Petri Net-Based Approach for "Cyber" Risks Modelling and Analysis for Industrial Systems

K. Labadi[1,2,3,], A.-M. Darcherif[1,2,3], I. El Abbassi[1,2,4], and S. Hamaci[1,2,3]*
[1]*ECAM-EPMI, 13 Bld de l'Hautil, 95092 Cergy-Pontoise, France*
[2]*LR2E Laboratoire de Recherche en Energétique et Eco-Innovation Industrielle*
[3]*Quartz-Lab (EA 7393) – [4]L2MGC (EA 4114) - France*

Abstract. Today, industrial systems are large, complex, and increasingly vulnerable. Specifically, due to the current digital transformation, the industry 4.0 creates crucial cyber-risks and cyber-security challenges. In this context, risk modelling and impact analysis has become a crucial research topic. Based on the formal modelling and performance analysis power of Petri Nets (PN), this paper represents a summary of our methodological approach for "risk" modelling and "impact" analysis of cyber vulnerabilities and / or other critical events. The applicability of the developed approach is demonstrated on a real-life industrial system.

1 General introduction

The current fourth industrial revolution affecting manufacturing systems (Industry 4.0), supply chains and logistic systems (Logistics 4.0) creates crucial cyber risks and cyber-security challenges [8]. In era of Industry and Logistic 4.0, the organizations are hyper connected with their smart devices and smart networks. Unfortunately, this creates cyber-attacks vulnerabilities and opportunities for cyber criminals to infiltrate networks via the weakest links.

As other critical events (technology failures, supplier bankruptcy, disturbances, disruptions, disasters …), a cyber-attack can affect many functions across the network such as production process, transportation organisation, data systems and, more generally, different performances of the system such as customer service, production level, product quality, costs and profits. Figure 1 represents the typical impact of a critical event on the performance of a system.

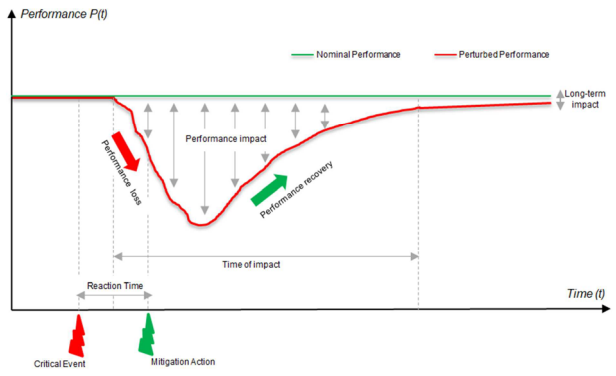

Fig. 1. Typical performance evolution under critical event(s)

Attacks can cause physical damage at facilities, disruption of the information, financial and material flows of the global system. They generally have a low probability and the potential for a large loss. Attacks come in many forms by inserting malicious hardware or software such as malware insertion within any system and malicious integration of counterfeit components during system design, system development or system management.

In practice, cyber security consists of all the technologies that keep computer and data systems [2]. Cybersecurity should no longer be viewed as a function of information technology or information security alone. It is a complex discipline that needs to combine between traditional cyber security and industrial management fields. It is concerned with mitigating risks both to products, services, information, process, and technology related to systems. Except for the technological aspects of the problem, industrial managers need methods and tools for control, analysis, and risk mitigation of their cyber vulnerabilities.

Motivated by this crucial context and problem, this paper suggests a promising modelling and analysis methodology for cyber risk and security purposes. Based on the formal modelling and performance analysis power of Petri Nets [7] for complex discrete event systems, including manufacturing systems, supply chains and logistic systems, this work demonstrates their potential for modelling, impact analysis, and risk mitigation of their critical events including cyberattack vulnerabilities. The developed technique based on the "Nominal" and "Perturbed" Petri net models is presented in a summary way (section 3) and an industrial manufacturing and packaging of pharmaceutical products is used to demonstrate the methodology (section 4).

* Corresponding author: k.labadi@ecam-epmi.com

2 DES and Petri Nets

In this work, the systems are viewed as "Discrete Event Systems" (DES). Many real world systems, including supply chains, logistic and manufacturing systems, can be considered as DES not because of their intrinsic characteristics, but because of the aspects of their behaviour that we want to emphasize. In this field, Petri Nets (PN) [7] have arisen as a practical formalism for modelling DES, widely used thanks to their graphical and mathematical foundation, ready to be exploited for modelling, simulation, theoretical analysis, as well as performance evaluation. They were applied not only to address modeling and performance analysis issues but also to study other specific topics such as logistics optimization, production scheduling and planning, system control and supervisory, diagnosis and fault detection in many discrete event systems [1, 4, 6, 9]. However, although the literature of Petri nets is very plentiful and have been widely used in various domains, their potential and applicability for cyber risk modelling and analysis still to be developed. Today, study, design and management of any industrial system or organization without considering risk evaluation and analysis issues lead to inconsistent networks. Besides some adequate technological solutions, industrial managers need methods and tools for modelling, analysis, and testing of their cyber risk and security issues. This work constitutes part of this emerging issue.

For readers not familiar with Petri nets, some of their basics concepts are given in the following. As illustrated in Figure 2, as a basic definition, a Petri net is bipartite directed graph composed of places (represented as circles), transitions (represented as rectangles or bars), and directed arcs used to connect between places and transitions. A place may contain tokens and the current marking (state) of the modeled system is specified by the number of tokens in each place. Each transition usually used to model an activity whose occurrence is represented by its firing. A transition can be fired only if it is enabled, which means that all preconditions for the activity are fulfilled (there are enough tokens available in the input places of the transition). When the transition is fired, tokens will be removed from its input places and added to its output places. The number of tokens removed or added is determined by the weight of the arc connecting the transition with the place.

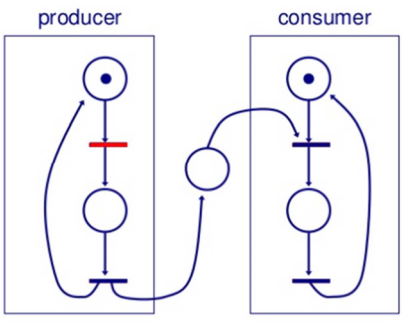

Fig. 2. Simple example (Producer / Consumer)

The signification of the places, transitions and arcs in a Petri net depends on the system modeled. As a simple example, Figure 2 shows a Petri net which models a producer-consumer system. The model consists of three different parts: a production part on the left, a consumption part on the right, and a buffer in the center which allows up to four items to be produced in the system at any time.

The concept of Petri nets has been originally proposed without any notion of time. For performance evaluation and analysis, "Time" is introduced in Petri nets. Generally, two types of transitions can be used to model discrete events: (i) immediate transitions, with zero firing delay and (ii) timed transitions with deterministic or stochastic firing delay [3]. Furthermore, the performance evaluation is based on the temporal evolution of the marking (state) process of the modeled system. If a system is modeled by a stochastic timed PN [3], its analysis can be performed based on the underlying stochastic process of the net. The analytic approach is feasible particularly when the stochastic process has a finite number of states and is analytically tractable under some assumptions. For large and complex systems, simulation techniques and associated software tools may be required.

3 "Nominal" and "Perturbed" Petri Net Based Approach

Based on the formal modeling and performance analysis power of (stochastic) Petri nets for complex discrete event systems, including industrial systems, supply chain and logistic systems, in this section, we develop a "Nominal" and "perturbed" Petri Net approach for "risk" modeling, "impact" analysis and risk mitigation of cyber vulnerabilities and / or other critical disruption events in such dynamical systems.

The proposed approach, synthesized in Figure 3, contains three different steps:

(1) Modelling step, (2) Analysis step and (3) Mitigation step, which can be used in a closed-loop configuration for risk mitigation purposes of the system network. More details of the methodology are given in the following:

- **(Step 1) –** Based on the modelling power of (Stochastic) Petri Nets, the system is modelled firstly as a "Nominal Petri Net model" (without any critical events), and secondly, we introduce one or several perturbation(s) event(s) into the nominal model to obtain its associated "Perturbed Petri Net model".

- **(Step 2) –** Based on the quantitative and/or qualitative methods associated to the Petri Net formalism, the modelled system can be studied through its "Perturbed PN model" in order to analyse the impact of the critical perturbation(s) inserted into the initial model. Both qualitative and quantitative analysis can be performed with the two models for impact study.

– **(Step 3) –** Based on the analysis of the perturbed model, actions and mitigation solutions can be proposed (new system design, new parameters, human error reduction …). Then, the "newly" system can be analysed as often as necessary by the steps above.

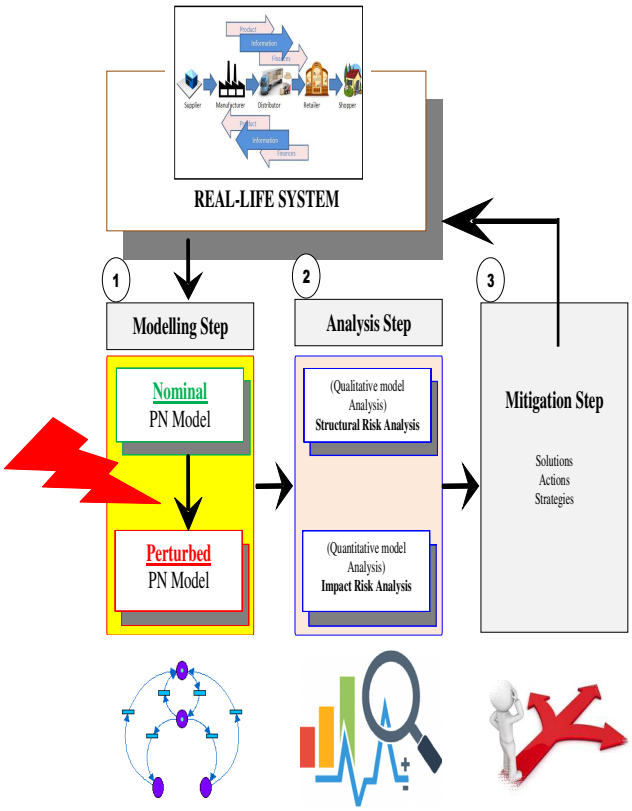

Fig. 3. The Nominal and Perturbed Petri Net Approach.

The main question is "How to introduce (model) a perturbation such as an attack event into the Nominal Petri net model that generates the Perturbed Petri Net model?"

– According to the practice, any attack (Hardware, Software, Process …) and/or critical event can cause operational and / or structural disruption across the system (machine breakdown, disruption of the flow, stock out, lateness, blocking, cancellation of operations, transport interruption …).
– "Perturbation(s)" can be inserted at any location in the Nominal Petri net model according to the critical event(s) to be represented (modelled). Indeed, parametric and/or structural modifications can then be introduced into the nominal model via its three different components: transitions, places and arcs.

4 Industrial Application

To demonstrate the applicability of the proposed approach, we consider a real-life industrial system in Figure 4. The system represents a pharmaceutical manufacturing and packaging system.

Fig. 4. A pharmaceutical manufacturing and packaging system

4.1. Presentation of the industrial system

The industrial system is composed of 7 automated machines (P_i) connected to each other by pallet conveyors (C_{ij}). All the system is controlled by PLC (Programmable Logic Controllers) and equipped with a computer system for monitoring and supervision (S) of different ranges and orders of the production. As schematized in Figure 5, the machines are structured around several conveyors, and three closed-circuits connected by pneumatic jacks. They are used to move pallets from conveyors and vice versa. At the end of the packaging process, two other pneumatic jacks are used for unloading of bottles from pallets and packaging them as finished products.

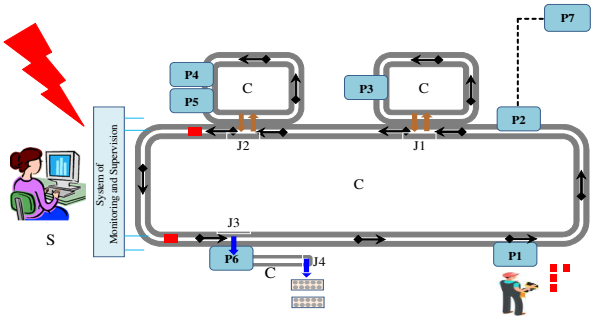

Fig. 5. Structure of the manufacturing and packaging system

Table 1. Components of the industrial system

S	System of Monitoring and Supervision
P1	Operator station (loading of pallets and empty bottles)
P2	Tablet counting/filling machine
P3	Granule dosing/filling machine
P4	Bottle capping machine
P5	Labeling machine for bottles
P6	Unloading and packaging machine
P7	Pharmaceutical tablet manufacturing machine
C1-C4	Convoyors between the differents machines
J1-J4	Input / output jacks for paletts

To more understand the general process of the system and the scheduling of its activities, Table 1 gives its different components and automated machines. Several ranges of manufacturing and packaging can be performed by the system according to their programs to choose by using the monitoring and supervision part of the system.

4.2. Nominal Petri Net model of the system

The nominal Petri net model of the industrial system is shown in Figure 6. The model reproduces its real structure represented in Figure 5.

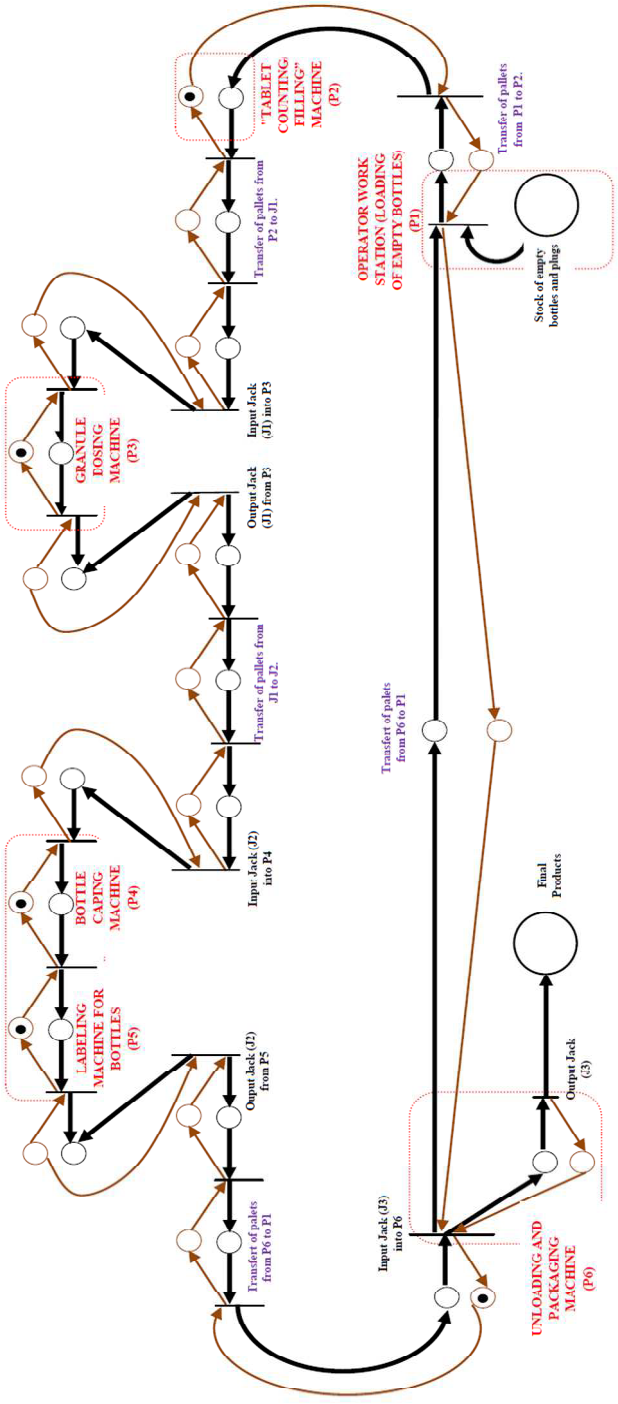

Fig. 6. The "Nominal" Petri Net model of the system

A set of parameters relating to capacities of the different conveyors between machines (Table 2) and the average operating delays (OT) of the different machines are given for three different production ranges: G1, G2, G3 (see Table 3).

Table 2. Capacities of conveyors

Conveyor (C_{ij})	Capacity [pallets]
$C_{(P1-P2)}$	20
$C_{(P2-J1)}$	13
$C_{(J1-P3)}$	26
$C_{(P3-J1)}$	9
$C_{(J1-J2)}$	21
$C_{(J2-P4)}$	26
$C_{(P5-J2)}$	9
$C_{(J2-J3)}$	22
$C_{(P6-P1)}$	32

Table 3. Operating delays of three different ranges

Machines	TO(G1)	TO(G2)	TO(G3)
P1	6	6	6
P2	14	30	-
P3	8	-	18
P4	8	8	8
P5	7	7	7
P6	15	15	15
P7	15	15	15

In addition, the speed of the conveyors is adjustable. So, the different ranges will be tested according to two different speeds: V1 = 15.0 cm/second and V2 = 28.8 cm/second. Thus, all travel times of pallets between the machines can be determined according to the different lengths (or capacities) of the conveyors. Then, by combining the three production ranges and the two conveyor speeds, the simulation results of this study can be given for six configurations denoted by GiVj (i = 1 to 3, and j = 1 to 2).

4.3. Performance evaluation of the Nominal PN model

The performance evaluation and analysis of the system is performed by discrete event simulation based on its associated nominal Petri net model represented in Figure 6. The production rate of the system is considered in this study.

For each configuration (G_iVj, Np), this performance indicator can be expressed in two different ways:

— As the number of products that can be produced during a given unit of time.

$$PR_1(G_iV_j, N_P) = \frac{1}{N_{Rep}}\left(\left(\sum_{k=1}^{N_{Rep}} M(P_{PROD})_k\right)\Big/ T_{Sim}\right)$$

— As the amount of time it takes to produce one unit of a product.

$$PR_2(G_iV_j, N_P) = \frac{1}{N_{Rep}}\left(T_{Sim}\Big/\left(\sum_{k=1}^{N_{Rep}} M(P_{PROD})_k\right)\right)$$

Where:

$PR_1 (G_iV_j, Np)$	Average number of products per unit of time.
$PR_2 (G_iV_j, Np)$	Average production time of a unit of product
T_{Sim}	Total time of simulation.
N_{Rep}	Number of replications.
k	1 … N_{Rep} (k-th replication).
$M(P_{PROD})_k$	Number of tokens, at the end the k-th simulation, of the place P_{PROD} that represent the stock of finished products.

The discrete simulation results are represented graphically in Figures 7 and 8. Clearly, from a given number of pallets (Np*), the production rate of the system is optimal (see Table 4).

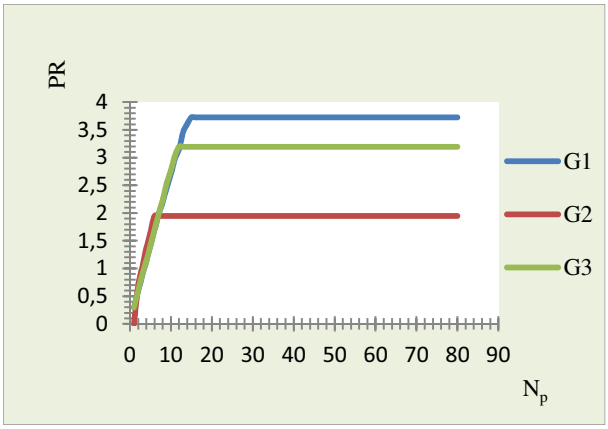

Fig. 7. Production rate evolution (case with V1)

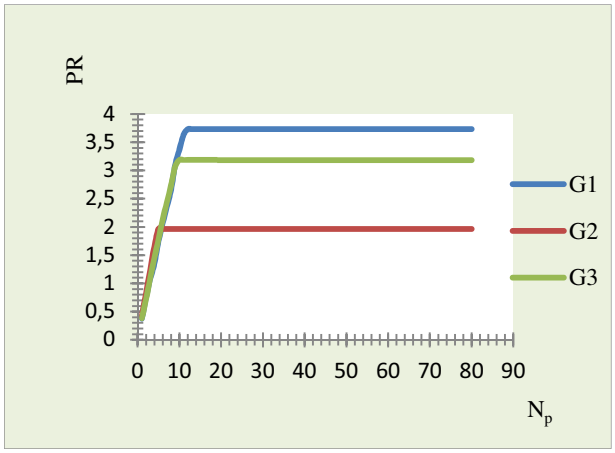

Fig. 8. Production rate evolution (case with V2)

Table 4. Optimal production rates of the industrial system

Ranges	PR*	N_P*
G1V1	3,725	15
G2V1	1,946	6
G3V1	3,195	12
G1V2	3,730	12
G2V2	1,965	5
G3V2	3,185	9

4.4. Modelling and Performance evaluation of the Perturbed PN model

Here, we develop the case of the perturbed model in order to evaluate the risk of a computer intrusion that could affect the transmission network between the monitoring system and all of its programmable logic controllers. The risk is due to the absence of Firwalls for industrial security. The perturbed PN model is represented in Figure 9, where we can distinguish between two PN modules described as follows:

— The first part (subnet 1) represents the nominal part of the industrial system studied previously. The global manufacturing system is represented by the stochastic transition T_{PROD}. Its firing leads to the finished products deposited in P_{PROD}. The stochastic firing delay to be associated to the transition T_{PROD} corresponds to the average production rate determined by using the nominal model (see Table 4).

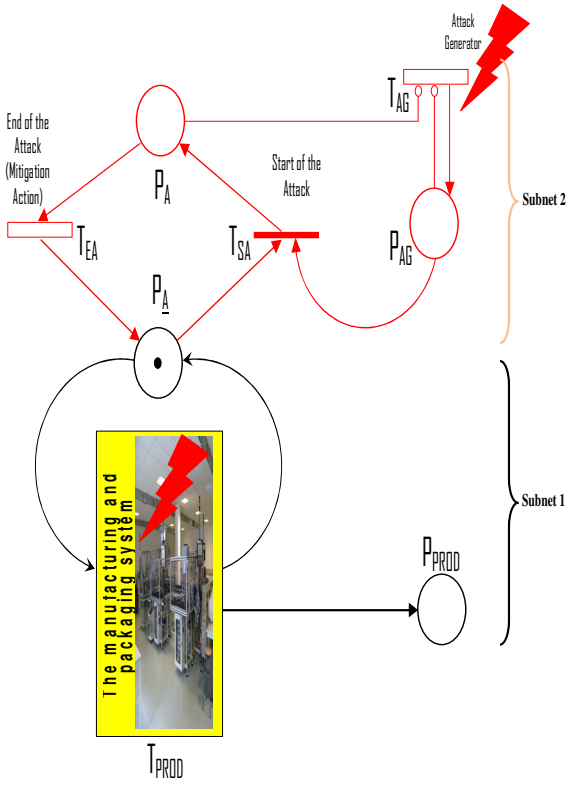

Fig. 9. The "Perturbed" Petri Net model

— The second part (subnet 2) represents the attack generator of the system. The stochastic transition T_{AG} means to generate randomly an attack. It can be set to generate on average "x" attacks/ unit of time. In this study, the perturbed system will be analyzed for several scenarios: 1 attack / year, 2 attacks/ year ...). By firing the transition T_{AG}, the generation of an attack will be indicated by marking the place P_{AG} with one token (i.e. $M(P_{AG}) = 1$). The use of the two inhibitor arcs connecting the transition T_{AG} with the places P_A and P_{AG} serves to avoid another attack, while the system is already subject to an ongoing

attack. When $M(P_{AG}) = 1$, the attack starts immediately by firing the transition T_{SA}. Indeed, this immediate transition is enabled if only if: $M(P_{AG}) = 1$ and $M(P_A) = 1$. The immediate firing of the transition T_{SA} (start of the attack) leads to: $M(P_A) = 1$ to indicate the current attack of the system; and $M(P_{\underline{A}}) = 0$ that makes the transition T_{PROD} not enabled (interruption of the production as long as the attack is untreated). After a stochastic delay that depends on the mitigation action, the transition T_{EA} can be fired to reverse the marking of the place P_A and P_A as $M(P_A) = 0$ and $M(P_{\underline{A}}) = 1$ indicating the end of the attack and the recovery of production with nominal conditions.

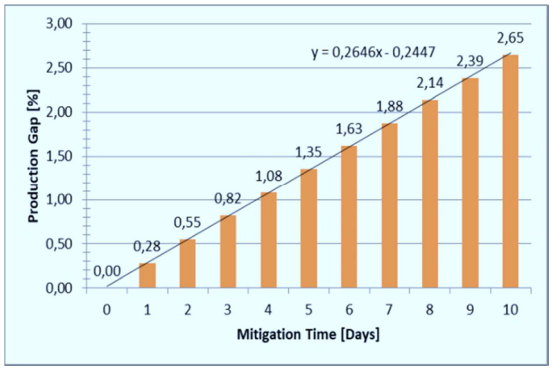

Fig. 10. The impact of the attack on Production Gap [%] according the mitigation delay.

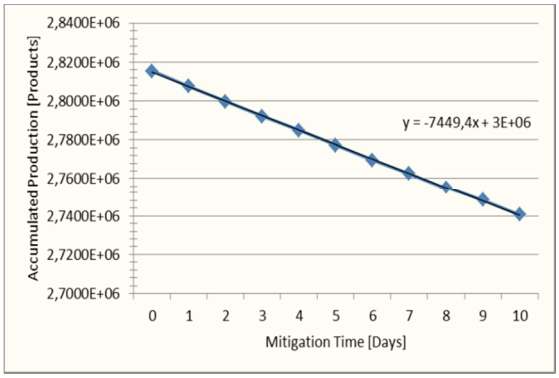

Fig. 12. The impact of the attack on Accumulated Production [Products] according the mitigation delay.

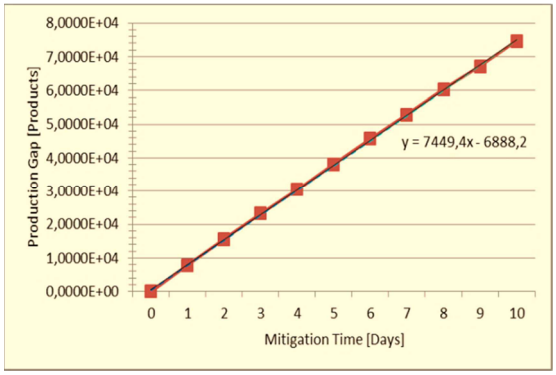

Fig. 11. The impact of the attack on Production Gap [Products] according the mitigation delay.

Finally, some discrete event simulation results obtained for the range G1V1 are given graphically in Figures 10-11-12. They represent a quantitative analysis of the impact of a computer intrusion (T_{AG}) on the productivity of the industrial system (T_{PROD}). The results are presented for ~1 Attack / Year and for several scenarios in terms of the mitigation time.

5 Conclusion

Based on the formal modelling and performance analysis power of Petri Nets (PN), this paper represents a summary of our methodological approach for "risk" modelling and "impact" analysis of cyber vulnerabilities and / or other critical events. The applicability of the developed approach is demonstrated on a real-life industrial system.

References

1. H. Chen, L. Amodeo, F. Chu, and K. Labadi, , IEEE TASE, Vol. 2, No. 2, pp.132–144 (2005).
2. Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, Xian-Ming Zhang, Vol. 275, pp. 1674-1683 (2018).
3. P.J. Haas, "Stochastic Petri Nets: Modelling, Stability, Simulation". Springer-Verlag, New York, (2002).
4. A.A. Kadri, K. Labadi, I. Kacem, EJIE, Vol. 9, No. 5, pp. 638-663, (2015).
5. K. Labadi, T. Benarbia, J.B. Barbot, and A. Omari, IEEE TASE, Vol. 12, No. 4, pp. 1380-1395, Oct. (2015).
6. K. Labadi, H. Chen, L. Amodeo, IEEE SMC, Part C, Vol. 37, pp.4515–4520 (2007).
7. Murata, Tadao, In: Proceedings of the IEEE, Vol. 77, No. 4, pages 541-580, (1989).
8. William Knowles, D. Prince, D. Hutchison, J. Ferdinand Pagna Disso, K. Jones, IJCIP, Vol. 9, Pages 52-80 (2015).
9. R. Zurawski, and Zhou Mengchu, IEEE TIE, Vol. 41, No. 6, pp.567–583 (1994).
10. K. Labadi, H. Chen, L. Amodeo, Journal Européen des Systèmes Automatisés, JESA, Vol. 39, n° 7, pp. 863–886. (2005).