulation.6.2.1

I. INTRODUCTION

Cyber-Physical Systems (CPS) is defined as the integration of computing, communication and physical resources [1]. In these systems, cyber part monitors and manipulates physical objects and processes. Although this integration has had many advantages, however, it has exposed CPSsto security threats and risks [2]. These systems are being used in various domains and critical infrastructures such as power plants, smart grids, chemical plant, transportation systems and natural gas distribution systems [3].

In these systems, sensors are in charge of measuring some physical phenomena, such as pressure, temperature and rotating speed from physical objects. Then, the sensed data is transferred to the controllers through communication channels to make suitable decisions. Finally, the control signals are transferred to actuators [4]. The aim of these interconnections is to improve the automation, intelligence and performance of CPSs [5]. An overall architecture of CPSs is represented in Fig. 1.

The targets of security attacks against CPSs are different from traditional cyber systems. The security attacks against CPSs may lead to some significant consequences such as the system loss, damage to equipment, damage to production, safety hazards and environmental pollution. So, the security of CPSs become a significant area of researches.

In CPSs, anomaly detection systems are in charge of detecting attacks due to the disordered and incorrect physical behavior of the system [6]. Classic attack detection studies concentrate on detecting the failures of sensors and actuators in physical process under control, however recent approaches focus on the possibility of deliberate attacks such as denial of service and jamming of communication channels, replay, deception, covert and false data injection (FDI) attacks [7].

This paper proposes a modeling approach for assessing the security of CPSs. The proposed approach is based on Stochastic Petri nets (SPNs) [8, 9] and model the system behavior equipped with anomaly detection systems (ADSs) in the normal and under security attacks situations. A Petri net is a mathematical modeling tool for describing distributed systems and falls into class of discrete event dynamic systems. Besides, it can be exploited to model the behavior of systems exhibiting concurrency in their operation. This is a suitable tool for designing and evaluating the performance of security models.

SPN is a type of Petri nets where transitions fire after random times. Since CPSs are confronted with attacks that occur randomly and add uncertainty in the behavior of the system even in the presence of defensive countermeasures, SPNs is a suitable tool to model and evaluate this effect quantitatively. In summary, by using the SPN, it can be possible to model and evaluate the concurrent behavior of the system, attacker and ADS. Furthermore, by exploiting probabilities along

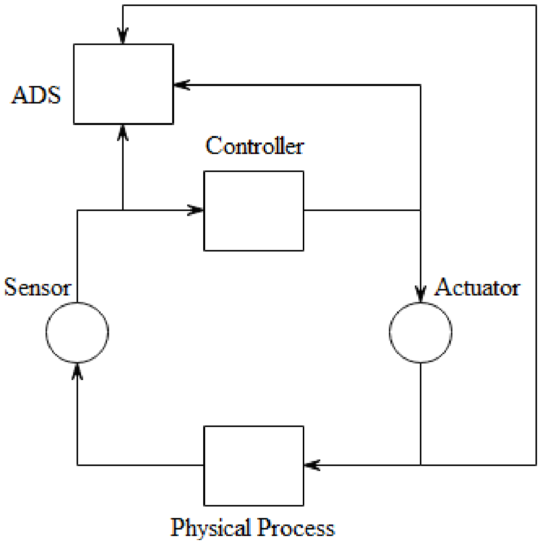

Fig. 1. An overall representation of CPSs

with the time distributions, we can study the temporal behavior of the system under security attacks.

The main contributions of this paper are as follows:

1. Proposing a modeling approach to consider the behavior of CPSs in normal situation and under security attacks.
2. Considering the behavior of the system, attackers and ADSs in the proposed modeling approach.
3. Investigating the effect of some important parameters, i.e. sensors reading intervals, actuators time to perform the desired action and the controller's time scheduling on the security of CPSs.
4. Evaluating the security of CPSs by solving the proposed model based on some security metrics, such as mean-time-to-Failure (or disrupt) (MTTF) and availability.

The proposed approach is applied to a chemical plant as an illustrative example and it is experimentally validated. The resulting quantitative analysis is useful for identifying significant control loops that require more accurate protection and accordingly, for determining appropriate countermeasure strategies. By using the evaluation results of the proposed model, it can be possible to recognize more vulnerable parts of the system and prioritize them for applying the countermeasure strategies.

The rest of this paper is organized as follows. We start by discussing related work in Section 2. In Section 3, the detailed description of the proposed method is provided. An illustrative example is presented in Section 4. And finally, in Section 5, the paper is concluded and an outlook to future work is given.

II. RELATED WORK

This section provides an overview of some related researches in security modeling and evaluation of CPSs. Yaacoub et al. [3] have studied and categorized some existing research on the security of CPSs. They generally focused on modeling and identifying attacks, investigating the main problems in the estimation of the attack consequences against these systems, and developing security architecture. The authors have not considered attacks against control loops.

Iannacone et al. [10] have proposed an evaluation framework to assess the CPS security by modeling the labor, resource and attack costs in dollars. In their framework, they have considered expected resource usage, accuracy metrics and time. The result of their estimation can promote a balance of accuracy, response time and resource use. In their study, they have not investigated the temporal behavior of attacks and attacks against control loops.

Lalropuia et al. [11] have proposed a zero - sum stochastic game approach to model attacker - defender confrontation in CPSs. By exploiting a continuous time Markov chain (CTMC) model, they have focused on the lifetime analysis of the attacked CPS and evaluated mean time to failure of the system. By exploiting the proposed game-based approach, critical states of the system are identifiable. The disadvantage of this method is the use of CTMC, which should have an exponential distribution function for the time of attacks.

Tantawy et al. [12] have developed an approach to model and assess the security risk of CPSs utilizing a CPS testbed with real-world industrial controllers and communication protocols. In their approach, they have not considered the attacker profile and this may lead to non-optimal design of systems.

Tripathi et al. [13] have proposed a design-time approach using Stochastic Petri nets SPN to evaluate CPS security qualitatively and quantitatively. They have provided an event-based model to analyze the system behavior under malicious attacks. They have not considered the attacks against sensor measurements and control signals.

Liu et al. [14] have provided a method for assessing the security of cyber-physical systems by using color weighted Petri nets and Bayesian game theory. The proposed game model is a total of zero games and includes only the components of cost and damage. The desired measure is the probability of attacking any node of these systems by solving the color weighted Petri net model. In this study, the authors have not considered the attacks against sensor and control signals.

Kholidy et al. [15] have presented an approach to estimate the security risk of CPSs by modeling the paths an attacker can traverse to reach certain goals. They have also considered the interaction between the system and the adversary as a multi-step, sequential, two players stochastic game. In this study, time analysis was not done on the attacks.

Jha et al. [16] have focused on the communications standards and communication protocols in smart grid cyber-physical systems. They have provided a systematic mapping among communication technologies, standards and protocols for various SG-CPS applications. They have also studied different existing challenges from SG-CPS's perspective, such as security, safety, reliability and resilience.

Li et al. [17] have concentrated on analyzing the performance consequences of false data injection attacks against power cyber-physical systems, by studying the cascading failures and identifying vulnerable nodes. In addition, they have defined a vulnerability evaluation index from two points of views: the topology integrity and power network operation characteristics.

Friedberg et al. [18] have presented a methodology for analyzing the security and safety of CPSs. Their investigation showed the dependencies between the vulnerabilities of cyber-security and the system safety. They have not focused on attacks against system signals and preforming time-based analysis. Barrère et al. [19] have proposed a security metric for industrial control systems (ICSs), by using hypergraphs. Their approach can be used to detect the set of critical security measures and components that may be disrupted by attackers with minimum effort and cost. They have not addressed the time aspect of the attacks and tried to rank the best attack options from the attacker's point of view.

Amin et al. [20] have proposed a Bayesian network-based framework for integrated safety and security assessment. In their approach, they have concentrated on the probabilistic nature of the events and related factors to analyze the real-time risk.

Barrere et al. [21] have proposed an attack graph-based approach to consider physical and cyber aspects of attacks against CPSs. By using the presented approach, we can model the attack scenarios and analyze the attack impacts on the system. The authors have discussed potential graph-based analysis techniques and focused on assessment.

Binnar et. al. [22] have suggested that in order to overcome the drawbacks of conventional security solutions, forensic tools can be utilized in terms of maintaining the privacy of data while sharing information with other systems. They have studied different models, overview, comparisons, and summarization of digital forensics incident response and intrusion detection systems-based techniques for CPS security.

The shortcomings of the studied methods can be mentioned as follows: None of the mentioned methods have dealt with the temporal analysis of attacks with physical consequences. In none of the studied works, cyber-attacks on sensor data and control signals are not considered. By modeling the temporal behavior of attacks on sensors and control signals, it is possible to analyze the amount of time until system failure due to attacks.

Compared with the described approaches, this paper presents a SPN based modeling method to provide a quantitative evaluation approach for the security of CPSs by focusing on sensor and control signals. The presented method employs the SPN tool to take the system and the attacker interactions into consideration. By employing the proposed method, we can model the attack against sensor readings and control signals and study the system behavior under attack. Besides, we can investigate the effect of some important security parameters such as time-to-failure, detection time, attack time, detection probability and attack probability on the CPSs security. The provided modeling approach can provide an appropriate vision about the security level of the CPS based on two security metrics.

III. THE PROPOSED MODEL

This section describes the proposed modeling approach, step by step. First, the model description is provided. Then, the model parameterization is explained. Finally, security metrics and evaluation of the model is presented.

III-I. Model Description

This section explains the proposed model. An SPN [8] can be defined as a tuple:

$$\text{SPN} =<\text{P, T, F, M}_0\text{, R, H}> \qquad (1)$$

where *P* is a set of places, *T* is a set of transitions, *F* is a set of arcs (from transitions to places and from places to transitions), $M_0{:}P \rightarrow N$ is the initial marking associating with each place a non-negative number, *R* is the set of firing rates associated with the transitions and *H* is a set of inhibitor arcs.

First, we concentrate on modeling control loops of CPSs. In control loops, sensor measurements make the process inputs (e.g., temperature, pressure, voltage). These input data are processed by the controllers to make a correct decision. Finally, the control signals are applied to actuator. These control signals have an effect on the process outputs (e.g., speed or torque of the motor). Fig. 2 depicts the SPN model for a normal behavior of a simple control loop.

Initially, *P_Sense* has one token. Each sensor sends its measurement according to a specific scheduled time to the controller (*T_Sense*). Firing the transition *T_Sense* displays that the input data is transferred to controller and one token is added to the place *P_Control* to start the relevant process by the controller. After processing the input by the controller and making a correct decision, *T_Control* will fire and a token will put in the place *P_Actuate*. This process needs to spend some time. Finally, by firing the *T_Actuate* one token will be removed from the place *P_Actuate* and a token will put in the place *P_ Sense* for the next measurement.

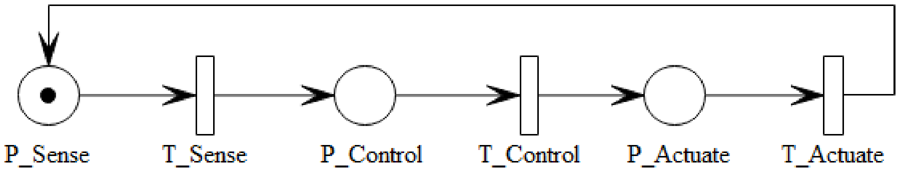

Fig. 2. The SPN model for a normal behavior of a simple control loop

It is possible to send the data received by the sensor to two or more controllers in a control loop. Fig. 3 displays this situation with two controllers. By firing the transition *T_Sense*, one token will be added to the places *P_Control1* and *P_Control2*. Furthermore, another possibility is to send data from two or more sensors to one controller. Fig. 4 shows this situation with two sensors. Firing the transitions *T_Sense1* and *T_Sense2* will add one token to the places *P_Control1* and *P_Control2*, respectively. After providing tokens in these two places, the transition *T_Control* will be activated. Furthermore, sequential data transfer between two controllers can be modeled as Fig. 5.

After modeling the system behavior, the next step is modeling the attacker behavior. It is assumed that security attacks are the incidents that occur randomly at any moment of the time. Therefore, they add uncertainty in the behavior of the system even in the presence of defensive countermeasures. Considering a simple control loop, Fig. 6 provides the SPN model of the system and the attacker behaviors.

Firing the transitions *T_Attack* indicates the occurrence of an attack with a probability and over a specific period of time. By firing the transitions *T_Attack*, one token will be added to the places *P_SenseAttack, P_AttackDetect and P_AttackDisrupt* for modeling the parallel operation of the attack against sensor readings, ADS behavior and the system disruption condition, respectively.

The transition *T_SenseAttack* models the attack against sensor reading. This transition is activated when one token is located in both places *P_Sense* and *P_ SenseAttack*. In this situation, the transition

T_Sense is disabled because of inhibitor arc from place *P_ SenseAttack* to this transition. By Firing the *T_SenseAttack* transition, one token is added to the place *P_Control*, to model the security attack against the sensor reading, one token is located to the places *P_ SenseAttack*, to model the next sensor reading attack and one token is placed in *P_ AttackDetect* to model the ADS behavior.

We now focus on modeling the ADS behavior. Initially, there is one token in the place *P_ Detection*. Each ADS performs a check operation at a specified time interval. If there is an attack, two situations may occur. First, the ADS successfully detects the abnormal behavior of the system as a result of the conducted attack (firing the transition *T_TruePositive*). In this case, the system

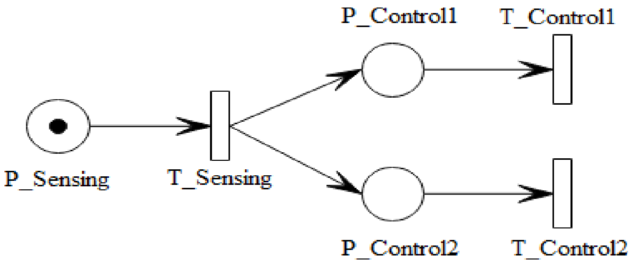

Fig. 3. Sending sensor measurement to two controllers

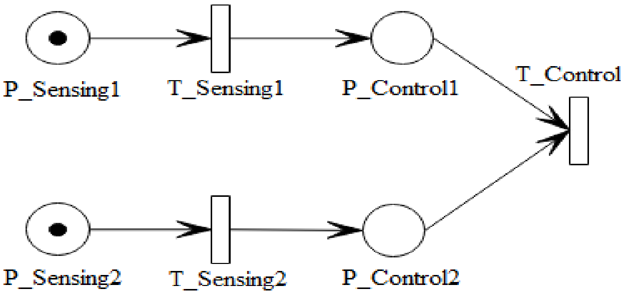

Fig. 4. Sending data from two or more sensors to one controller

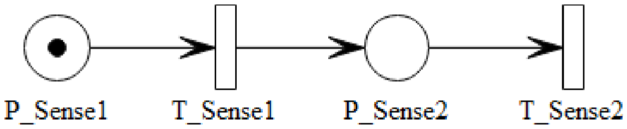

Fig. 5. Sequential data transfer between two controllers or sensors

will return to the normal state after performing the necessary checks and completely stopping the effects of the attack (*T_Rebound*).

The next case is when the ADS is unable to detect the attack (firing the transition *T_FalseNegative*). If the ADS fails to detect the attack before firing the transition *T_Disrupt*, a token is placed in the place *P_Disrupt*, in which case the system is physically disturbed. This scenario shows that the attacker was successful in attacking the system and achieved his goal. In this situation, the system can return back to the normal behavior after a period of time (*T_Repair*) when the effects of the attack have disappeared and the necessary repairs have been made. As long as there is a token in the place *P_Disrupt*, the transition *T_Actuate* will be disabled.

T_RemoveAD and *T_RemoveCD* are immediate transitions for removing tokens from *P_Actuate* and *P_Control* places in the case of detecting the attack, respectively. Besides, *T_RemoveAR* and *T_RemoveCA* are immediate transitions for removing tokens from *P_Actuate* and *P_Control* places in the case of disruption of the system, respectively.

Now, it is the time to discuss about the reachability graph of the proposed SPN model. Fig. 7 depicts the underlying reachability graph of the SPN model.

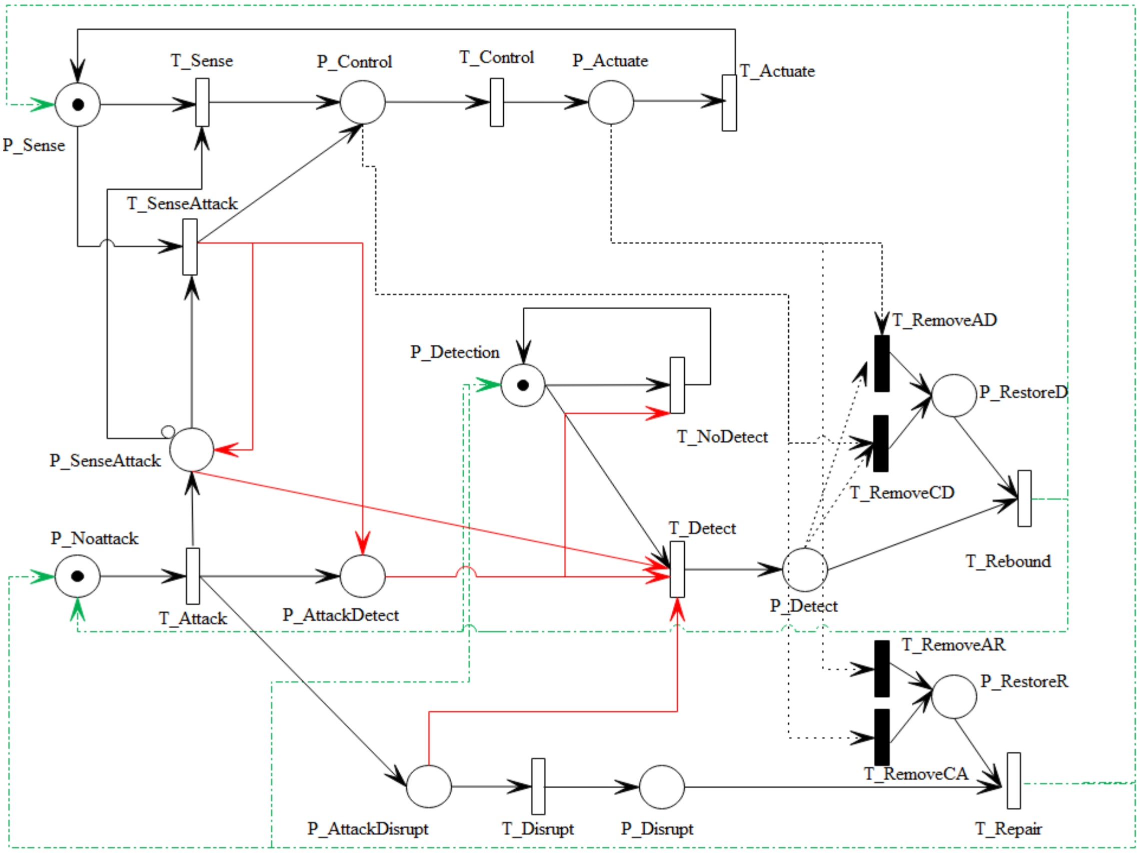

Fig. 6. The SPN model of the system and the attacker behaviors

Reachability graph of the SPN model is created corresponding to marking deviated from the state vector representation [*P_Sense*, *P_Control*, *P_Actuate*, *P_NoAttack, P_SenseAttack*, *P_AttackDetect, P_AttackDisrupt, P_Detection*, *P_Detect*, *P_RestoreD*, *P_RestoreA*, *P_Disrupt*]. This state vector is used for representing the system dynamics. In this representation, 12 variables are exploited for depicting the number of tokens in the places. Table 1 provides different states of the reachability graph of the model.

III-II. Model Is Parameterization

In this section, the presented SPN-based model is parameterized. Because we can employ generally distributed transition times as firing time, we will have a semi-Markov chain (SMC) as the underlying model. One of the important advantages of the SMC is the feasibility of obtaining closed-form solutions.

Now it is the time to focus on parameterizing the model. The attack rate (λ_{attack}) can be estimated as follows:

$$\lambda_{attack} = P_a / T_a \qquad (2)$$

Table 1. Different states of the reachability graph of the model

State Number	Representation
1	[1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0]
2	[0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0]
3	[0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0]
4	[1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0]
5	[0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0]
6	[0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0]
7	[1, 0, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0]
8	[0, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 0]
9	[0, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0]
10	[1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0]
11	[0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0]
12	[0, 0, 1, 0, 0, 0, 1, 0, 1, 0, 0, 0]
13	[1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1]
14	[0, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1]
15	[0, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 1]
16	[0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0]
17	[0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 1]

where P_a is the attack probability and T_a is the attack initiation interval. The ADS true-positive rate (λ_{tp}), can be calculated using this formulation:

$$\lambda_{tp} = P_d/T_d \tag{3}$$

where P_{tp} is the detection probability and T_d is the ADS detection interval.

The system disruption rate () can be derived using the following equation:

$$\lambda_f = 1/T_f \tag{4}$$

where T_f is the time to physical disruption, after successful penetration of attacker into the system.

λ_{RD}, which is the recovery rate from the detected state, can be derived by using the formulation:

$$\lambda_{RTP} = 1/T_{RD} \tag{5}$$

where T_{RD} is the duration of time required for recovering the system from the attacked state back to the normal state. In the fail-safe case, this parameter represents the suspending time of the system for performing recovery actions. Finally, the recovery rate from the failure or disrupted state (λ_{RF}) can be derived using the formulation:

$$\lambda_{RF} = 1/T_{RF} \tag{6}$$

where T_{RD} is the time needed to repair the system to the initial normal state.

After describing and parameterizing the proposed model, now it is the time to determine the parameters of the underlying semi-Markov model. To this end, first, we should estimate the mean holding time in each state and second, we should compute the transition probabilities. The mean holding time in the state i (h_i) can be calculated as follows [8]:

$$h_i = (\sum_{k\epsilon M} U_{i,k})^{-1} \tag{7}$$

where $U_{i,j}$ is the transition rate between the state i and the state j, M is the set of markings in the underlying semi-Markov model. The probability of the transition between the state i and the state j ($P_{i,j}$) can be estimated using the following equation [8]:

$$P_{i,j} = U_{i,j} \times h_i \tag{8}$$

III-III. Security Metrics

This section describes the considered security measures and states the method of estimating them.

1. **MTTF** is defined the time required to achieve one of the absorbing states of the model [23, 24]. This measure is an essential metric to express the resiliency of a CPS. The MTTF can be calculated as follows [23, 24]:

   $$MTTF = \sum v_i h_i,\ i\epsilon S \tag{9}$$

   where v_i is the average visit count of the transient state i in the model before reaching to one of the absorbing states and h_i is the mean sojourn time in state i. The visit count parameters (v_i) can be estimated by using the following system of equations [23, 24]:

   $$v_i = q_i + \sum_j v_j q_{ji},\ i,j\epsilon S \tag{10}$$

   where the quantity q_i is the probability that the model starts in the state i. initially, there is not any attack and the system starts from a secure state. So, we will have:

   $$q = [q_i] = [100...0] \tag{11}$$

2. **Availability** is the proportion of time the system is in a specified operable and committable state. In order to evaluate the availability metric, studying the system behavior in the steady state is required. To do so, we need to convert all permanent states into transient states. This means that, after the occurrence of physical disruption and repair, the system returns to its original functional state after performing corrective and restorative actions.

   For the fail-operation case, the system should continue its operation as much as possible. So, the system is considered to stop only when the system is broken. Therefore, the availability of a fail-operation CPS can be calculated as follows:

   $$A = 1 - \pi_F \tag{12}$$

where π_F is the steady-state probability that the presented model being in disrupted or failed state (F). For the fail-safe case, the system stops with any suspicious event. Therefore, the availability of a fail-safe CPS can be calculated as follows:

$$A = 1 - (\pi_F + \pi_{FP} + \pi_D) \tag{13}$$

For the steady-state probabilities of the underlying semi-Markov model, we have [23, 24]:

$$\pi_i = q_i h_i \,/\, \sum_j q_j h_j \tag{14}$$

where h_i is the mean sojourn times and q_i is the embedded DTMC steady-state probabilities. The embedded DTMC steady-state probabilities can be estimated as the following equation [23, 24]:

$$q = q.P \tag{15}$$

where P is the transition probability matrix.

IV. AN ILLUSTRATIVE EXAMPLE

In this section, by providing an illustrative example, we intend to show how the presented modeling method can be used to assess the security of CPSs. A chemical plant is considered as a case study. Fig. 8 shows the graphical representation of the considered boiling water plant [25]. The plant has three sensors: steam pressure, water level and generated electricity, three valves: fuel, feed-water and steam and it consists of three PLCs: fuel, steam and water PLC. In the steady state behavior of the plant, the normal valve positions are considered as: $u_1 = 0.34$, $u_2 = 0.69$ and $u_3 = 0.433$ and the steam pressure inside the tank is equal to108 kg/cm2. The process model of the plant (PM) is as follows:

$$\begin{aligned}
&x'_1 = -0.0018u_2x_1\ 9/8 + 0.9u_1 - 0.15u_3,\\
&x'_2 = (0.073u_2 - 0.016)x_1\ 9/8 - 0.1x_2,\\
&x'_3 = (141u_3 - (1.1u_2 - 0.19)x_1/85,\\
&y_1 = x_1,\\
&y_2 = x_2,\\
&y_3 = 0.05(0.1307yx_3 + 100s_q + e_r/9 - 67.975),\\
&s_q = (1-0.001538\mathrm{x}_3)(0.8x_1 - 25.6) / x_3(1.0394 - 0.0012304x_1),\\
&0 \leq u_i \leq 1 (i = 1,2,3).
\end{aligned} \tag{16}$$

where u_1, u_2, u_3 represent the positions of the fuel, steam and water valve, respectively, x_1, x_2, x_3 are the drum pressure (kg/cm2), electric output (MW) and fluid density (kg/cm3), respectively, y_3 denotes the drum water level (m), s_q and e_r are the evaporation rate and the steam quality. The task scheduling of PLCs is considered as 100*ms*. The safety limitation of the plant is to prevent

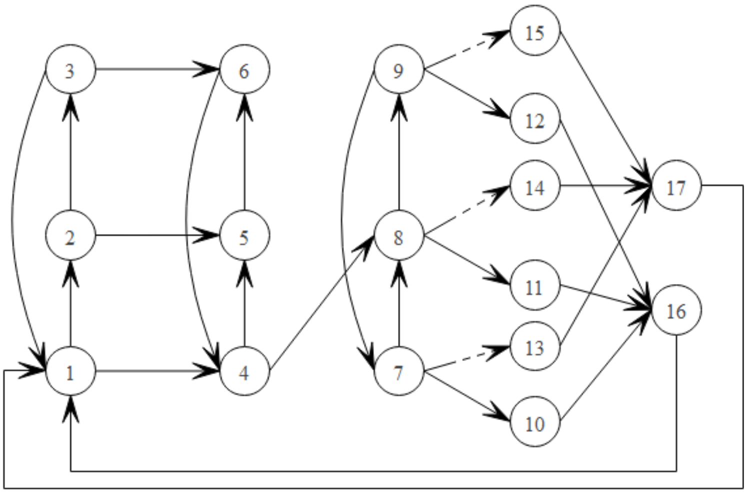

Fig. 7. The reachability graph of the SPN model

the pressure inside the tank from exceeding 250 kg/cm2. Fig. 9 depicts the steam pressure inside the tank in the normal situation with noisy inputs.

Now, we concentrate on describing attack scenarios against the considered plant. The investigated attacks are integrity attacks against control signals exported by the PLCs. For this purpose, individual and combined attacks are considered. In order to reach the desired access level and bring the system into catastrophic state, it is assumed that attackers exploit the VPN vulnerabilities. In industrial systems VPNs are basic tools of attackers for intruding the system. Fig. 10 represents the steam pressure inside the tank as a result of seven integrity attacks. The integrity attacks on control signals as assumed as follows: $u_1 = u_1 \times 1.05$, $u_2 = u_2 \times 1.05$ and $u_3 = u_3 \times 0.95$.

First, we consider the integrity attack conducted on the control signal u_1. By performing this attack, after T = 424.6 (sec), the pressure inside the tank reaches 250kg/cm^2. The second considered attack is the integrity attack on control signal issued by the steam PLC (u_2). For this attack, the attacker tries to close the stream valve by issuing false signals to it. In this case, the pressure inside the tank reaches the explosion level (250kg/cm^2) at T = 590.0 (sec).

For the third attack, we now investigate the integrity attack against the water PLC control signal (u_3). In order to achieve his/her goal, the attacker must try to send continuously manipulated signals to the feed-water valve to put it in the closed position. We now consider a situation in which an attacker intends to make a combined attack on control signals u_1 and u_2. To bring the system into the unsafe state, he/she tries to force the fuel valve to open and the steam valve to close. The time to explosion in the case of this attack is equal to T = 203.9 (sec).

For the next combined attack, integrity attacks against control signals u_1 and u_2 is investigated. In this case, after T = 362.7 (sec) the steam pressure inside the tank reaches the undesired state.

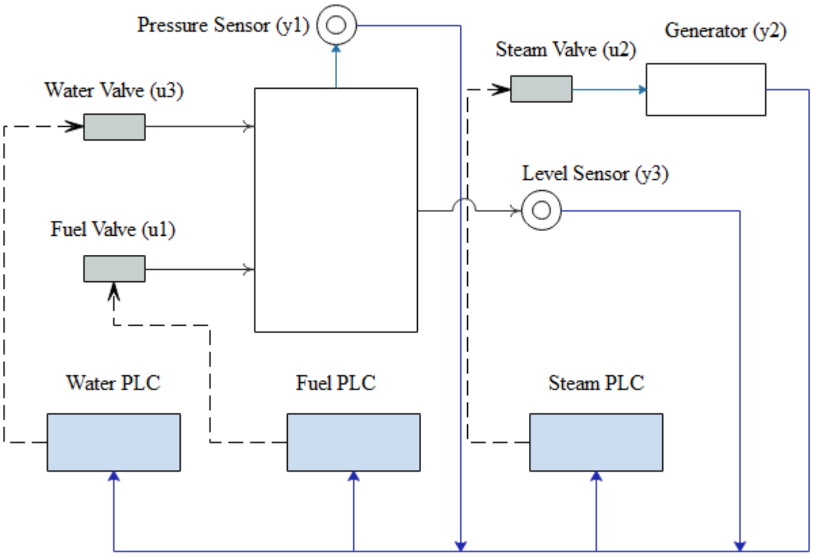

Fig. 8. The chemical plant under study

Table 2. Input parameters to the model and their values

Parameter	Value
P_a	0.5
P_d	0.9
T_a (sec)	86400
T_d (sec)	20
T_{RD} (sec)	270
T_{RFP} (sec)	30
T_f (sec)	424.6, 590, 203.9, 362.7, 465.1, 189.6
T_{RF} (*sec*)	7200

Besides, for the combined integrity attack against the steam valve (u_2) and feed-water valve (u_3), the steam pressure inside the tank reaches to the unsafe state at T = 465.1 (sec). For the last combined attack, the integrity attack against the fuel valve (u_1), steam valve (u_2) and feed-water valve (u_3) control signals are investigated. By conducting this attack, the safety limitation is violated after T = 189.6 (sec). Table 2 lists the input parameters to the model and their values.

Fig. 11 and Fig. 12 show the availability and MTTF of the introduced chemical plant under the considered security attacks, respectively. As these figures show, the highest level of availability and MTTF are related to the attack on control signal 3, which does not disturb the system. Besides, the lowest level of the availability and MTTF are related to the combined attack against control signals 1, 2 and 3. As investigation results show, time-to-failure plays a significant role in availability and MTTF measures.

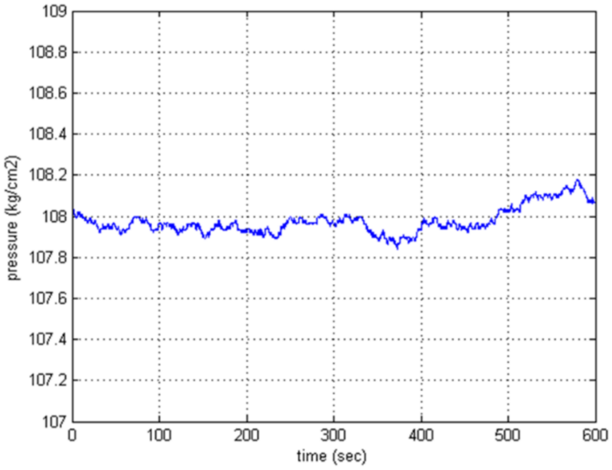

Fig. 9. The steam pressure inside the tank with noisy inputs

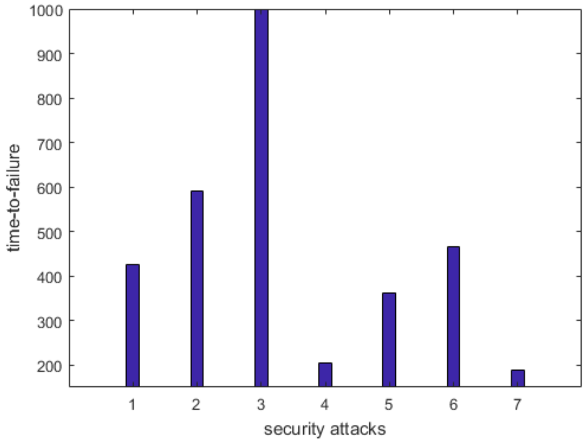

Fig. 10. Steam pressure inside the tank as a result of integrity attacks

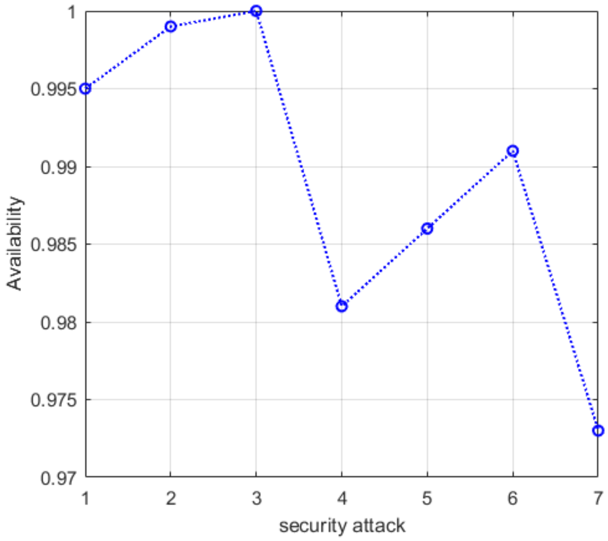

Fig. 11. Availability of the planet under conducted security attacks

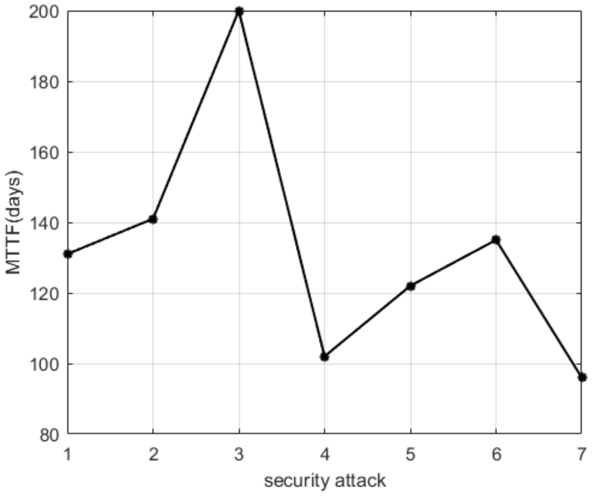

Fig. 12. MTTF of the planet under conducted security attacks

V. CONCLUSION

This paper provides a method to model the security of CPSs in normal and under attack situations. In the proposed model, the physical operation of the system, the attacker behavior and ADS are considered. By using the proposed approach, we can model the attacks against sensor readings and control signals to examine the security status of the system due to these attacks. Several security parameters are employed in the parameterization stage of the model include: the attack probability, the detection probability of ADS, time-to-attack, time-to-disruption, time-to-recover and time-to-repair. By solving the presented SPN-based model, the security of CPSs can be evaluated according to the availability and MTTF measures. In order to display the effectiveness of the proposed modeling approach, the presented model is applied to a chemical plant. Investigation results show that the studied security parameters play a significant role in the security of CPSs. In the context of CPSs security, there are some main challenges which should be considered in future researches. Addressing the role of human in the CPSs security is one of the main research areas in this domain. Another research field in the CSPs security is proposing an applicable risk assessment mechanism with or without automatic monitoring and response [26]. For future work, we want to focus on the security risk modeling of CPSs and provide a modeling approach for this purpose.

REFERENCES

[3] H. Kopetz, Real-Time Systems: Design Principles for Distributed Embedded Applications, 2d. ed., *Real-Time Systems Series*, Sep. 2011.

[4] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212–223, Sep. 2018.

[5] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli, "Cyber-physical systems security: Limitations, issues and future trends," *Microprocessors and Microsystems*, vol. 77, p. 103201, Sep. 2020, doi: https://doi.org/10.1016/j.micpro.2020.103201..

[6] M. Krotofil and J. Larsen, "Are You Threatening My Hazards*?," Lecture Notes in Computer Science*, pp. 17–32, Jan. 2014, doi: https://doi.org/10.1007/978-3-319-09843-2_2.

[7] M. Krotofil, A. Cárdenas, J. Larsen, and D. Gollmann, "Vulnerabilities of cyber-physical systems to stale data—Determining the optimal time to launch attacks," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 4, pp. 213–232, Dec. 2014.

[8] C.-W. Ten, J. Hong, and C.-C. Liu, "Anomaly detection for cyber security of the substations," *IEEE Trans. Smart Grid,* vol. 2, no. 4, pp. 865-873, Dec. 2011.

[9] S. S. Jagtap, S. S. V. S., and S. V., "A hypergraph based Kohonen map for detecting intrusions over cyber–physical systems traffic," *Future Generation Computer Systems*, vol. 119, pp. 84–109, Jun. 2021.

[10] M.K. Molloy, "Performance analysis using stochastic Petri nets," *IEEE Trans. Computers,* vol. 31, pp. 913–917, Sep. 1982.

[11] M. A. Marsan, G. Balbo, G. Conte, S. Donatelli, and G. Franceschinis, "Modelling with Generalized Stochastic Petri Nets," *ACM SIGMETRICS Performance Evaluation Review*, vol. 26, no. 2, p. 2, Aug. 1998.

[12] M. D. Iannacone and R. A. Bridges, "Quantifiable & comparable evaluations of cyber defensive capabilities: A survey & novel, unified approach," *Computers & Security*, vol. 96, p. 101907, Sep. 2020.

[13] K. C. Lalropuia and V. Gupta, "Modeling cyber-physical attacks based on stochastic game and Markov processes," *Reliability Engineering & System Safety*, vol. 181, pp. 28–37, Jan. 2019.

[14] Tantawy, S. Abdelwahed, A. Erradi, and K. Shaban, "Model-Based Risk Assessment for Cyber Physical Systems Security," *Computers & Security*, vol. 96, p. 101864, May 2020.

[15] D. Tripathi, L. K. Singh, A. K. Tripathi, and A. Chaturvedi, "Model based security verification of Cyber-Physical System based on Petrinet: A case study of Nuclear power plant," *Annals of Nuclear Energy*, vol. 159, p. 108306, Sep. 2021.

[16] X. Liu, J. Zhang, P. Zhu, Q. Tan, and W. Yin, "Quantitative cyber-physical security analysis methodology for industrial control systems based on incomplete information Bayesian game," *Computers & Security*, vol. 102, p. 102138, Mar. 2021.

[17] H. A. Kholidy, "Autonomous mitigation of cyber risks in the Cyber–Physical Systems," *Future Generation Computer Systems*, vol. 115, pp. 171–187, Feb. 2021.

[18] A.V. Jha, B. Appasani, A.N. Ghazali, P. Pattanayak, D.S. Gurjar, E. Kabalci, D.K. Mohanta., "Smart grid cyber-physical systems: communication technologies, standards and challenges," *Wireless Networks*, Mar. 2021.

[19] J. Li, C. Sun, and Q. Su, "Analysis of cascading failures of power cyber-physical systems considering false data injection attacks," *Global Energy Interconnection*, vol. 4, no. 2, pp. 204–213, Apr. 2021.

[20] Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer, "STPA-SafeSec: Safety and security analysis for cyber-physical systems," *Journal of Information Security and Applications*, vol. 34, pp. 183–196, June 2017.

[21] M. Barrère, C. Hankin, N. Nicolaou, D. G. Eliades, and T. Parisini, “Measuring cyber-physical security in industrial control systems via minimum-effort attack strategies,” *Journal of Information Security and Applications*, vol. 52, p. 102471, June 2020.

[22] Md. T. Amin, F. Khan, S. Z. Halim, and S. Pistikopoulos, “A holistic framework for process safety and security analysis,” *Computers & Chemical Engineering*, vol. 165, p. 107963, Sep. 2022.

[23] M. Barrère, C. Hankin, and D. O’Reilly, “Cyber-physical attack graphs (CPAGs): Composable and scalable attack graphs for cyber-physical systems,” *Computers & security*, vol.132, p.103348, Sep. 2023.

[24] P. Binnar, and S. Bhirud, “Security Analysis of Cyber Physical System using Digital Forensic Incident Response,” *Cyber Security and Applications*, p.100034, Dec. 2023.

[25] B. B. Madan, K. Goševa-Popstojanova, K. Vaidyanathan, and K. S. Trivedi, “A method for modeling and quantifying the security attributes of intrusion tolerant systems,” *Performance Evaluation*, vol. 56, no. 1–4, pp. 167–186, Mar. 2004.

[26] K.S. Trivedi, Probability and statistics with reliability, queuing and computer science applications, John Wiley & Sons Ltd., Chichester, UK, Feb. 2001.

[27] W. Tan, H. J. Marquez, T. Chen, and J. Liu, “Analysis and control of a nonlinear boiler-turbine unit,” *Journal of Process Control,* vol. 15, no. 8, pp. 883–891, Dec. 2005.

[28] W. S. Admass, Y. Y. Munaye, and A. A. Diro, “Cyber security: State of the art, challenges and future directions,” *Cyber Security and Applications*, vol. 2, p. 100031, Jan. 2024.