Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 26 (2018) 1116–1127

Procedia MANUFACTURING

www.elsevier.com/locate/procedia

46th SME North American Manufacturing Research Conference, NAMRC 46, Texas, USA

A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems

Alejandro Bracho[a], Can Saygin[a,b,*], HungDa Wan[a,b], Yooneun Lee[a,b], Alireza Zarreh[a]

[a] *Department of Mechanical Engineering, University of Texas at San Antonio, San Antonio, Texas 78249, USA*
[b] *Center for Advanced Manufacturing and Lean Systems, University of Texas at San Antonio, San Antonio, Texas 78249, USA*

* Corresponding author. Tel.: +1-210-458-5194; fax: +1-210-458-6504.
E-mail address: can.saygin@utsa.edu

Abstract

Smart manufacturing systems can be considered within the Cyber-Physical Systems (CPS) domain, where currently, there is a major concern regarding cybersecurity. This paper introduces a simulation-based model to assess the repercussions on manufacturing systems' performance under the potential presence of cyber-threats. The applicability of the assessment model has been validated through the implementation of a case study for the manufacturing sector. Different scenarios have been developed in order to apply an experimental design analysis, where several factors on the model will permit to elucidate the combination of controllable defense policies and uncontrollable security-based parameters that will reduce the negative impact on the manufacturing system's performance. Results have revealed that the impact of cyber-attacks on manufacturing physical operations can be reduced by different defense policies such as increasing capacity of resources at the shop floor and applying more conservative reorder policies for certain situations. Levels among recovery times did not yield the same magnitude of effect. As far as the uncontrollable factors for companies are concerned, it was revealed that the mean time between attacks and the number of potential threat sources have a significant influence on the performance metrics of the system.

Peer-review under responsibility of the scientific committee of the 46th SME North American Manufacturing Research Conference.

Keywords: Simulation; Manufacturing; Cybersecurity; Cyber-Attacks; Defense Policies

1. Introduction

The concept of Cyber-Physical Systems (CPS) is applied in manufacturing systems that incorporate the dynamics and characteristics of tangible processes with commands originated from the computer software and communication platforms [1-3]. Some of the important characteristics of CPS, compared to the

2351-9789
Peer-review under responsibility of the scientific committee of the 46th SME North American Manufacturing Research Conference.
10.1016/j.promfg.2018.07.148

traditional manufacturing systems, include embedded/real-time systems, wireless sensor network (WSN), and other software platforms [2]. Since these types of systems provide tools for the analysis, coordination and monitoring of the integrated architecture, it should be emphasized the importance of highly reliable operations for its automated processes. In CPSs, advanced feedback control technologies, known as Industrial Control Systems (ICS), will be governing the operability of these systems, and hence, its reliability and security are extremely critical.

Over the last decade, the security of ICS has been investigated by many researchers. Most of them focused on introducing cybersecurity vulnerabilities' assessments and suggesting the imperative need of customized Information Technology (IT) security mechanisms to validate the proper performance and safety requirements for ICS [4-6]. Given the increasing availability of software platforms and internet-based capabilities incorporated to these controlling systems, CPS has been exposed to further vulnerabilities from the cybersecurity point of view. Hence, the purpose of this paper is to develop a simulation-based model that will permit the manufacturing sector to assess the effects on systems' performance metrics under the potential presence of cyber-threats throughout their continuous operations.

Manufacturing companies have increasingly adopted these Cyber-Physical technologies for their processes, where software capabilities work in conjunction with human resources (i.e. Human-Machine-Interface) as a multi-level architecture [1]. These type of intelligent systems will promote real-time and collaborative interactions by implementing information analytics and networked resources that will be able to drive results to the manufacturing industry more efficiently and collaboratively through internet-based applications, including cloud computing. Unfortunately, these new capabilities are also augmenting the risk of potential cyber-attacks from malicious outsiders in manufacturing systems.

Cybersecurity has become one of the major concerns for CPS operability and their tangible components for the last decade. In fact, The National Institute of Standards and Technology (NIST) emphasized the importance of strengthening the cybersecurity of the computer-controlled systems within any physical process, while revealing that cyber-attacks could have been translated into approximately $400B of direct costs for companies per year around the globe, with numerous documented incidents [7]. Malicious attacks can compromise automated processes in many possible ways, as several situations have been exemplified where the manufacturing sector could be a huge potential target [8]. Cyber-attacks not only can affect design parameters, overall performance or even quality control (QC) procedures, but also disrupt the product and system design process, so as to make an adverse impact on the design intent of the product for manufacturing companies.

Currently, most manufacturing companies consider that there could be innumerable potential cybersecurity risks, thus aiming to invest in protection against each type of malicious attack appears to be infeasible. That is why the current problem for this industry is analyzing what could be the appropriate countermeasures (i.e. defense policies) that will promote a fair immunity threshold where they can ensure proper functionality of their CPS with similar performance, while taking into consideration their actual financial structure. Thus, there is a need of developing quantitative models that can evaluate the behavior under security breaches for a CPS in the manufacturing sector.

This study addresses the impact of having different controllable defense policies from the company's standpoint, while having different security-based parameters form the attacker's standpoint. A discrete-event simulation model is proposed, given its proven reliability for evaluating the impact of specific circumstances in manufacturing systems and potentially enhancing business decisions [9-12].

The main contributions of this paper will be as follows: (i) Modeling the behavior of a manufacturing system in normal condition and under security attacks through simulation software, (ii) Examining how different controllable and uncontrollable factors, such as resource capacity, reorder policies, mean time between attacks, single or multiple simultaneous attackers and mean time to recover from attacks may affect the performance of the CPS in manufacturing, (iii) Using a simplified game theoretic approach to mimic the interaction between the attacker and defender, and (iv) Assessing the effects of factors based on performance metrics such as throughput, work-in-process, customer lead time, and utilization rates, through the proposed discrete-event simulation model.

The rest of this paper is organized as follows. Section 2 summarizes related work in the fields of

security of ICS, cybersecurity in manufacturing and game-theory approach in cybersecurity. Section 3 describes the research methodology applied in this study. Section 4 presents the case study that was developed in order to validate the applicability of the model. Sections 5 and 6 describe the experimental design and statistical analysis applied to results. Finally, Section 7 provides a summary of the main conclusions and contributions for this paper, while remarking the future research approach.

2. Literature Review

2.1. Security of Industrial Control Systems (ICS)

Over the last decade, the presence of ICS for highly automated processes has been widely discussed. In fact, ICS are typically found in the main industrial sectors such as electricity, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, food and beverage, and certainly manufacturing. As ICS being a critical part of many advanced manufacturing systems, it is imperative to study ICS's classic topologies and vulnerabilities to cyber-threats [13].

Supervisory control and data acquisition (SCADA) systems are the most common type of ICS, which are responsible for monitoring and controlling intelligent networks, thus making this type of infrastructures major targets for malicious attacks. The importance of identifying cybersecurity vulnerabilities and creating autonomous defense methods for these controlling systems have been extensively discussed before [14-17]. Specifically, a research study used a mathematical form of vectors for representing simple and complex attacks as potential industrial radio vulnerabilities [18]. Likewise, other authors developed a method for analyzing uncertain network transmission time delays in real-time, while creating a closed-loop control of manufacturing plants through networks [19]. In manufacturing, it is currently known that the increasing use of wireless networking technologies in ICS, have increased the risk from many adversaries who do not even have a direct physical access to equipment on the shop floor.

That being stated, risk assessment and possible defense policies implementation against attacks in Manufacturing Systems have been examined. Security mechanisms for control systems have been proposed before, while only a few have explored new and fundamentally different research problems for securing control systems when compared to securing traditional information technology (IT) systems [20]. Incorporating knowledge of the physical system under control has been discussed, so it could be possible to detect computer attacks that change the behavior of the targeted control system. Similarly, Atighetchi et al. [21] have shown an overview of the current set of network-level defenses for Applications that Participate in their Own Defense (APOD). They described specific network-based defense mechanisms and remarked on the appropriate strategy to utilize them in local defensive behavior.

2.2. Cybersecurity in Manufacturing

As many documented incidents exist for different industries over the recent years, there is an emerging interest in evaluating the impact of these cyber-threats in manufacturing systems. Wells et al. [8] highlighted some specific cybersecurity vulnerabilities for manufacturing systems, while describing potential approaches that should be utilized for analyzing this type of issues. Sturm et al. [22] focused on the vulnerabilities of additive manufacturing (AM) technologies, mainly in using .STL files during its processes, while Zeltmann et al. [23] also demonstrated the significance of modifying the design intent of the products for manufacturing companies.

In terms of vulnerabilities in manufacturing, DeSmit et al. [24] proposed an approach for assessing cyber-physical systems in the manufacturing sector, using decision tree analysis. Vincent et al. [25] introduced a real-time detection approach for enhancing quality control in manufacturing environments affected by Trojan attacks. Finally, security of SCADA systems in advanced manufacturing has also been investigated recently [26].

In summary, researchers have been focused on the conceptual and final objective of the attack and potential vulnerabilities, and not on how the effects of these attacks can be quantified in automated processes. In fact, a general quantitative model to assess the effects of having cyber-threats in manufacturing environments has not been found on the literature.

2.3. Game Theory Framework in Cybersecurity

Game theory is a decision-making tool for analyzing behaviors of competing agents under a conflict condition. It assesses the conflicting and cooperative nature of rational agents who try to pursue their own benefits [27, 28]. In fact, this theory has been applied by many researchers to solve various problems in physics, economics, computer science, international relations, engineering and more [29]. Each agent attempts to maximize its payoffs by selecting the best actions from a cooperative or individual point of view.

Specifically, in cyber-attack incidents, since any set of actions from both attacker and defender will cause perturbations on the network, the need of adaptive policies for the entire system is increasing. For instance, the malicious attacker could be economically rewarded, while the system administrator (i.e. defender) can be impacted by potential theft of data and decline of the overall performance. It is convenient to use a game theoretic approach to bring to mind the actual behavior between a cyber-attacker and the defender of the CPS, where consequences or rewards for the ultimate game result will be encountered. For this reason, there is a research trend of using a stochastic game-theoretic model approach for capturing the results of these specific interactions from a cybersecurity point of view, where the integrity of networked CPSs has been evaluated under the presence of attacks through the Internet [30-35]. Overall, many researchers have successfully highlighted in their work that the game theory concept is quite appropriate for analyzing the results of the stochastic interactions between attackers and defenders as a security assessment, yet, the applicability of this modeling technique has not been found in the published literature specifically for the manufacturing industry.

In this paper, a cyber-game approach will be used as a way for mimicking the interaction between the attacker and the defender through a simulation model. Hence, the stochastic model will consider cyber-attacks that could be successful or defused, depending on the result of the game. If the attack is successful the control system of the whole manufacturing CPS will change its status, which will ultimately have an impact on the processing times for its physical operations.

3. Research Methodology

The main purpose of this study is to determine the effects of having potential cybersecurity threats on the performance of a cyber-physical manufacturing system. In order to answer the research question, computer-based simulation has been chosen as the experimental technique.

First, a simulation model has been developed using Arena® from Rockwell Automation. A CPS in the manufacturing sector has been modeled, which includes three sub-parts: i) the game, which uses a simplified game-theoretic approach to mimic the interaction between the two players (i.e. attacker and defender) after an attack has been launched by a potential outsider; ii) the cyber part, which refers to the ICS platform in charge of controlling the physical operation of the manufacturing processes; and, iii) the physical part, which simulates the physical manufacturing production system. The overview of the simulated system will be further discussed in the next section. The sub-parts of the model are considered to be interrelated between each other, therefore, the possibility of simulating cyber-attacks on the control system will ultimately expose the quantitative impact on the performance measurements from the physical manufacturing production line.

Following that, a complete factorial design of experiments has been created in order to develop multiple scenarios for analysis, where five main factors with different levels will be considered in the model, regarded as controllable defense policies for the company or uncontrollable factors from the potential attacker's side. Performance metrics such as Throughput rate (TH), Work-In-Process (WIP) and Customer Lead Time (LT) will be considered as the data or responses that will be collected from the simulation output. Finally, statistical tests such as Analysis of Variance (ANOVA) among factors, pair-wise comparison of factors' levels, main effects and interaction plots, among others, will be conducted in order to reach to conclusions.

4. Case Study: A Simulated Manufacturing System

A CPS model of a manufacturing company was developed through simulation software. It includes the potential interaction between the defender (i.e. manufacturing company) and the attacker trying to compromise the integrity of the networked control

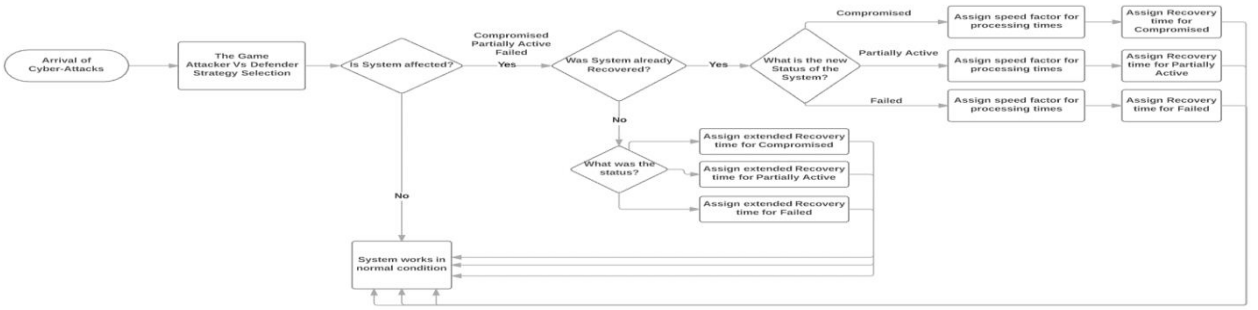

Fig. 1. Flowchart logic for Cyber part

system (i.e. ICS), which could cause a partial or complete disruption of the operability of the physical production line of the company. The flowchart of the simulation model, for the cyber part and the physical part, can be observed in Fig. 1 and Fig. 2 respectively. Components of the simulation model are explained further in the following sub-sections.

4.1. The Game

This part of the model represents the interaction between a potential attacker and the defender of the CPS. Potential cyber-attacks, where the hacker is trying to reduce the production rate of the machines, arrive following an exponential distribution of time between attacks, which will vary according to scenarios described in Section 5. Each player has a set of possible playing strategies that will determine the outcome of the game. The possible set of defense strategies are: *D1 "IT Firewalls and security", D2 "Unidirectional Gateway", D3 "Autonomic computing technology" and D4 "Do Nothing"*. Similarly, the possible set of attack strategies are: *A1 "theft of intellectual properties", A2 "send phishing email", A3 "send malware" and A4 "Do Nothing",* as these actions have been used in the literature before [16, 36, 37]. Both the attacker and defender will choose an action among their potential strategy sets. Finally, once a potential attack has arrived, the outcome of the game has a consequence on the current status of the system, for what the CPS will either behave in a "Normal (G)", "Compromised (C)", "Partially Active (PA)" or "Failed (F)" state. Fig. 3 defines the possible current states of the system depending on the player's action selection.

4.2. The Cyber System

This portion of the model represents the Intrusion Detection System (IDS) of the whole networked CPS. The IDS will detect the arrival of a threat and will try to defuse it; otherwise, this will impact the current status of the system. Once the system detects that it is not in a Normal (G) state, it will try to recover based on the actual condition. The recovery rate or Mean Recovery Time (MRT) will be longer if a consecutive attack arrives into the system while it is trying to recover itself.

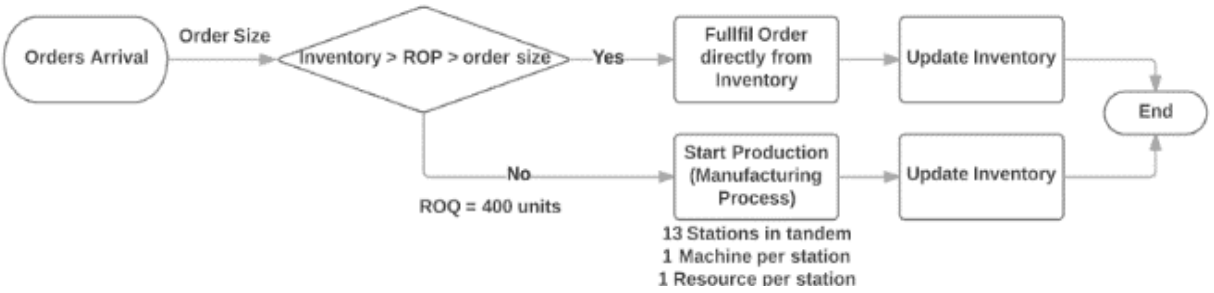

Fig. 2. Flowchart logic for Physical Part

$$\textit{Status of the CPS} = \begin{array}{c} \\ A1 \\ A2 \\ A3 \\ A4 \end{array} \begin{array}{c} \begin{array}{cccc} D1 & D2 & D3 & D4 \end{array} \\ \begin{bmatrix} G & C & C & C \\ PA & G & PA & PA \\ F & F & G & F \\ G & G & G & G \end{bmatrix} \end{array}$$

Fig. 3. Status of the Cyber-Physical System

4.3. The Physical System

This portion of the model represents the material's flow throughout the manufacturing production line. A model has been created with the following considerations:

- The physical production line consists of 13 stations in tandem with one resource as capacity (i.e. machine) located at each station.
- Customers' orders arrive following a normal distribution with a mean of every 1.6 hours and a standard deviation of 0.3 hours.
- Order size is normally distributed with a mean of 230 units and a standard deviation of 46.
- Orders can be served directly from current on-hand inventory (i.e. finished units) or through the physical production of more units.
- The system will consider reorder policies for production, where the reorder quantity (ROQ) and reorder point (ROP) are defined as fixed variables.

4.4. Run Setup

For each experiment, the model ran for 365 days, 24 hours a day, with 2 replications. It excluded a warm-up period of 30 days, which was not counted for the statistics. After the replications, average value of each metric for the long-run was reported.

5. Design of Experiments

A complete factorial design was developed in order to best quantify the effects of five factors, considered as parameters for the model, on the physical manufacturing system's performance under the presence of potential cyber-attacks. 108 scenarios were experimented, where 2 replications were run for each particular scenario. The averaged metrics of the replication length were considered as the simulation output (i.e. responses) for each scenario, resulting in a total of 216 runs where performance metrics have been collected as data to be analyzed.

5.1. Factors

- **Resources:** This factor represents the capacity (i.e. number of resources available) at each station of the production line throughout the replication length.
- **Mean Time between Attacks (MTBA):** This factor represents the mean time between possible cyber-attacks to the automated manufacturing system. We will use the mean time following an exponential distribution.
- **Reorder Policies:** This factor represents the combination of the values that are set for the Reorder Point and Reorder Quantity in the model. Since the manufacturing system has the capability of serving customers' orders directly through on-hand inventory (i.e. no production needed), then the manufacturing of parts will only start when we ran out of physical inventory. Hence, these two parameters will be considered as the inventory-based safety condition for the production line operability.
- **Single or Multiple Attackers:** This factor represents the capability of the model to simulate potential cyber-attacks from one or multiple simultaneous attackers.
- **Mean Recovery Times (MRT):** This factor represents the mean time needed for the system to be fully recovered from a cyber-attack. Since we have three different possible affected states after a cyber-attack, we will have three different values for this factor at each level.

The factor/levels information of the design can be visualized through Table 1.

5.2. Responses

Three performance metrics are considered as the simulation output of the created scenarios. These metrics are the number of Orders Out (TH), Work-In-Process level (WIP) and Customer Lead Time (LT).

Table 1. Factors' Information for Design Matrix

Factors	Level Values
Resources	1
	2
	4
Mean Time Between Attacks	0.25 days (EXPO)
	5 days (EXPO)
	30 days (EXPO)
Reorder Policies	400 ROQ and 280 ROP
	800 ROQ and 400 ROP
Single or Multiple Attackers	Single
	Multiple
Mean Recovery Time	2, 6 and 15 Hrs (EXPO)
	10, 22 and 50 Hrs (EXPO)
	15, 40 and 125 Hrs (EXPO)

6. Statistical Analysis

After conducting the proposed simulation-based experiments, a general linear model (GLM) with all factors was developed based on the total set of scenarios included in the experimental design for each type of metric. The purpose is to determine which parameters on the model most affected the performance metrics of the automated manufacturing system. Tables 2, 3 and 4 show the statistical results from the GLM. These tables only include the main factors.

Table 2. General Linear Model for TH

Source	DF	Adj SS.	Adj. MS	F-Value	P-value	R-sq
Model	107	68312881	638438	130.68	0.0000	99.04%
Linear	8	38760343	4845043	786.82	0.0000	-
Resources	2	11244823	5622411	913.06	0.0000	-
MTBA	2	17305747	8652874	1405.2	0.0000	-
ROQ and ROP	1	17152236	7152236	1161.5	0.0000	-
Single or Mult.	1	2924387	2924387	474.91	0.0000	-
Recovery Times	2	133149	66575	10.81	0.0000	-

Table 3. General Linear Model for WIP

Source	DF	Adj SS.	Adj. MS	F-Value	P-value	R-sq
Model	107	23748387	221948	90.94	0.0000	98.90%
Linear	8	14095681	1761960	721.97	0.0000	-
Resources	2	3670645	1835323	752.03	0.0000	-
MTBA	2	6356160	3178080	1302.24	0.0000	-
ROQ and ROP	1	2791030	2791030	1143.64	0.0000	-
Single or Mult.	1	1205936	1205936	494.14	0.0000	-
Recovery Times	2	71909	35955	14.73	0.0000	-

Table 4. General Linear Model for LT

Source	DF	Adj SS.	Adj. MS	F-Value	P-value	R-sq
Model	107	18256016	170617	42.51	0.0000	97.68%
Linear	8	11308063	1413508	352.2	0.0000	-
Resources	2	2515878	1257939	313.44	0.0000	-
MTBA	2	5064352	2532176	630.94	0.0000	-
ROQ and ROP	1	2759987	2759987	687.7	0.0000	-
Single or Mult.	1	855077	855077	213.06	0.0000	-
Recovery Times	2	112770	56385	14.05	0.0000	-

Interestingly, the ANOVA tables reveal that all the main factors have significant impact on TH, WIP and LT at a 95% significance level. Similarly, the Pareto chart on effects for each metric also confirmed the fact that all factors are significant for these responses, where the reorder policies appear to be the factor with the greatest effect, as can be seen in Fig. 4 for Orders Out specifically.

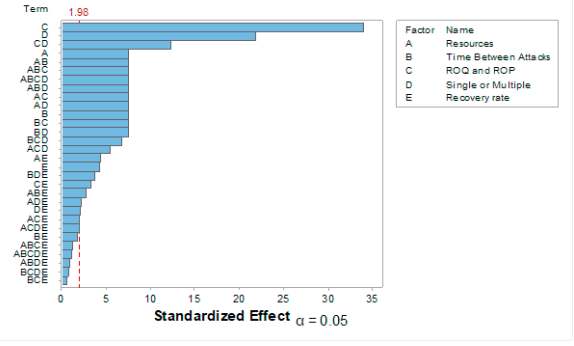

Fig. 4. Pareto Chart of Standardized effects on Orders Out

In the following sub-sections, the impacts of experimental factors on four performance metrics (i.e.,

TH, WIP, LT, and Utilization) are discussed in more details.

6.1. Impact on Orders Out (TH)

The main effect results for throughput can be graphically seen in Fig. 5. As expected, throughput has increased as the number of resources available at each station increased. Similarly, as MTBA were more frequent, the throughput rate was adversely affected, while the Reorder Policy of increasing the ROQ and having a higher ROP has also a positive effect on maximizing the total orders served. In terms of cyber-based parameters, the Single-vs-Multiple attacker's factor has a significant effect. Finally, there is a particular finding between the three levels of Recovery Times. The first two levels do not seem to have a significantly different impact on throughput from each other. In fact, only the third level at the slowest recovery rate seems to have a negative impact on this metric.

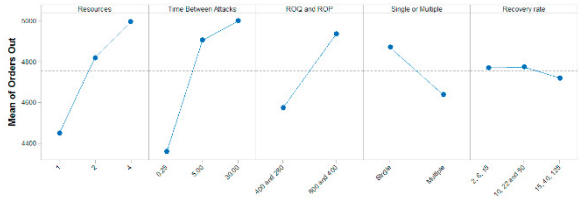

Fig. 5. Main Effects for Orders Out

Additionally, a Tukey's pairwise comparison test has also been performed at a level of 95% confidence, in order to specifically substantiate the claims on the significance between levels of MRT mentioned before.

Furthermore, it is also fundamental to analyze the interaction between different factors and determine the best combination for the best overall performance of the system. First of all, by looking at Fig. 7, where the interaction between Resources and MTBA is shown, the highest mean values of throughput are encountered at the highest level of resources, and the performance has a strong correlation with the level of resources as expected. Specifically, the maximum mean value is found at 4 resources with a MTBA of 30 days. On the contrary, when we have resources set as 4, it practically does not make any difference whether the MTBA is equal to 5 or 30. Actually, if the MBTA is equal to 5 or 30 days, the system will have the same performance for this metric between choosing a capacity of 2 or 4 resources, thus, in this specific case the company will be able to maintain the same throughput level without having to set the resource capacity at the highest level.

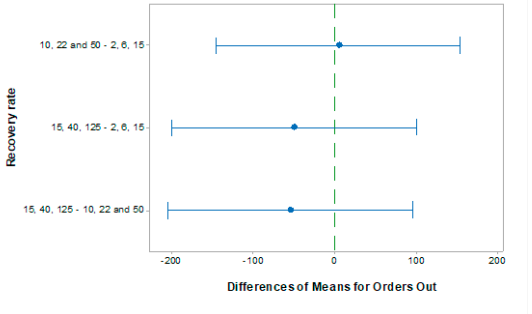

Fig. 6. Tukey Pairwise Comparison between levels of Recovery Time for Orders Out

Moreover, in terms of orders served, the actual production rate (i.e. new throughput rate divided by the original throughput rate) from being potentially affected by cyber-attacks is observed in Fig. 8. As expected, it is confirmed that when having more resources allocated in each station we will stabilize the system faster until reaching the 100% production rate at some point of MTBA. Fundamentally, the more frequent the attacks are received, the system will spend

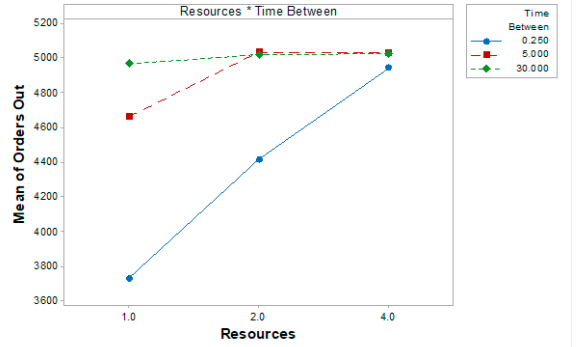

Fig. 7. Interaction Plot (Resources Vs MTBA)

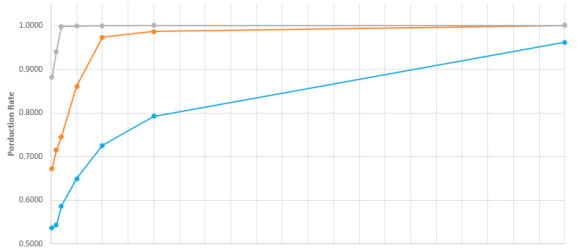

Fig. 8. Production Rates Vs MTBA

more time trying to recover and reaching the original average production rate.

The interaction between MTBA and the reorder policies is shown in Fig. 9, where it can be concluded that when the MTBA is set at 30 days, the effect of having any of the two levels of reorder policies is almost the same, differently from MTBAs of 0.25 or 5 days.

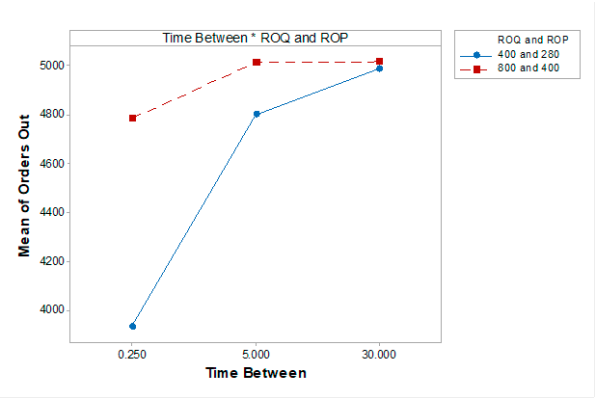

Fig. 9. Interaction Plot (MTBA Vs Reorder Policies)

6.2. Work-In-Process (WIP) and Customer Lead Time (LT)

Main effects plot for WIP is shown in Fig. 10. As expected, the averaged WIP level and LT of the system will diminish as the number of resources available at each station increase. In fact, LT and WIP, being directly proportional metrics, will have a quite similar behavior for the main and interaction effects.

The interaction between resources and MTBA in Fig. 11, shows that the lowest mean value of WIP is found at the highest level of resources, as expected. This value diminishes while the number of resources increase. Again, the best mean value is found at 4 resources with a MTBA of 30 days. However, when the company have resources set at 2 or 4, it practically

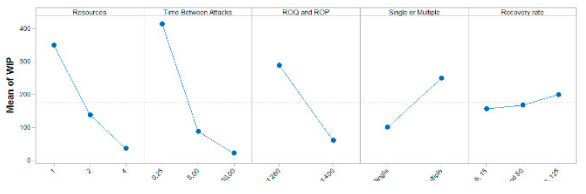

Fig. 10. Main Effects for WIP

does not make a strong argument to be concerned about potential MTBA between 5 and 30 days, differently form a MTBA equal to 0.25.

In general, the interaction of factors for WIP and LT will reveal the opposite effect as determined for the orders out. Thus, this paper concentrated on presenting all the two-way interaction plots for throughput rate only.

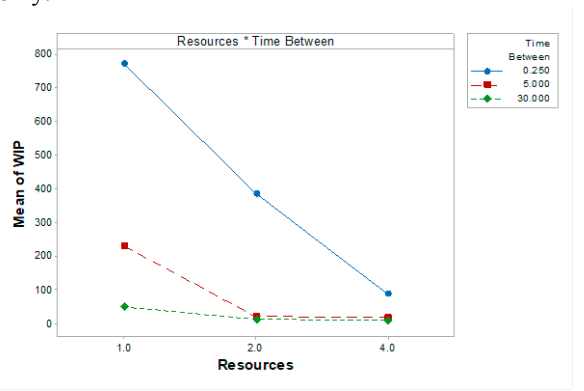

Fig. 11. Interaction Plot (Resources Vs MTBA)

6.3. Utilization Rates:

Cybersecurity issues will also have an impact in other metrics for the manufacturing production line. Considering the case study, the utilization rates among stations after a cyber-attack have been examined. For this purpose, Table 5 was created to demonstrate the behavior of this metric with a standard MTBA of 5 days and different levels of resources' capacity among stations.

Overall, Table 5 shows that depending on the number of sources for potential attackers, the quantity and location of bottlenecks for the production line will differ, for each level of resources' capacity. For instance, if the level of resources is set at the lowest, the bottleneck for the original scenario will be station #6. However, if the system starts receiving attacks from a single source, the bottleneck will now be stations #4 as wells as #6. For multiple attackers, bottleneck has again changed to stations #1, #4 and #6. This condition reveals that any station regarded as the bottleneck of a serial manufacturing production line will not necessarily maintain this condition after potential cyber-attacks have occurred.

In summary, it is observed that station #1 is the most susceptible station to attacks when the number of potential attackers increases in this specific case study,

even if the number of resources available is also augmented.

6.4. Performance Metrics Summary

The statistical analysis revealed that all the factors included in the experimental design were considered significant for the overall performance of the system. In terms of quantifying the effects, the reorder policies appear to be the factor with the greatest impact. Overall, this case study revealed that when resources or reorder policies are set on the highest level, the effect of having lower or higher mean time between attacks (MTBA) is not relevant across the performance metrics. Similarly, when these defense policies are set at the highest level, it seems worthless to invest in a more robust software infrastructure that provides a faster recovery rate from cyber-attacks.

As far as the uncontrollable factors are concerned, it was revealed that the mean time between attacks and the number of potential attack sources have a significant impact on the performance metrics, while the different levels among recovery times do not have the same magnitude of impact. Specifically, the effect of having multiple potential attackers has been substantiated by causing a negative effect on each metric, while the impact on having different levels of recovery time was not statistically significant. Finally, the examination of utilization rates among stations also revealed that the bottleneck station of the original manufacturing production line (i.e. no attacks) will not necessarily remain as the same after potential cyber-attacks have occurred.

7. Conclusions

In this paper, discrete-event simulation was used for evaluating the adverse impact of cybersecurity threats on a manufacturing system's performance. Different experimental scenarios have been created, where factors, such as resources, reorder policies, time between attacks, and recovery times, were assessed in order to elucidate the system's performance against cybersecurity issues.

The statistical assessment permitted to identify conclusions based on the performance of the simulation model output, where all the factors included in the experimental design were considered significant for the overall performance of the system. Overall, this specific case study revealed that when controllable factors on the shop floor, such as capacity and reorder policies, are set on the highest level, the effect of having lower or higher mean time between attacks (MTBA) is not relevant. The study also revealed trade-off regions for specific scenarios where the companies will be able to choose between investing in a higher level of resources and maintaining higher inventory levels in the shop floor (i.e. increasing level of reorder policies). Utilization rates among stations were also examined for the case study.

For future research, these directions should be considered: i) A cost function to evaluate economical combinations of controllable factors while minimizing the impact on the system, ii) A regression model or other supervised machine learning algorithms that will permit to quantitatively evaluate results from implementing different combinations of controllable factors, and iii) Other types of manufacturing environments (e.g. open-shop system) where dynamic

Table 5. Utilization rates among Stations

		Stations												
Capacity	Cyber Status	1	2	3	4	5	6	7	8	9	10	11	12	13
1 Resource	No attacks	0.80	0.81	0.83	0.86	0.83	**0.88**	0.81	0.83	0.09	0.04	0.11	0.07	0.05
	One Attacker	0.96	0.97	0.99	**1.00**	0.95	**1.00**	0.92	0.57	0.10	0.05	0.13	0.08	0.06
	Multiple Attackers	**1.00**	0.99	0.99	**1.00**	0.95	**1.00**	0.92	0.51	0.08	0.04	0.12	0.06	0.04
2 Resources	No attacks	0.40	0.40	0.41	0.43	0.41	**0.44**	0.41	0.27	0.04	0.02	0.05	0.04	0.02
	One Attacker	**0.56**	0.53	0.52	0.54	0.50	0.54	0.48	0.31	0.05	0.02	0.06	0.04	0.03
	Multiple Attackers	**0.87**	0.81	0.83	0.85	0.80	0.86	0.80	0.47	0.08	0.03	0.09	0.07	0.05
4 Resources	No attacks	0.20	0.20	0.21	**0.22**	0.21	**0.22**	0.20	0.13	0.02	0.01	0.03	0.02	0.01
	One Attacker	**0.27**	0.25	0.23	0.24	0.22	0.23	0.22	0.13	0.02	0.01	0.03	0.01	0.01
	Multiple Attackers	**0.60**	0.48	0.43	0.43	0.39	0.40	0.36	0.21	0.03	0.01	0.04	0.03	0.01

scheduling policies could be applied in real-time in order to minimize the impact of cyber-threats.

8. References

[1] J. Lee, B. Bagheri and H. A. Kao, A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3 (2015), 18-23.

[2] R. R. Rajkumar, I. Lee, L. Sha and J. Stankovic, Cyber-physical systems: the next computing revolution. In Proceedings of the 47th Design Automation Conference (2010) (pp. 731-736). ACM.

[3] J. Shi, J. Wan, H. Yan and H. Suo, A survey of cyber-physical systems. In Wireless Communications and Signal Processing (WCSP), 2011 International Conference on (2011) (pp. 1-6). IEEE.

[4] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A. Sadeghi, M. Maniatakos and R. Karri, The cybersecurity landscape in industrial control systems. Proceedings of the IEEE, 104(5), (2016) 1039-1057. doi:10.1109/JPROC.2015.2512235

[5] W. Knowles, D. Prince, D. Hutchison, J. Disso and K. Jones, A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, 9, (2015), 52-80. doi:10.1016/j.ijcip.2015.02.002

[6] A. Chaves, M. Rice, S. Dunlap and J. Pecarina, Improving the cyber resilience of industrial control systems. International Journal of Critical Infrastructure Protection, 17, 2017, 30-48. doi:10.1016/j.ijcip.2017.03.005

[7] National Institute of Standards Techonology (NIST), Framework for Improving Critical Infrastructure Cybersecurity. 2012

[8] L. J. Wells, J. A. Camelio, C. B. Williams and J. White, Cyber-physical security challenges in manufacturing systems. Manufacturing Letters, 2(2), 2014, 74-77.

[9] B. Y. Ekren and A. M. Ornek, A simulation based experimental design to analyze factors affecting production flow time. Simulation Modelling Practice and Theory, 16(3), 2008, 278-293.

[10] O. Feyzioğlu, H. Pierreval and D. Deflandre, A simulation-based optimization approach to size manufacturing systems. International journal of production research, 43(2), 2005, 247-266.

[11] P. Korytkowski and R. Karkoszka, Simulation-based efficiency analysis of an in-plant milk-run operator under disturbances. The International Journal of Advanced Manufacturing Technology, 82(5-8), 2016, 827-837.

[12] R. Caprihan, A. Kumar and K. E. Stecke, Evaluation of the impact of information delays on flexible manufacturing systems performance in dynamic scheduling environments. The International Journal of Advanced Manufacturing Technology, 67(1-4), 2013, 311-338.

[13] National Institute of Standards Techonology (NIST). Guide to Industrial Control Systems (ICS) Security.2015

[14] Q. Chen, M. Trivedi, S. Abdelwahed, T. Morris and F. Sheldon, Model-based autonomic security management for cyber-physical infrastructures. International Journal of Critical Infrastructures (2016), 12(4), 273-294.

[15] J. Hernández Jiménez, Q. Chen, J. Nichols,C. Calhoun and S. Sykes, Towards a Cyber Defense Framework for SCADA Systems Based on Power Consumption Monitoring (2017). Proceedings of the 50th Hawaii International Conference on System Sciences

[16] Q. Chen, R. K. Abercrombie and F. T. Sheldon, Risk assessment for industrial control systems quantifying availability using mean failure cost (MFC). Journal of Artificial Intelligence and Soft Computing Research (2015), 5(3), 205-220.

[17] Q. Chen and S. Abdelwahed, A Model-based Approach to Self-Protection in SCADA Systems. In Feedback Computing (2014).

[18] B. Reaves and T. Morris, Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. International Journal of Critical Infrastructure Protection, 5(3-4), 2012, 154-174. doi:10.1016/j.ijcip.2012.10.001

[19] B. Rahmani and A. H. D. Markazi, Networked control of industrial automation systems—a new predictive method. The International Journal of Advanced Manufacturing Technology, 58(5), 2012, 803-815. doi:10.1007/s00170-011-3416-1

[20] A. A. Cárdenas, S. Amin, Z. S. Lin, Y. L Huang, C. Y Huang and S. Sastry, Attacks against process control systems: risk assessment, detection, and response. In Proceedings of the 6th ACM symposium on information, computer and communications security (2011) , pp. 355-366, ACM.

[21] M. Atighetchi, P. Pal, F. Webber and C. Jones, Adaptive use of network-centric mechanisms in cyber-defense. In Object-Oriented Real-Time Distributed Computing, 2003. Sixth IEEE International Symposium on (pp. 183-192). IEEE.

[22] L. D. Sturm, C. B. Williams, J. A. Camelio, J. White, and R. Parker, "Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. STL file with human subjects," *J. Manuf. Syst.*, vol. 44, pp. 154–164, 2017.

[23] S. E. Zeltmann, N. Gupta, N. G. Tsoutsos, M. Maniatakos, J. Rajendran, and R. Karri, "Manufacturing and security challenges in 3D printing," *Jom*, vol. 68, no. 7, pp. 1872–1881, 2016.

[24] Z. DeSmit, A. E. Elhabashy, L. J. Wells and J. A. Camelio, An approach to cyber-physical vulnerability assessment for intelligent manufacturing systems. Journal of Manufacturing Systems, 43, 2017, 339-351.

[25] H. Vincent, L. Wells, P. Tarazaga, and J. Camelio, "Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems," *Procedia Manuf.*, vol. 1, pp. 77–85, 2015.

[26]N. B. Portilla, M. H. de Queiroz, and J. E. Cury, "Integration of supervisory control with SCADA system for a flexible manufacturing cell," in *Industrial Informatics (INDIN), 2014 12th IEEE International Conference on*, 2014, pp. 261–266.

[27] C. Hauert and G. Szabó, Game theory and physics. American Journal of Physics, 73(5), 2005, 405-414. doi:10.1119/1.1848514

[28] X. Liang and Y. Xiao, Game theory for network security. IEEE Communications Surveys & Tutorials, 15(1), 2013, 472-486. doi:10.1109/SURV.2012.062612.00056.

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

[30] H. Orojloo and M. Azgomi, M., A game-theoretic approach to model and quantify the security of cyber-physical

systems. Computers in Industry, 88, 2017, 44-57. doi:10.1016/j.compind.2017.03.007

[31] D. Shen, G. Chen, E. Blasch and G. Tadda, Adaptive Markov game theoretic data fusion approach for cyber network defense. In Military Communications Conference, 2007. MILCOM 2007. IEEE (pp. 1-7). IEEE.

[32] L. Chen and J. Leneutre, A game theoretical framework on intrusion detection in heterogeneous networks. IEEE Transactions on Information Forensics and Security, 4(2), 2009, 165-178.

[33] K. W. Lye and J. M. Wing, Game strategies in network security. International Journal of Information Security, 4(1-2), 2005, 71-86.

[34] K. Sallhammar, B. E. Helvik and S. J. Knapskog, Towards a stochastic model for integrated security and dependability evaluation. In Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on (pp. 8-pp). IEEE.

[35] B. G. Schlicher and R. K. Abercrombie, Information security analysis using game theory and simulation. In WORLDCOMP'12-The 2012 World Congress in Computer Science, Computer Engineering, and Applied Computing; SAM'12-2012 International Conference on Security and Management (2012), pp. 540-546.

[36] Deloitte US, Cyber risk in advanced manufacturing. https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html. Accessed 23 August 2017

[37] Deloitte Belgium, Global Cyber Executive Briefing Manufacturing https://www2.deloitte.com/be/en/pages/risk/articles/Manufacturing.html. Accessed 23 August 2017