International Journal of Multidisciplinary and Current Research ISSN: 2321-3124
Research Article Available at: http://ijmcr.com

Evaluation of Dynamic Scheduling Policies against Cyber-attacks on an Open-Shop Manufacturing System using Simulation

Alejandro Bracho Avila, Alireza Zarreh*, Can Saygin, Hung-Da Wan, Yooneun Lee

The University of Texas at San Antonio, San Antonio, TX, Department of Mechanical Engineering
Department of Electrical and Computer Engineering, Center for Advanced and Lean Systems (CAMLS)

Received 20 June 2021, Accepted 15 Aug 2021, Available online 21 Aug 2021, **Vol.9 (July/Aug 2021 issue)**

Abstract

In the domain of Cyber-Physical Systems (CPS), there is a significant concern regarding cybersecurity, especially for smart manufacturing systems, allegedly a target of numerous recent cyber attacks. Given this situation, this paper introduces a simulation-based model to assess the repercussions on manufacturing systems' performance under the presence of cybersecurity issues. The objective is to validate countermeasures regarded as a Dynamic Intrusion Response, which could potentially reduce the adverse impact of specific malicious cyber attacks. The effectiveness of adjusting dynamic scheduling policies in response to cyber-attacks has been evaluated through a simulation study based on a manufacturing system. The results reveal that adaptive real-time scheduling policies such as dynamic resource allocation and rerouting of jobs will efficiently reduce the adverse impact of cyber attacks on an open-shop manufacturing environment.

Keywords: *Simulation, Cybersecurity, Manufacturing, Open-shop, Scheduling Policies*

Introduction

The concept of Cyber-Physical Systems (CPS) is applied in manufacturing systems that incorporate the dynamics and characteristics of physical processes with commands originating from the computer software and communication platforms (Shi *et al.* 2011; Lee *et al.* 2015). CPS's are characterized by embedded systems, wireless sensor networks (WSN), and other software platforms when compared to traditional manufacturing systems. (Rajkumar *et al.* 2010). Since these types of systems provide tools for real-time analysis, coordination, and monitoring of the integrated architecture, the operational reliability of such automated processes is critical. In CPS's, 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 numerous researchers. Most of them concentrated on presenting cybersecurity vulnerabilities' assessments and recommending the imperative need of customized Information Technology (IT) security mechanisms to validate the proper execution and safety requirements for ICS (Knowles *et al.* 2015; McLaughlin *et al.* 2016; Chaves *et al.* 2017).

*Corresponding author's ORCID ID: 0000-0002-2093-7859,
Mail: alireza.zarreh@gmail.com
DOI: https://doi.org/10.14741/ijmcr/v.9.4.6

CPS has become exposed further to cyberthreats because of the increasing availability of software platforms and Internet-based capabilities joined into these controlling systems. Hence, the purpose of this paper is to develop a simulation-based model that will enable the manufacturing sector to assess systems' performance metrics under the potential presence of cyber-threats throughout their continuous operations.

Manufacturing companies have been increasingly adopting 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 (Alguliyev *et al.* 2018). This 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 recent capabilities are also augmenting the risk of potential cyber-attacks from malicious outsiders in manufacturing systems.

According to recent information, cybersecurity has become a critical concern for CPS operability for the last decade. A recent report published by the National Institute of Standards and Technology (NIST), indicates that cyber-attacks incurred more than $400B of direct costs per year for companies around the globe (Keith

Stouffer *et al.* 2015). Malicious attacks harm automated processes in many possible ways, and, as shown in several cyber-attack incidents, the manufacturing sector can be one of the main targets (Wells *et al.* 2014). Cyber-attacks on manufacturing systems not only can affect design parameters, overall performance or even quality control (QC) procedures, but also disrupt the product and system design process that makes an adverse impact on the design intent of the products for manufacturing companies.

Nowadays, an important topic for the manufacturing companies is to evaluate the appropriate countermeasures (i.e., defense policies) that will promote an immunity threshold. Considering the fact that investing in protection against all types of malicious attacks is infeasible, a pratical goal for the manufacturers is to ensure proper functionality of their CPS to maintain a similar level of performance during a cyber attack while taking into consideration financial constraints.

This study evaluates the impact of having different controllable defense policies from the company's standpoint while having different security-based parameters from the attacker's perspective. It proposes a discrete-event simulation model that is proven reliable for evaluating the impact of specific circumstances in manufacturing systems and potentially enhancing business decisions (2015, 2016, 2017a; Chen *et al.* 2016).

The main contributions of this paper will be as follows: (1) It demonstrates a method to model the behavior of a manufacturing system in a healthy condition and under security attacks, using a game-theoretic approach to mimic the interaction between the attacker and defender through simulation. (2) It examined how different controllable and uncontrollable factors, such as resource capacity and reorder policies, may affect the performance of the CPS in manufacturing. (3) It proposed and validated countermeasures regarded as Dynamic Intrusion Response, which could potentially reduce the adverse impact of certain malicious cyberattacks.

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 the open-shop scheduling problem. Section 3 describes the research methodology applied in this study. Section 4 presents a case study that is developed in order to validate the applicability of the model. Finally, Section 5 provides a discussion of the results, while Section 6 provides a summary of the main conclusions, the contributions for this paper, and the future research approach.

Literature Review

Security of Industrial Control Systems (ICS)

Over the last decade, the presence of ICS for highly automated processes has been widely discussed. ICS is typically found in the main industrial sectors such as electricity, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, food and beverage, and 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 (2017b).

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 infrastructure important targets for malicious attacks. The importance of identifying cybersecurity vulnerabilities and creating autonomous defense methods for these controlling systems have been extensively discussed before (Chen *et al.* 2015). A research study used a mathematical form of vectors for representing simple and complex attacks as potential industrial radio vulnerabilities (Reaves and Morris 2012). 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 (Rahmani and Markazi 2012). 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 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 considered. 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. For all that, Zhang *et al.*(2019) believed that the current efforts of ICS cybersecurity may not be sufficient for growing cyber threats. Thus, a cyber-attack detection system built on the concept of defense-in-depth is developed. This attack detection system provides a multiple-layer defense to gain the defender's precious time before unrecoverable consequences occur in the physical system.

Cybersecurity in Manufacturing

As many documented incidents exist for different industries over recent years, there is an emerging interest in evaluating the impact of these cyber-threats in manufacturing systems. Wells *et al.* (2014) highlighted some specific cybersecurity vulnerabilities for manufacturing systems while describing potential approaches that should be utilized for analyzing this type of issue. Bracho *et al.* (2017; 2018) suggest a simulation based with statistical analysis to measure the valunerabilies in manufacturing systems while Sturm *et al.* (2017) focused on the vulnerabilities of additive manufacturing (AM) technologies, mainly in using. STL files during its processes. Zeltmann *et al.* (2016) also demonstrated the significance of modifying the design intent of the products for manufacturing companies.

In terms of vulnerabilities in manufacturing, DeSmit *et al.* (2016) proposed an approach for assessing cyber-physical systems in the manufacturing sector, using decision tree analysis. Shih-Yuan Yu *et al.* (2020)

presented a multi-modal sabotage attack detection system for AM machines. They demonstrated that a sabotage attack detection system can detect various attacks by correlating multiple forms of physical-domain emissions of the AM system with cyber-domain information. Vincent *et al.* (Vincent *et al.* 2015) introduced a real-time detection approach for enhancing quality control in manufacturing environments affected by Trojan attacks. Zarreh *et al.* (2018, 2019a, b, 2020; 2019) identified research gaps and challenges to improve overall equipment effectiveness (OEE) in presence of cybersecurity threats in critical manufacturing industries, besides they presented a method to create and solve a game theory model to address cybersecurity issues specifically for advanced manufacturing systems with high-level computer-controlled integration. Shahin *et al.* (2020) proposed a framework to address threats in industry 4.0 environment. Finally, the security of SCADA systems in advanced manufacturing has also been investigated recently (Portilla *et al.* 2014).

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. A general quantitative model to assess the impact of having cyber-threats in manufacturing environments has not been found in the literature.

Open-Shop Scheduling Problem (OSSP) in Manufacturing

Scheduling in manufacturing systems, which is a calendar for manufacturing products or components, is crucial for productivity. Anand and Panneerselvam (2015) provided a systematic literature review on open-shop scheduling problems, as one of the categories of scheduling problems. They classified the problem base on the open-shop measures of performance, namely: minimization of makespan, minimization of the sum of completion times of jobs, minimization of the sum of weighted completion times of all jobs, minimization of total tardiness of all jobs, minimization of the sum of weighted tardiness of all jobs, minimization of the weighted sum of tardy jobs, and miscellaneous measures of the open shop scheduling problem.

To address each or a combination of these problems, different methods are utilized. Panneerselvam *et al.* (2019) considered a Meta-heuristic genetic algorithm (GA) to minimize the makespan of the OSSP. They proposed a new crossover operator, namely the Three Chromosome Juggling Crossover(TCJC) operator for the GA methods to determine whether the GA methods developed using TCJC operator provide better Makespan results when compared to those values given by the GA method developed using one-point crossover operator. Dror (1992) analyzed the minimizing both the mean flow time and the makespan in an open shop problem with machine-dependent processing time using an optimal algorithm with the complexity function. Haidar M. Harmanani *et al.*(Marrouche and Harmanani 2018) resented two *metaheuristic* algorithms for solving the non-preemptive open-shop scheduling problem. The algorithms are based on cuckoo search and dynamic ant optimization. Furthermore, Shareh *et al.* (2020) investigated the task scheduling problem in open shops using the Bat Algorithm (BA) based on ColReuse and substitution meta-heuristic functions to reduce total execution time.

Mahapatra *et al.* (2017) addressed the waiting time in task scheduling problems by minimizing the waiting time variance of a task which is an NP-hard problem to achieve the quality of service in a single or parallel processor. They applied five heuristic-based solutions to minimize the waiting time variance.

In contrast with deterministic approaches used by most researchers, Nasiri *et al.* (2017) developed a simulation-based real-time scheduling composite dispatching rule to mimic realistic circumstances in open shop scheduling problems which consist of uncertainty and stochastic parameters. They minimized the mean waiting time of jobs in a non-preemptive open shop with stochastic ready times using a multi-response optimization approach based on computer simulation for scheduling.

Research Methodology

In this research, the effect of cybersecurity threats on the performance of a manufacturing system with highly integrated cyber and physical subsystems has been studied. A quantitative study is proposed to evaluate the impact of implementing different countermeasures regarded as a Dynamic Intrusion Response, and attacker-related factors under the presence of potential cyber-threats that cause delays in processing times of the production system. A case of manufacturing is modeled and simulated using Arena® from Rockwell Automation to illustrate the method. The selected manufacturing system consists of an open-shop environment with different types of jobs that need to be scheduled. Then, three potential scenarios have been developed to evaluate the overall performance of the system in the presence of cyber-attacks while different dynamic intrusion responses have been implemented.

Model Description

A model of a cyber-physical manufacturing system was developed using Arena® simulation software. It includes the arrival of attacks, which will be modeled as entities that will impact the cyber-system, and therefore, the physical workstations' processing time. Components of the simulation model are explained further in the following sub-sections. The flowchart of the created simulation logic for this case study can be seen in
Figure **1** and

Figure **2**. Again, the objective is using simulation for revealing the average long-run performance metrics of the system for the entire simulation length, which will permit to have a quantitative assessment of the breach impact for a CPS in this type of physical manufacturing environment.

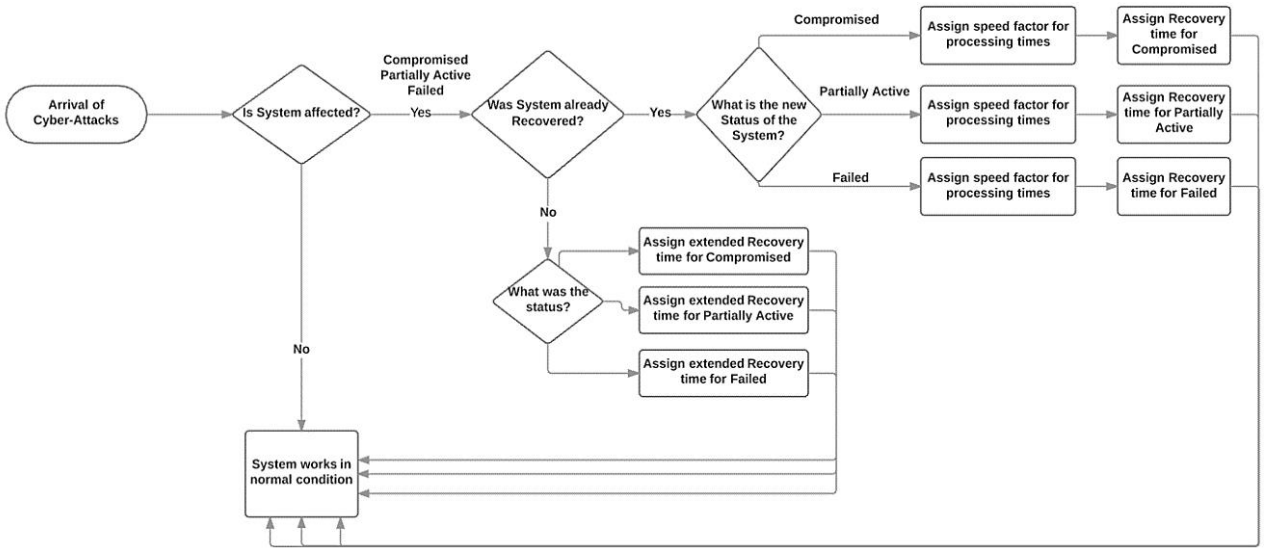

Figure 1. Flowchart logic for the cyber system

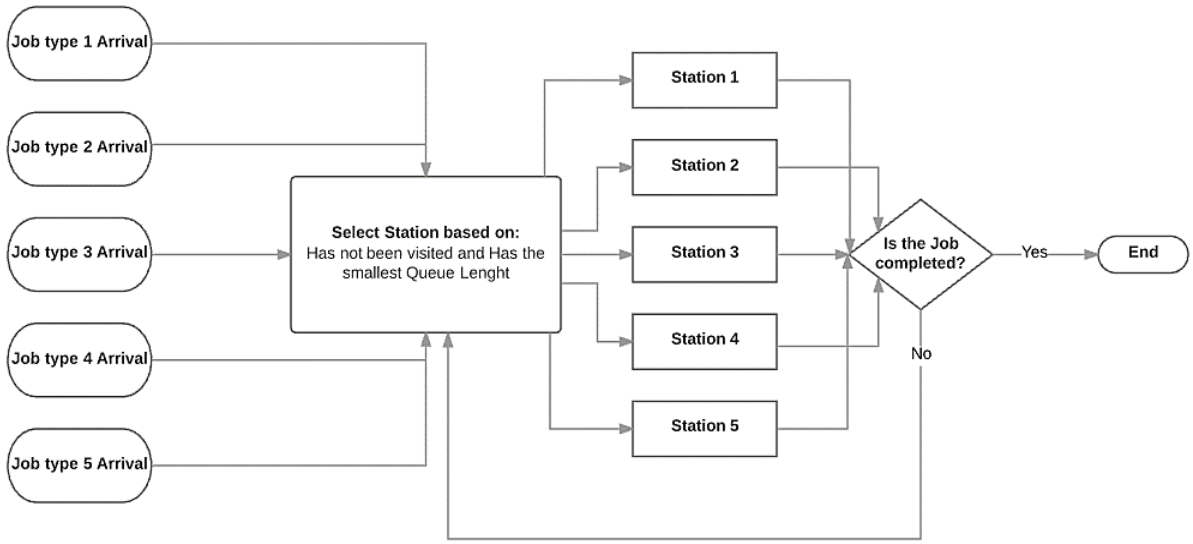

Figure 2. Flowchart logic for the physical system

Arrival of Cyber-attacks

Cyber-attacks are modeled as entities that will arrive following an exponential distribution with a mean time between arrivals of 5 hours. Again, these attacks can be successful or defused, which will maintain or modify the current status of the cyber-system. The CPS will either behave in a "Normal (G)", "Compromised (C)", "Partially Active (PA)" or "Failed (F)" state depending on the levels of impact from cyber-attacks. The outcome of the attacks for this case study will be probabilistic with the following considerations: 30% chance of ending in (G) (i.e. attack defused), 30% chance of ending in (C), 20% chance of ending in (PA) and 20% chance of ending in (F). Finally, based on the current status of the system, the processing times of physical workstations will be multiplied by a stochastic "speed factor", which will cause delays in the overall production performance of the manufacturing system.

The Cyber System

This portion of the model represents the Intrusion Detection System (IDS) of the whole networked CPS, and it has the same considerations as Case Study #1. Once attacks affect the cyber-system, the impact will be induced on its physical operations. Then, the IDS will deploy a Dynamic Intrusion Response in order to reduce the adverse impact on the system's performance. The system will need a certain period of time (MRT) to return to a "Normal" state. The MRT for affected states will follow an exponential distribution with the following mean values: 1.5 hours for "Compromised", 3 hours for "Partially Active" and 15 hours for "Failedharm

The Physical System

This portion of the model represents the material's flow layout throughout the physical manufacturing system. In

this case, the physical system represents an automated Order Picking Operations system in a manufacturing warehouse, which is equivalent to an open-shop manufacturing system. The data for this model follow the considerations described in Nasiri *et al.* (2017). These are described as follows:

- The physical manufacturing system consists of an open-shop environment with five types of jobs as entities and five different workstations. Being an open-shop scheduling problem (OSSP), all jobs have to visit all five stations in order to be completed, yet, there is no specific sequence for these operations.
- Workstations are not identical. Each workstation consists of a single machine that performs a different type of operation.
- Each job type has a different arrival rate and processing time at each workstation. Arrival rates for each job type and Processing Time of each job at each workstation is modeled as stochastic and can be seen in Table 1 and Table 2, respectively.
- Once jobs arrive into the system, station selection will be made based on the Queue Length.
- Once a job has visited a specific station, it does not need to be revisited by that same entity.
- Once a job enters a Queue, the dispatching priority of these jobs will be based on the score from a combined equation. This equation will be further discussed in section 4.2.
- The performance metrics selected for assessing the impact of cyber-attacks will be the average waiting time for each job type and the average flow time of jobs. Therefore, the objective is to determine what could be the best dynamic intrusion responses that will reduce the overall value of these averaged metrics.

The OSSP is considered to be an NP-hard problem. Therefore, mathematical modeling is not efficient for capturing the behavior of this type of system since most of the parameters are stochastic. For this reason, simulation software is an excellent fit for modeling this type of complex systems.

Table 1. The time between arrivals for each Job type

Job Type	The time between arrivals (minutes)
1	Uniform(40,60)
2	Triangular(50,51,62)
3	Normal(45,6)
4	Normal(35,3)
5	Exponential(43)

Table 2. Processing times of each Job in each Station

Job Type	Station (Machine)	Processing Time (minutes)
1	M1	Normal(6,0.2)
1	M2	Uniform(4,6)
1	M3	Triangular(4,5,6)
1	M4	Normal(6,0.4)
1	M5	Normal(4,0.1)
2	M1	Normal(6,0.1)
2	M2	Triangular(5,6,7)
2	M3	Normal(8,0.5)
2	M4	Triangular(3,4,5)
2	M5	Triangular(5,6,8)
3	M1	Exponential(7)
3	M2	Exponential(6)
3	M3	Normal(6,0.5)
3	M4	Uniform(4,8)
3	M5	Triangular(7,8,10)
4	M1	Uniform(8,9)
4	M2	Normal(7,0.2)
4	M3	Triangular(6,7,8)
4	M4	Normal(4,0.1)
4	M5	Normal(7,0.5)
5	M1	Exponential(6)
5	M2	Normal(8,0.5)
5	M3	Uniform(6,8)
5	M4	Exponential(4)
5	M5	Uniform(6,9)

Run Setup

For each scenario, the simulation model was run for 30 days, 8 hours a day, with 10 replications. At the end, the long-run average values of selected performance metrics were collected.

Evaluation of Dynamic Intrusion Responses

Once the model is built as the original scenario, "what-if" scenarios are created to elucidate the best responses among different countermeasures. Different manufacturing scheduling policies will be used as parameters for the scenarios; thus the benefit of implementing these potential countermeasures will be assessed through the performance of the system under the presence of cyber-attacks that impact the processing times of jobs for each scenario. The average waiting time for each job type, the average utilization of workstations, and the average flow time per job will be collected as performance metrics for each scenario.

The policies that will be implemented in the original manufacturing system as countermeasures against cyber-threats are described as follows:

Optimization of Dispatching Priority rule for Jobs waiting in a Queue

In this case study, the priority of jobs to be processed in a queue will be determined by the score of a combined dispatching priority rule, which is a revised version of the equation introduced by Nasiri *et al.* (Nasiri *et al.* 2017). The value of this rule is computed by the weighted sum of the two standardized dispatching rules: (1) processing time of a current job on the current machine and (2) remaining processing time of the job to be entirely completed. This combined dispatching rule is calculated for each job that enters a queue, and the jobs with a higher score will be considered as prior jobs to be processed on the machine. The combined dispatching rule (CDR) is calculated by the following equation:

$$CDR = W_1 * \left(1 - \left(\frac{P_{ij}}{\sum_{j=1}^{n} P_{ij}}\right)\right) + W_2 * \left(\frac{R_i}{\sum_{j=1}^{n} P_{ij}}\right) \quad (1)$$

where W_1 is the weight of processing time of the job in the combined dispatching priority rule, W_2 is the weight of the remaining time of the job in the combined dispatching priority rule, R_i is the remaining processing time of the job i to be completed, and P_{ij} is the processing time of job i on machine j.

This countermeasure is used to find the optimal value of the weights in the CDR, so that the mean waiting time of jobs can be minimized. Instead of finding the optimal value from a brute-force enumeration, we use a simulation optimization package, OptQuest, in searching solution space efficiently. For this purpose, differently, from their approach, Arena ® simulation software package in conjunction with its optimization tool called "OptQuest" was used, because it is a user-friendly tool included in the Arena Software application that can search throughout the solution space universe much more efficiently than brute force enumeration.

On-call for additional resources

The purpose of this policy is to temporarily compensate for the impact on processing times caused by cyber-attacks by adding additional resources on affected machines until the system is fully recovered.

Dynamic Resource Allocation (DRA)

The purpose of this policy is to temporarily compensate for the impact on processing times caused by cyber-attacks by relocating existing resources among stations until the system is fully recovered. The concept of DRA has been implemented by many researchers in many areas related to manufacturing before. For example, the studies of Saygin & Tamma (Saygin and Tamma 2012) and Gunn (Gunn 2010) have already been mentioned in section 2.

However, in terms of smart manufacturing systems that heavily rely on automated processes, it might not be that simple to find real-world applications that are suitable for this type of policy. In other words, the concept of DRA may be more suitable with service industries where human resources can be redistributed in real-time among different locations of the whole system in order to compensate for current bottlenecks or variability.

Nevertheless, DRA is not unique to service or production processes. Having an open-shop environment case study where cyber-attacks can compromise the operability of the system, makes possible to imagine different applications where tools, operators, or even computing servers can be seen as resources that could move throughout the system, therefore, the results of implementing this policy as a potential countermeasure should be analyzed. Previous research work on the topic of dynamic resource allocation has addressed the optimization of computing and parallel servers, where it is vital to obtain the maximum computing capacity available with existing resources.

Rerouting of Jobs among Stations

The purpose of this policy is that, in situations where the security of the system has been compromised, some of the jobs that were waiting in an affected machine's queue are rerouted to a different alternative machine that is not affected by the attack. With this, the possibility of jobs waiting in a machine's queue with a higher processing time is shortened, and therefore, the mean waiting time of jobs can also be reduced.

This policy has been extensively discussed in the literature before. To give a few examples, Nof & Grant (Nof and Hank Grant 1991) provided a survey of adaptive scheduling policies in manufacturing systems, where they highlighted the importance of rerouting jobs to alternative machines motivated by stochastic events. Similarly, Kim & Kim (Kim and Kim 1994) and Belz & Mertens (Belz and Mertens 1996) used simulation software to reschedule jobs in flexible manufacturing systems effectively. Finally, Kutanoglu & Sabuncouglu (Kutanoglu and Sabuncuoglu 2001) examined different reactive scheduling policies based on the rerouting of jobs for machine breakdowns in a dynamic job shop environment.

Experimental Scenarios

In order to evaluate these dynamic intrusion responses in our model, the cyber-attacks will be modeled as random events that affect the availability of machines according to the current status of the system described in Section 3.1.1. As shown in Table 3, several experimental scenarios have been created and are described in the following sub-sections.

Table 3. Overview of experimental scenarios

Setting 1: Original System with No Attacks
Scenario 1: Baseline Model with No Attacks
Setting 2: Original System under Attacks
Scenario 2-0: No Defense to Attacks
Scenario 2-1: Dispatching Priority Rule
Scenario 2-2: On-call for Additional Resource
Setting 3: Dual-Capacity System under Attacks
Scenario 3-0: No Defense to Attacks
Scenario 3-1: Dynamics Resource Allocation
Scenario 3-2: Rerouting of Jobs
Scenario 3-3: Hybrid Policy of 3-1 and 3-2

Scenario 2-1: Optimization of Dispatching Priority rule

From the result of the simulation optimization, the optimal values of the weights in the combined dispatching rule should be 0.9025 and 0.0267 for W1 and W2, respectively. For future scenarios, the optimal values of the Weights for the dispatching priority rule will be considered.

Scenario 2-2: On-call for additional resources

For this scenario, an on-call logic for additional resources during recovery from attacks have been implemented. The affected machines' capacity will be temporarily increased by one while the system is not working under normal conditions.

Scenario 3-0: The Physical System has been revised

At this point, even though the policies applied in Scenario 1 and 2 have shown considerable improvement on performance metrics, they are not considered as dynamic reactive policies for real-time stochastic events in a manufacturing system, but as fixed solutions that ultimately will improve the system's performance for the long-run. The reality is that, for a considerably small open-shop environment like this (i.e., 5 jobs x 5 machines), there is not enough flexibility of resources and alternative machines for implementing dynamic scheduling policies such as DRA and rerouting of jobs; thus the results of examining these potential intrusion responses in such system's size will be barely influential.

For this scenario and further, the physical system will be modeled as an open-shop environment with five types of jobs and five workstations, but each workstation will consist of two alternative machines in parallel for the same operation (i.e., 5 jobs and 10 machines). This consideration also implies that the total resource capacity of the system has been increased to 10, instead of 5; where we will have two alternative machines for each operation needed. The arrival rates of the jobs have also been doubled so that all scenarios can be consistent and comparable.

Scenario 3-1: Dynamic Resource Allocation (DRA)

For this scenario, a DRA policy during recovery from attacks has been implemented. The resources will be temporarily moving throughout the system to compensate for the increase in utilization rates for affected machines while the system is not working under normal conditions.

Scenario 3-2: Rerouting of jobs

Under this scenario, cyber-attacks do not cause a complete breakdown of machines but a temporary increase of its processing times. For this reason, once the system is affected by cyber-attacks, the approach for this scenario is that affected machines will maintain a fixed buffer of jobs waiting in the queue. The new arrivals that exceed this cap will be rerouted to an alternative machine that: (1) was not affected by the attack, (2) has not been visited before and (3) has the smallest queue length. These machines only would be utilized in case of failure of production machines.

Scenario 3-3: Dynamic Resource Allocation + Rerouting of jobs

For this scenario, a combination of both policies applied in scenarios 3-1 and 3-2 will be implemented as a way of validating its overall effect on the system's performance under the presence of cyber-attacks.

Results and Discussions

In this section, the validation of the proposed method as a countermeasure of cyber-attack is discussed. As can be seen, the attack could drastically change the waiting time and flow time in the system which could lead to considerable harm in company's financial income as well as its reputation.

The performance of the physical system under the presence of potential cyber-attacks will be assessed by comparing the results obtained in the experimental scenarios mentioned in the previous section. Specifically, an ANOVA statistical test was applied to all scenarios where intrusion responses are being executed, based on the average flow time of jobs for each scenario. Overall, the experimental scenarios have revealed that all dynamic intrusion responses applied are significant for the performance of the system, as in Table 3., A comparison of results among scenarios is shown in Table 4, Table 5, Figure 3, and Figure 4.

Table 3. Analysis of Variance for Average Flow Time among scenarios

Source	DF	Adj SS	Adj MS	F-Value	P-Value
Scenarios	5	374.6	74.915	24.20	0.0000
Error	54	167.2	3.096		
Total	59	541.8			

Table 4 summarizes performance of the original system with 5 jobs and 5 machines, i.e., Scenario 1 and 2. Although Scenario 2-1 is effective, Scenario 2-2 shows the most significant improvement compared to the no defense system under attack (Scenario 2-0) with a 58.49% decrease in the average flow time of jobs.

Table 4. Performance comparison among scenarios for setting 1 and 2 (5 jobs, 5 machines)

	Job Type	Scenario 1	Scenario 2-0	Scenario 2-1	% Change	Scenario 2-2	% Change
Waiting Time (Hrs)	J1	0.22	9.77	7.95	-18.63	2.67	-72.67
	J2	0.20	9.13	3.26	-64.29	0.79	-91.35
	J3	0.19	7.57	7.72	1.98	4.60	-39.23
	J4	0.18	8.51	4.16	-51.12	1.04	-87.78
	J5	0.27	8.74	14.84	69.79	7.19	-17.73
Average Flow Time (Hrs)		0.74	9.42	7.90	-16.14	3.91	-58.49

For Scenario 3, the revised physical system with alternative machines (5 jobs and 10 machines) shown in Table 5, the best results are encountered in Scenario 3-3 where dynamic scheduling policies related to both resource allocation and rerouting of jobs are applied. This was translated into 64.88% of improvement in terms of average flow times for jobs, consequently making it possible to compensate for the adverse impact of process delays caused by cyber-attacks.

Table 5. Performance comparison among scenarios for setting 3 (5 jobs, 10 machines)

	Job Type	Scenario 3-0	Scenario 3-1	% Change	Scenario 3-2	% Change	Scenario 3-3	% Change
Waiting Time (Hrs)	J1	0.49	0.34	-30.61	0.39	-20.41	0.19	-61.22
	J2	0.54	0.32	-40.74	0.40	-25.93	0.19	-64.81
	J3	3.11	0.33	-89.39	2.10	-32.48	0.20	-93.57
	J4	0.78	0.27	-65.38	0.51	-34.62	0.17	-78.21
	J5	2.32	0.43	-81.47	1.42	-38.79	0.22	-90.52
Average Flow Time (Hrs)		2.05	0.86	-58.05	1.57	-23.41	0.72	-64.88

Even though the outcome of the first two scenarios (Tabel 5) are less significant in comparison with the revised system (Table 6) since their deployment would need no extra cost, they could be considered by some company. Every company should have a threshold for their security. If the system cannot afford the cost of implementing scenario 3 (extended system) and the first two scenarios could satisfy this security limit, they could be utilized to reduce the effect of a cybersecurity attack (Figure 3). Moreover, the effectiveness of these scenarios will be higher for more complex systems with a higher number of jobs and more machines to process them when only a few of the machines are under attack and cannot perform with standard capacity and speed.

On the other side, if the consequences of an attack are too devastating, or the recovery of such an attack is expensive, the impact of the attack could be almost entirely compensated in terms of average flow time, as can be seen with implementing the third scenario and providing backup machines (Figure 4), which would be ideal for a sensitive system with mass production.

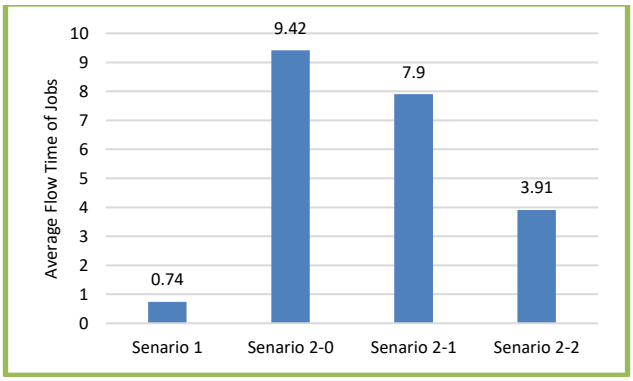

Figure 3. Average flow time comparison among scenarios, setting 1 and 2

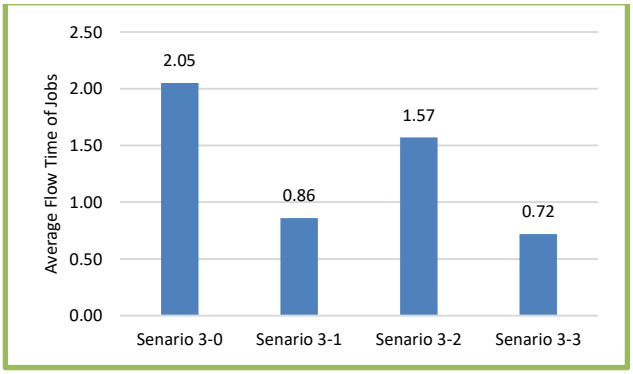

Figure 4. Average flow time comparison among scenarios, setting

Furthermore, when dynamic scheduling policies are compared, it is observed that the DRA policy outperforms the possibility of rerouting jobs as a potential countermeasure during security breaches in manufacturing systems for this specific case study. One of the reasons for this finding could be attributed to the flexibility of the system determined by the quantity of alternatives machines. Finally, as the expanded system also considers doubling arrival rates for jobs, it can be concluded that the best performance among all scenarios is found in 3-3, where the system has enough capacity to apply dynamic scheduling policies as potential countermeasures against cyber-threats that affect processing times of machines.

Conclusions

In this paper, a simulation study was developed as a way to quantify the impact of potential cybersecurity threats on the manufacturing system's performance. In order to elucidate an effective set of scheduling policies that will reduce the adverse impact of cyber-threats, several experimental scenarios have been created through the development of two case studies for the manufacturing sector.

For the case study, the potential arrival of cyber-attacks in an open-shop manufacturing environment was modeled. Again, finding the most effective set of scheduling policies was the objective, which was addressed by comparing the performance results obtained in the experimental scenarios created for this case. Overall, the scenarios have revealed that all dynamic intrusion responses applied, such as optimization of the dispatching rule, dynamic resource allocation, and rerouting of jobs, can significantly reduce the adverse impact on the performance of the system. Subsequently, the original physical system configuration was revised to analyze the benefit of implementing dynamic scheduling policies in this type of manufacturing system by having on-call resources as in scenarios 3-1, 3-2 and 3-3. In fact, since the expanded system also considers the increase of the arrival rates for jobs, it can be concluded that the best performance among all scenarios is scenario 3-3, where dynamic resources allocation in conjunction with a dynamic rerouting of jobs are applied as countermeasures, which achieved 64.88% reduction in average flow times. Mainly for this case study, a suitable immunity threshold can be found when the physical layout has enough capacity and flexibility to apply dynamic scheduling policies as potential intrusion responses against cyber-threats that affect processing times of machines in smart manufacturing systems.

One limitation of this research is that it focuses on the availability of equipment and capability to fulfill customer demand, while in practice, manufacturers are also concerned about Cost and Quality as the primary performance metrics. This limitation leads to an opportunity to improve the accuracy of modeling and analysis.

In summary, these directions can be considered for future research: i) incorporating a cost function for the implementation of the scheduling policies, which will permit to introduce an optimization approach to find the best combination of effective scheduling policies while minimizing costs for the manufacturing company, ii) assessing the impact of information delays in the integrated management software platform (e.g. ERP systems) of a whole supply chain environment caused by cyber-attacks, iii) modeling the impact of cyber-attacks in manufacturing, by using a client-server architecture for the cyber-system and evaluating performance metrics from a computer information systems point of view using simulation and iv) introduce a simulation study for analyzing the evolution of cyber-attacks overtime in manufacturing.

References

[1]. Alguliyev R, Imamverdiyev Y, Sukhostat L (2018) Cyber-physical systems and their security issues. Comput Ind 100:212–223. https://doi.org/10.1016/j.compind.2018.04.017

[2]. Anand E, Panneerselvam R Development of efficient genetic algorithm for open shop scheduling problem to minimise makespan. 35

[3]. Anand E, Panneerselvam R (2015) Literature review of open shop scheduling problems. Intell Inf Manag 7:33

[4]. Belz R, Mertens P (1996) Combining knowledge-based systems and simulation to solve rescheduling problems. Decis Support Syst 17:141–157

[5]. Bracho A (2017) Assessing the Impact of Cyber-Threats on Smart Manufacturing Systems through a Simulation Study - ProQuest

[6]. Bracho A, Saygin C, Wan H, et al (2018) A simulation-based platform for assessing the impact of cyber-threats on smart manufacturing systems. Procedia Manuf 26:1116–1127. https://doi.org/10.1016/j.promfg.2018.07.148

[7]. Chaves A, Rice M, Dunlap S, Pecarina J (2017) Improving the cyber resilience of industrial control systems. Int J Crit Infrastruct Prot 17:30–48

[8]. Chen Q, Abercrombie RK, Sheldon FT (2015) Risk assessment for industrial control systems quantifying availability using mean failure cost (MFC). J Artif Intell Soft Comput Res 5:205–220

[9]. Chen Q, Trivedi M, Abdelwahed S, et al (2016) Model-based autonomic security management for cyber-physical infrastructures. Int J Crit Infrastruct 12:273–294
[10]. DeSmit Z, Elhabashy AE, Wells LJ, Camelio JA (2016) Cyber-physical vulnerability assessment in manufacturing systems. Procedia Manuf 5:1060–1074
[11]. Dror M (1992) Openshop scheduling with machine dependent processing times. Discrete Appl Math 39:197–205. https://doi.org/10.1016/0166-218X(92)90176-B
[12]. Gunn G (2010) Maximizing throughput using dynamic resource allocation and discrete event simulation. PhD Thesis, Clemson University
[13]. Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, et al (2015) Guide to Industrial Control Systems (ICS) Security
[14]. Kim MH, Kim Y-D (1994) Simulation-based real-time scheduling in a flexible manufacturing system. J Manuf Syst 13:85–93
[15]. Knowles W, Prince D, Hutchison D, et al (2015) A survey of cyber security management in industrial control systems. Int J Crit Infrastruct Prot 9:52–80
[16]. Kutanoglu E, Sabuncuoglu I (2001) Routing-based reactive scheduling policies for machine failures in dynamic job shops. Int J Prod Res 39:3141–3158
[17]. Lee J, Bagheri B, Kao H-A (2015) A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manuf Lett 3:18–23
[18]. Mahapatra S, Dash RR, Pradhan SK (2017) Heuristics Techniques for Scheduling Problems with Reducing Waiting Time Variance. In: Heuristics and Hyper-Heuristics-Principles and Applications. InTech
[19]. Marrouche W, Harmanani HM (2018) Heuristic Approaches for the Open-Shop Scheduling Problem. In: Latifi S (ed) Information Technology – New Generations. Springer International Publishing, Cham, pp 691–699
[20]. McLaughlin S, Konstantinou C, Wang X, et al (2016) The cybersecurity landscape in industrial control systems. Proc IEEE 104:1039–1057
[21]. Nasiri MM, Yazdanparast R, Jolai F (2017) A simulation optimisation approach for real-time scheduling in an open shop environment using a composite dispatching rule. Int J Comput Integr Manuf 30:1239–1252
[22]. Nof SY, Hank Grant F (1991) Adaptive/predictive scheduling: review and a general framework. Prod Plan Control 2:298–312
[23]. Portilla NB, de Queiroz MH, Cury JE (2014) Integration of supervisory control with SCADA system for a flexible manufacturing cell. In: Industrial Informatics (INDIN), 2014 12th IEEE International Conference on. IEEE, pp 261–266
[24]. Rahmani B, Markazi AHD (2012) Networked control of industrial automation systems—a new predictive method. Int J Adv Manuf Technol 58:803–815
[25]. Rajkumar RR, Lee I, Sha L, Stankovic J (2010) Cyber-physical systems: the next computing revolution. In: Proceedings of the 47th design automation conference. ACM, pp 731–736
[26]. Reaves B, Morris T (2012) Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. Int J Crit Infrastruct Prot 5:154–174
[27]. Saygin C, Tamma S (2012) RFID-enabled shared resource management for aerospace maintenance operations: a dynamic resource allocation model. Int J Comput Integr Manuf 25:100–111
[28]. Shahin M, Chen FF, Bouzary H, Zarreh A (2020) Frameworks Proposed to Address the Threat of Cyber-Physical Attacks to Lean 4.0 Systems. Procedia Manuf 51:1184–1191. https://doi.org/10.1016/j.promfg.2020.10.166
[29]. Shareh MB, Bargh SH, Hosseinabadi AAR, Slowik A (2020) An improved bat optimization algorithm to solve the tasks scheduling problem in open shop. Neural Comput Appl. https://doi.org/10.1007/s00521-020-05055-7
[30]. Shi J, Wan J, Yan H, Suo H (2011) A survey of cyber-physical systems. In: Wireless Communications and Signal Processing (WCSP), 2011 International Conference on. IEEE, pp 1–6
[31]. Sturm LD, Williams CB, Camelio JA, et al (2017) Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the. STL file with human subjects. J Manuf Syst 44:154–164
[32]. Vincent H, Wells L, Tarazaga P, Camelio J (2015) Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems. Procedia Manuf 1:77–85
[33]. Wells LJ, Camelio JA, Williams CB, White J (2014) Cyber-physical security challenges in manufacturing systems. Manuf Lett 2:74–77
[34]. Yu S-Y, Malawade AV, Chhetri SR, Al Faruque MA (2020) Sabotage Attack Detection for Additive Manufacturing Systems. IEEE Access 8:27218–27231. https://doi.org/10.1109/ACCESS.2020.2971947
[35]. Zarreh A (2019) Proactive Evaluation and Risk Analysis for Cybersecurity in Manufacturing Systems Using Game Theory Method - ProQuest
[36]. Zarreh A, Lee Y, Janahi RA, et al (2020) Cyber-Physical Security Evaluation in Manufacturing Systems with a Bayesian Game Model. Procedia Manuf 51:1158–1165. https://doi.org/10.1016/j.promfg.2020.10.163
[37]. Zarreh A, Saygin C, Wan H, et al (2018) A game theory based cybersecurity assessment model for advanced manufacturing systems. Procedia Manuf 26:1255–1264. https://doi.org/10.1016/j.promfg.2018.07.162
[38]. Zarreh A, Wan H, Lee Y, et al (2019a) Cybersecurity Concerns for Total Productive Maintenance in Smart Manufacturing Systems. Procedia Manuf 38:532–539. https://doi.org/10.1016/j.promfg.2020.01.067
[39]. Zarreh A, Wan H, Lee Y, et al (2019b) Risk Assessment for Cyber Security of Manufacturing Systems: A Game Theory Approach. Procedia Manuf 38:605–612. https://doi.org/10.1016/j.promfg.2020.01.077
[40]. Zeltmann SE, Gupta N, Tsoutsos NG, et al (2016) Manufacturing and security challenges in 3D printing. Jom 68:1872–1881
[41]. Zhang F, Kodituwakku HADE, Hines JW, Coble J (2019) Multilayer Data-Driven Cyber-Attack Detection System for Industrial Control Systems Based on Network, System, and Process Data. IEEE Trans Ind Inform 15:4362–4369. https://doi.org/10.1109/TII.2019.2891261
[42]. (2017a) Cyber risk in advanced manufacturing | Deloitte US. In: Deloitte U. S. https://www2.deloitte.com/us/en/pages/manufacturing/articles/cyber-risk-in-advanced-manufacturing.html
[43]. (2016) Manufacturing - Cyber Executive Briefing | Deloitte | Analysis. In: Deloitte Belg. https://www2.deloitte.com/be/en/pages/risk/articles/Manufacturing.html
[44]. (2015) Dell Security Annual Threat Report 2015
[45]. (2017b) Framework for Improving Critical Infrastructure Cybersecurity