ANALYSIS OF THE IMPACT OF CYBER ATTACK ON SEMICONDUCTOR MANUFACTURING ENERGY QUANTIFICATION

Busra Ezici
Paulo Costa
Jie Xu

Systems Engineering and Operations Research
George Mason University
4400 University Dr
Fairfax, VA, USA
{bozoglu, pcosta, jxu13}@gmu.edu

ABSTRACT

Semiconductor manufacturers deal with complex processes, diverse product lines, and rapidly changing technologies while facing a competitive global market. There is also increased adoption of digital technologies with globalization, which creates an interconnection between each process. Digital connectivity and adaptation to advanced automated technologies increase dependence on data and the vulnerability to cyber-attacks. The presence of cyber-attacks in manufacturing causes delays in processing times for manufacturing, which impact performance and energy consumption. This study proposes a framework consisting of an energy quantification model, cyber risk modeling, and simulation analyses to address the impact of cyber threats on the energy quantification of semiconductor manufacturing. The performance of the wafer fab is analyzed using the cycle time, throughput rate, and work-in-process level since they lead to the energy quantification in processes. Then the cyber-attack scenario is included in the simulation model to evaluate the impact of the cyberattack on energy quantification.

Keywords: Semiconductor Manufacturing, Simulation Analysis, Workflow Modeling, Cyber-attacks

1 INTRODUCTION

A semiconductor, also known as integrated circuits (ICs), or chips, is a tiny electronic device composed of many components that store, move, and process data (Platzer, Jr, and Sutter 2020). The manufacturing of semiconductors begins with the arrival of raw input and materials, which is then followed by front-end (wafer fab) and back-end operations (assembly, sort, test) (Kannaian 2018). In a wafer fab, first, a furnace forms a cylinder of silicon or other semiconducting materials, which is then cut into disc-shaped wafers. A chip may contain so many layers in total and require many chemical processes such as deposition, oxidation, diffusion, photolithography, etching, photoresisting, layering, and doping. Deposition tools form the basis of a new permanent layer by adding a material film. Then, the photolithography process draws circuit patterns in the layer, starting with coating a photoresist on the deposited material. A photolithography tool passes light through a photomask to transfer that pattern to the photoresist. The light dissolves parts of the photoresist considering the circuit pattern. Etching is the tool carving the newly created pattern in the photoresist into the permanent layer below the photoresist. The photoresist is removed, and the etched material is cleaned off the layer. Other times, atoms are embedded into the layer in an ion implantation process

ANNSIM'22, July 18-20, 2022, San Diego, CA, USA;

instead of etching. Then, the completed layer is flattened with chemical mechanical planarization(CMP) process. This allows a new layer to be added, and the cycle begins again. Process control tools are used to inspect the wafer and its layers throughout fabrication to ensure no errors in the system (Khan 2021). This process requires 300 to 700 different processing steps and makes it the most complex portion of the entire manufacturing process (Kannaian 2018). Assembly, testing, and packaging (ATP) are also known as back-end processes. The wafer is cut into individual ICs, also known as dies, and the failed ICs are scrapped (Kannaian 2018). The Assembly phase starts with cutting a finished wafer into separate chips. Each chip is attached to a frame with wires that connect the chip to external devices and enclosed in a protective casing, so a dark gray rectangle with metal pins at the edges produces a final look. The testing procedure is also applied to the chips to ensure it operates as intended (Khan 2021).

The US depends on global supply chains and production concentrated in East Asia. Therefore, vulnerability to disruption or denial due to trade disputes could be detrimental. Manufacturing disruptions during the COVID-19 pandemic have significantly increased this concern. So, it is very important to improve processes and expand/retain advanced domestic semiconductor fabrication plants (Platzer, Jr, and Sutter 2020). Also, high-tech fabrication plants used for the production of the semiconductor or thin-film-transistor liquid crystal display (TFT-LCD) are energy and technology-intensive industries (Hu, Lin, Fu, Chang, and Cheng 2019). In addition to a very competitive global market and energy intensity, semiconductor manufacturers must deal with complex processes, sophisticated equipment, diverse product lines, and rapidly changing technologies. The digitization in the industry increases dependence on data, and the adaptation with advanced automated technologies increases the vulnerability for cyber-attacks (Laboratory 2020). The presence of cyber attack in manufacturing cause delays in processing times for manufacturing (Avila 2017) and have an impact on production performance and energy consumption.

The objective of this study is to establish and assess performance metrics by exploring the modeling and simulation of semiconductor wafer fab manufacturing processes, with the goal of providing an energy quantification framework for semiconductor manufacturing in the presence of a cyber attack. This study also aims to provide a cyber risk assessment framework for semiconductor manufacturing. This analysis included three important steps: the energy quantification model, cyber risk analysis framework, and simulation analysis. The rest of the paper is organized as follows. Section 2 provides the related literature. Section 3 introduces the methodology for energy quantification, cyber risk quantification framework, and simulation model. Section 4 proposed the experimental analysis for Intel minifab model. The research is concluded, and further research directions are provided in Section 5.

2 LITERATURE REVIEW

Several studies in literature are relevant to our research, which include simulation modeling of semiconductor manufacturing, general cyber threats in manufacturing, and cyber risk assessment with simulations. (Rose 2000) analyzed the behavior of complex wafer fabs in certain scenarios by estimating cycle time and WIP level using simulation on the MIMAC dataset. (Morrice, Valdez, Chida, and Eido 2005) proposed a model for supply chain planning and inventory control to predict the effect of internal on-time delivery, inventory, and WIP changes on the customer order fulfillment service level by using simulation. Their work was based on historical data and expert opinion. (Li, Ramírez-Hernández, Fernandez, McLean, and Leong 2005) proposed a model for standard modular simulation of semiconductor wafer fabrication facilities. They used the Intel minifab model to analyze the impact of the workforce in production performance using cycle time, throughput rate, and WIP level as performance metrics. (Liu, Li, Yang, Wan, and Uzsoy 2011) proposed production planning for semiconductor manufacturing via simulation optimization. (Valente, Christiano Cecone, Alvim, and Cassiano 2015) aimed to optimize the semiconductor manufacturing process using variation in the number of machines and operators. They used the Intel Five-Machine Six-Step Mini-Fab model during experimental analysis but considered only two different entities as input and ignored

the test wafer. Also, preventive maintenance time was different for each cell from the real case study for Intel minifab (IE 4803 Intel Mini Fab Case Study - Model-Based Systems Engineering and the Intel MiniFab Case Leon, n.d.). They assumed that all five machines presented in the model require 30-minute preventive maintenance every 12 hours. They also ignored the stocker requirement (buffer capacity) in each cell during the modeling. (Shinde 2018) proposed modeling and simulation of a semiconductor manufacturing fab for cycle time analysis. The thesis analyzes the effects of scheduling policies and machine failures on the manufacturing cycle time of the IC manufacturing process for two processor chips, namely Skylake and Kabylake, manufactured by Intel. (Werling, Yugma, Soukhal, and Mohr 2020) proposed an agent-based simulation model with human resource integration for semiconductor manufacturing facility. All these studies focus on cycle time, WIP, and throughput rate. In comparison, this study uses a framework for energy quantification. Similar work is (Kannaian 2018), which proposed two methods to estimate electric energy consumption and carbon dioxide emission of a semiconductor wafer fab. They analyzed the impact of wafer starts per year and product mix, but they did not consider the cyber threat impact on manufacturing. (Bracho, Saygin, Wan, Lee, and Zarreh 2018) introduces a simulation model to assess the repercussions on manufacturing systems' performance in the presence of cyber threats, but they did not include the impact on energy quantification. This study contributes to the literature by integrating cyber-attack into semiconductor manufacturing simulation modeling to analyze the impact of cyber-attack on energy quantification.

The cybersecurity threats and vulnerabilities of the general manufacturing processes are analyzed through the literature. Those are mostly derived from emerging technologies. (Sobb, Turnbull, and Moustafa 2020) investigated the threats against 5G and wireless communication, cloud computing, IoT, cyber-physical systems, and blockchain technology. (Ervural and Ervural 2018) considered the security threats and vulnerabilities of IoT at the perception, network, service, and application layer. (Prinsloo, Sinha, and von Solms 2019) analyzed the types of cyber-physical attacks through the system. (Grover and Berghel 2011)] studied the system vulnerabilities and privacy issues for RFIDs. (Chen, Zhang, Li, Zhang, Deng, Ray, and Jin 2018) analyzed the IoT attacks based on application, middleware, network, and perception layer. (Hasanova, Baek, Shin, Cho, and Kim 2019) provided cybersecurity vulnerabilities of blockchain technology, including smart contracts. (Clark, Doran, and Andel 2017) investigated potential cyber threats and vulnerabilities for robotics applications at hardware, firmware, and application levels. (Rawat, Doku, and Garuba 2019) is also explored the security attacks in big data and how to develop secure solutions with big data analytics for traditional attacks. Table 1 summarizes the threat and vulnerabilities for the main technologies analyzed in the literature.

3 METHODOLOGY

3.1 Energy Quantification Model

Energy quantification term is used to describe the result of annual power consumption which is generated from the ARENA model using the model parameters: WIP(work in process), throughput rate, and cycle time. Production Efficiency Index (PEI) and Electrical Utilization Index (EUI) are both performance metrics to define the power consumption of a wafer fab. Production Efficiency Index (unit of kWh/cm2) is defined as a fab's total annual electricity consumption divided by its total wafer surface area produced as shown in Eq.(1). It represents the energy efficiency of a fab without including the wafer production's complexity, but the wafer area's physical scales are processed.

$$PEI = L/(TH * A) \tag{1}$$

Table 1: Cyber Security Threats and Vulnerabilities for technologies in digital SCM ((Ervural and Ervural 2018)(Chen, Zhang, Li, Zhang, Deng, Ray, and Jin 2018),(Sobb, Turnbull, and Moustafa 2020)(Prinsloo, Sinha, and von Solms 2019)(Yaacoub, Salman, Noura, Kaaniche, Chehab, and Malli 2020)(Rawat, Doku, and Garuba 2019),(Clark, Doran, and Andel 2017))

Technologies	*Cyber Security Threats and Vulnerabilities*
IoT(Layer Based)	
Perception Layer	Eavesdropping, Node Capture, Fake Node and Malicious, Replay and Timing Attack
Network Layer	DoS, MitM , Storage Attack, Exploit Attack , Data Breach
Application Layer	Sensitive Data Manipulation, Cross Site Scripting, Malicious Code, Phishing Attack
CPS	Eavesdropping
	Cross-Site Scripting
	SQL Injection
	Password Cracking
	Phishing, Replay, DoS
	Malware (Botnets, Trojan, Virus, Worm, Spyware, Etc.)
	Strike Surfaces
	Jamming Of Tracing Signals
	Zero-Day Attacks
	False Data Injection
Big Data Analytics	Unprocessed Information
	Confidentiality Breach
	Data Access Denial
	Data Storage
	Data Encryption
Robotics	Hardware: Backdoors, Trojans, Eavesdropping, Fault Injection, Hardware Modification
	Firmware: Dos, Execution Of Arbitrary Code, Root-Level Access to System, Malware
	Application: Viruses, Worms, Software Trojans, And Buffer Overflow

Electrical Utilization Index (unit of kWh/UOP) is defined as a fab's total annual electric power consumption divided by its annual UOP as shown in Eq.(2). EUI quantifies the energy efficiency of how a fab uses electric power consumption for wafer production, which considers the wafer process complexity

$$EUI = L/UOP \tag{2}$$

The units of production (UOP)(in pieces) of a fab are defined in Eq.(3)

$$UOP = TH * A * M \tag{3}$$

The number of mask layers is used to represent the complexity of production. The number of masks is directly proportional to the processes required to produce a wafer. Considering the throughput rate(TH), wafer surface area (A), and an average number of mask layers (M), Units of Production (UOP) give a good estimate of the total production capability of a wafer fab.

3.1.1 kWh-WIP Model for Energy Quantification

kWh-WIP model is used for energy quantification in semiconductor manufacturing:

$$UOP = \frac{WIP}{CT} * TH * A \tag{4}$$

$$L(kWh) = PEI * TH * A \tag{5}$$

The unit of production Eq.(4) is computed based on the wafer area and the number of mask layers in the process. Total energy consumption of the fab is calculated Eq.(5) with the selected optimal PEI value, the computed throughput TH, and wafer area. PEI value is given above as 1.312. This value comes from the reference paper considering the total number of fabs and processes. In this analysis, only PEI value is considered as a performance metric for wafer fab power consumption, EUI ignored. The equations are also based on Little's Law which describes the essential relationships among WIP, CT, and TH. According to littles law, the fundamental relationship between WIP is the multiplication of throughput rate and cycle time.

3.2 Cyber Risk Quantification

Cyber Risk Quantification defines cyber risk and evaluates risk impact parameters to decide the severity of the cyberattack on the system. Cyber risk is defined as the combined likelihood of an undesirable event and its impact level. The goal is to compute the cyber risk for IoT systems considering the IoT-specific factors and apply this method to IoT devices to determine their risk level(Kandasamy, Srinivas, Achuthan, and Rangan 2020). The risk for any given device d is computed in Eq.(6):

$$r(d) = w(d)s(d) \tag{6}$$

w(d) represents the potential risk impact due to vulnerabilities/attacks, and s(d) represents the likelihood of the risk(Kandasamy, Srinivas, Achuthan, and Rangan 2020). To calculate the risk impact, the parameters such as type of network, protocol type, number of heterogeneous systems devices security, and CIA (confidentiality, integrity, availability) type are taken into consideration. (Kandasamy, Srinivas, Achuthan, and Rangan 2020) provided risk impact parameters with weights as shown in Table 2.

Based on the above discussion, the risk impact w of device d can be derived as in Eq.(7).

$$w(d) = [nwt(d) + prt(d) + het(d) + des(d) + cia(d)]/5 \tag{7}$$

To calculate the likelihood of the risk, parameters and weights in Table 3 are considered. Based on the above discussion, the likelihood of risk can be derived as in Eq.(8).

$$s(d) = [pat(d) + lyr(d) + scr(d) + drf(d)]/4 \tag{8}$$

With a given risk score r(d), the risk will be a very high concern and a severe impact if the risk score range is between 81-100. The risk between 51-80 has a high concern, 21-50 moderate concern, 5-20 low concern, 0-4 no concern. Considering the risk score, the impact of specified cyber risk could be defined in ARENA simulation model.

Table 2: Risk Impact Parameters and Weights

S.no	*Risk impact parameter*	*Risk impact parameter type*	*Weight*
1	Type of network (nwt)	Unsecured network	10
		network with minimum security	5
		Completely secured network	2
2	protocol prone to attacks(prt)	Prone to more attacks	10
		Prone to fewer attacks	5
		No prone to attacks	2
3	count of heterogeneous systems involved(het)	More heterogeneous systems involved	10
		Few heterogeneous systems involved	5
		No heterogeneous systems involved	2
4	Device security(des)	Completely unsecured device	10
		Partially secured device	5
		Totally secured device	2
5	CIA type affected	CIA- all three are affected	10
		Only CI or AI or CA is affected	5
		Either C or I or A get affected	2

Table 3: Risk Likelihood Parameters and Weights

S.no	*Risk likelihood parameter*	*Risk likelihood parameter type*	*Weight*
1	Past attacks on the device (pat)	The device underwent lots of past attacks	10
		The device underwent few past attacks	5
		The device underwent no attack in the past	2
2	IoT layer with more attacks(lyr)	Network layer	10
		Application layer	5
		Physical layer (Perception)	2
3	Sector(scr)	Healthcare	8
		Financial	7
		Others	5
4	Device Risk factor	Network devices	8
		Application layer	8-10
		Perception(sensors)	4-6

4 EXPERIMENTAL ANALYSIS

This study provides an initial overview of our work on establishing and assessing performance metrics by exploring the modeling and simulation of semiconductor wafer fab manufacturing processes, with the goal of providing an energy quantification framework for semiconductor manufacturing in the presence of a cyber attack. In this study, semiconductor manufacturing processes are used as a case study. The detailed Intel minifab model (Kempf , Case 2021) is provided in Figure 1. There are three types of products that are processed as batches or lots through the same manufacturing steps. On average, 51 lots of pa, 30 lots of Pb, and 3 lots of TW(test wafer) for a total of 84 lots are processed weekly(roughly six lots/shift). There are six different steps where every product follows the same sequence. There are also three different cells for different processes.

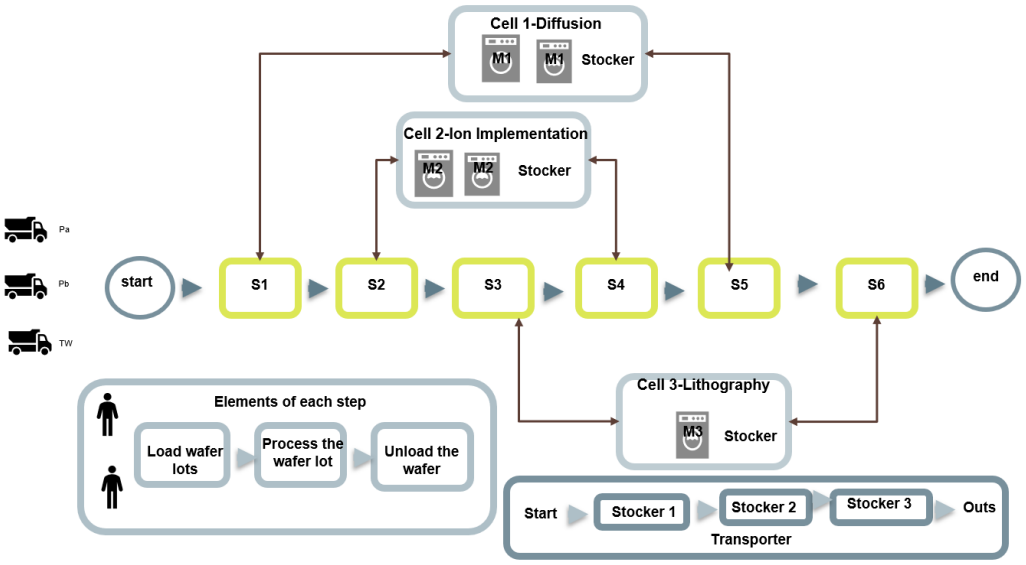

Figure 1: Intel minifab model

Each cell has a different number of identical machines. Cell 1 has two machines(M1), cell 2 has two machines(M2), and cell 3 has one machine(M3). There are three different elements in each step, loading, processing, and unloading of wafer lots. Step 1 and 5 is processed in cell 1, step 2 and 4 are processed in cell 2, and step 3 and 6 are processed in Cell 3. Loading time, processing time, and unloading time for each of the steps are provided in Table 4. The machines on this model have essential batching, failure/repair, and setup properties. In machine 1, when batching step S1, one can mix products. However, when batching step S5, one cannot mix products. Machine 2 requires no setup, and there is no batching. Machine 3 requires setup according to process number and product type. There are four different possibilities to assign the setup time but having different setup times is very challenging (given a project period). It is assumed that all setup times are equal to 10 min in the case study. Operators are available for loading, unloading, and setup. There are two production operators: production operator one(PO1) can service M1 and M2, while production operator two(PO2) can service M2 and M3. The machine in cell 2 requires both preventive and emergency maintenance. All machines in three different cells require 30-minute preventive maintenance every 12 hours (Kempf , Case 2021). The machine uptime follows the uniform function UNIF(24,84) hours, and machine downtime follows the UNIF(6,8) hours for emergency maintenance(Valente, Christiano Cecone, Alvim, and Cassiano 2015). Each cell also contains a stocker to store the production lots before and after processing in the machine. Stocker for cell 1 has a capacity of 18 lots. Cells 2 and 3 each have a stocker with a capacity of 12 lots.

Table 4: Loading, processing , unloading time for each step

Step	*Loading Time(min)*	*Processing Time(min)*	*Unloading Time(min)*
Step 1	20	225	40
Step 2	15	30	15
Step 3	10	55	10
Step 4	15	50	15
Step 5	20	255	40
Step 6	10	10	10

The machines on this model have essential batching, failure/repair, and setup properties. In machine 1, when batching step S1, one can mix products. However, when batching step S5, one cannot mix products. Machine 2 requires no setup, and there is no batching. Machine 3 requires setup according to process number (two cell processes: Step 3 and 6) and product type). There are four different possibilities to assign the setup time but having different setup times is very challenging(given a project period), so I assume that all setup times are equal to 10 min. Operators are available for loading, unloading, and setup. There are two production operators: production operator one(PO1) can service M1 and M2, while production operator two(PO2) can service M2 and M3. The machine in cell 2 requires both preventive and emergency maintenance. All machines in three different cells require 30-minute preventive maintenance every 12 hours.

This study just focuses on the cyber threats of IoT devices on semiconductor manufacturing for energy quantification. To do so, the first step is the modeling of cyberattack's impact on manufacturing. The workflow language YAWL (Yet Another Workflow Language) (Adams, Hense, and Ter 2020) is used for cyber part modeling. A workflow model describes three aspects of the business process: defining activities that build up the process, defining logic between activities, and defining relations between resources and activities. YAWL is an open-source Business Process Management System, which was firstly released in 2003. YAWL developed in the university research environment to become a unique system deployed worldwide as a laboratory environment for research in Business Process Management and as a productive system in other scientific domains. It offers comprehensive support for the vast majority of the identified control-flow, data, resource, and exception handling patterns. Thus YAWL is able to manage processes of practically any complexity. The modeling of cyber-attack impact is modeled using YAWL. Then, a discrete event system simulation software is used to analyze the performance of the wafer fab using the cycle time, throughput rate, and work-in-process level as output - which can lead to the quantification of energy in processes. ARENA Rockwell simulation software is used for the discrete event system simulation. To see the impact of cyber attack on energy quantification, the risk impact analysis is applied only on IoT devices in semiconductor manufacturing(only diffusion process) due to the complexity of the problem. This study assumed that higher cyber risk causes more detrimental effect and increase the risk of the system is being compromised.

The simulation model runs under three different circumstances to analyze the cyber risk impact on energy quantification: under normal conditions, partially compromised, and fully compromised. Semiconductor manufacturing is very complex as shown in the case study, so it is assumed only the diffusion process can be attacked. The cyber risk modeling is created using YAWL workflow modeling and provided in Figure 2.Some assumptions are made once the cyber attack has been arrived. It is assumed that if the risk is low or has no concern, the system can still work properly. If the cyber risk is medium, the system most likely be partially compromised. If the cyber risk is high, the system will be fully compromised. For example, DoS attack has a high risk score in the network layer. Therefore, we can assume that if the system(network) is attacked by DoS, the probability of being fully compromised will be higher. The determination of risk factors(low, medium, high) is decided after applying the cyber risk quantification framework. Once the system detects that it is not working properly, it will try to recover based on the actual condition. The recovery time will be longer if the system is fully compromised while it is trying to recover itself(Bracho, Saygin, Wan, Lee, and Zarreh 2018).

IoT in supply chains provides an interconnection between smart objects and information technology systems. They optimize the performance thanks to decision capability and collaborate all the supply chain processes((Abdel-Basset, Manogaran, and Mohamed 2018)). On the other hand, the interconnectivity via wireless networks makes the system vulnerable to cyber threats. We considered IoT architecture with three different layers: perception, network, and application layers. The perception layer is also known as the sensor layer since it collects information from sensors((Burhan, Rehman, Khan, and Kim 2018)). Network Layer is also known as the transmission layer since it transmits the collected information from the sensors to the perception layer, so this layer acts as a bridge between them. The transmission can be provided by the

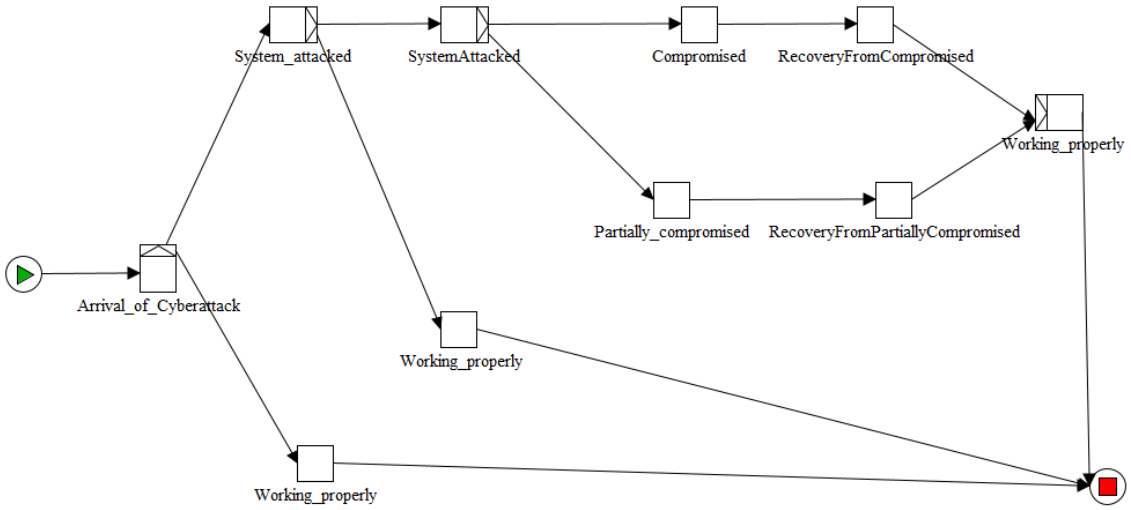

Figure 2: YAWL model for cyber-attack modeling

wired or wireless network such as Wi-Fi, Bluetooth, Zigbee, cellular network, etc. Application Layer provides services to the applications. The most common attack types in IoT devices for the perception layer are eavesdropping, node capture, fake node and malicious, replay attack, and timing attack. Denial of Service (DoS), Main-in-The-Middle (MitM), storage attack, exploit attack, and data breach are the common attack types for the network layer. Also, cross-site scripting, malicious code attack, and the ability to deal with mass data are the common attack types for the application layer(Park, Oh, and Lee 2019, Burhan, Rehman, Khan, and Kim 2018). According to the results of cyber risk quantification model, we can state that network layer cyber attacks cause the system will be fully compromised. Perception and application-layer attacks will cause the system to mostly be partially compromised.

Cyber risk quantification support that the risk impact of the network layer attacks is higher than the perception and application layer. We can assert that the network layer attack will require more time to recover from attack since they are very vulnerable to being fully compromised. We categorized each attack considering its risk factor and decided which attack required more recovery time from attack. It is provided the ARENA simulation model as an input. We consider that if the system is fully compromised, the recovery time will be 20 hrs(EXPO), and if the system is partially compromised, the recovery time from the attack will be 8 hrs(EXPO). The recovery times from partially/fully attacks are randomly selected. If the recovery times change, it has an impact on simulation output since it directly affects the waiting time of the system to recover from attacks. We analyze the impact of cyber attacks on energy quantification, adding a cyber-attack model with a mean time between attacks, and recovery time from attack to the existing simulation model. The outputs are units of production(in pieces) and total annual power consumption(KWh). The result is provided in Table 5.

Table 5: Simulation Results with and without the presence of cyber threat

	Unit of Production (in pieces)	*Total Annual Power Consumption(kWh)*
Normal Condition	8882.58	56675.45
Partially Compromised	8398.87	54419.23
Fully Compromised	8209.35	53985.35

As shown in Table 5, there is a decrease on production unit when the system is partially or fully compromised. However, the total annual power consumption for one piece unit of production is higher if the system is fully compromised. It is lower if the system is working under normal conditions. Given energy quantification and cyber risk analysis framework model, it could be stated that cyber attack affect the performance metrics which is used for energy quantification.

5 CONCLUSION AND FUTURE WORK

In the present effort, we addressed the establishment and assessment of performance metrics on energy quantification by exploring the model and simulation of semiconductor wafer fab manufacturing processes. Then, we extended our analysis by the presence of cyber attacks on the diffusion process in semiconductor manufacturing. The work brings a different perspective that combines cyber attack workflow modeling, risk assessment, and discrete-event simulation techniques to describe complex relations within an advanced manufacturing system. The study was part of our goal of establishing an energy quantification framework with the presence of cyber attacks for advanced manufacturing processes such as a semiconductor. Our initial insight was that the presence of a cyber attack in manufacturing causes delays in manufacturing processing times, accordingly impacting production performance and energy consumption. Our experiments support that compromising of the system has an important impact on the energy quantification model. In this study, some Intel minifab model details were ignored due to the short time frame available, so this model specification can be expanded with some of the process details for having the same case scenario with the real Intel minifab model in future works. Also, the cyber attack model only integrated into the diffusion process. This analysis could be expanded by adding cyber analysis framework for other processes. Having some optimization tools can also provide better performance metrics.

REFERENCES

Abdel-Basset, M., G. Manogaran, and M. Mohamed. 2018, September. "Internet of Things (IoT) and its Impact on Supply Chain: A Framework for Building Smart, Secure and Efficient Systems". *Future Generation Computer Systems* vol. 86, pp. 614–628.

Adams, M., A. Hense, and A. Ter. 2020, July. "YAWL: An Open Source Business Process Management System from Science for Science". *SoftwareX* vol. 12, pp. 100576.

Avila, A. J. B. 2017. *Assessing the Impact of Cyber-Threats on Smart Manufacturing Systems through a Simulation Study*. Ph. D. thesis, The University of Texas at San Antonio.

Bracho, A., C. Saygin, H. Wan, Y. Lee, and A. Zarreh. 2018, January. "A Simulation-based Platform for Assessing the Impact of Cyber-threats on Smart Manufacturing Systems". *Procedia Manufacturing* vol. 26, pp. 1116–1127.

Burhan, M., R. A. Rehman, B. Khan, and B.-S. Kim. 2018. "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey". *Sensors* vol. 18 (9), pp. 2796.

Intel Minifab Case 2021. "IE 4803 Intel Mini Fab Case Study - Model-Based Systems Engineering and the Intel MiniFab Case Leon".

Chen, K., S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin. 2018, June. "Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice". *Journal of Hardware and Systems Security* vol. 2.

Clark, G. W., M. V. Doran, and T. R. Andel. 2017, March. "Cybersecurity Issues in Robotics". In *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, pp. 1–5. Savannah, GA, USA, IEEE.

Ervural, B. C., and B. Ervural. 2018. "Overview of Cyber Security in the Industry 4.0 Era". In *Industry 4.0: Managing The Digital Transformation*, edited by A. Ustundag and E. Cevikcan, Springer Series in Advanced Manufacturing, pp. 267–284. Cham, Springer International Publishing.

Grover, A., and H. Berghel. 2011. "A Survey of RFID Deployment and Security Issues". *J. Inf. Process. Syst.*.

Hasanova, H., U.-j. Baek, M.-g. Shin, K. Cho, and M.-S. Kim. 2019, March. "A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures". *International Journal of Network Management* vol. 29 (2), pp. e2060.

Hu, S.-C., T. Lin, B.-R. Fu, C.-K. Chang, and I.-Y. Cheng. 2019, November. "Analysis of Energy Efficiency Improvement of High-tech Fabrication Plants". *International Journal of Low-Carbon Technologies* vol. 14 (4), pp. 508–515.

Kandasamy, K., S. Srinivas, K. Achuthan, and V. P. Rangan. 2020, May. "IoT Cyber Risk: A Holistic Analysis of Cyber Risk Assessment Frameworks, Risk Vectors, and Risk Ranking Process". *EURASIP Journal on Information Security* vol. 2020 (1), pp. 8.

Kannaian, Thulasi Krishna 2018. "Capacity Model with Sustainability Scope to Predict the Semiconductor Manufacturing's Energy Consumption and Carbon Dioxide Emissions".

Kempf, Karl. "Intel Five-Machine Six Step Mini-Fab Description".

Khan, S. 2021, January. "The Semiconductor Supply Chain: Assessing National Competitiveness". Technical report, Center for Security and Emerging Technology.

Lawrence Livermore National Laboratory 2020. "Dragonstone Strategy – State of Cybersecurity in the Oil & Natural Gas Sector".

Li, H., J. A. Ramírez-Hernández, E. Fernandez, C. R. McLean, and S. Leong. 2005. "A Framework for Standard Modular Simulation: Application to Semiconductor Wafer Fabrication". pp. 17.

Liu, J., C. Li, F. Yang, H. Wan, and R. Uzsoy. 2011, December. "Production Planning for Semiconductor Manufacturing via Simulation Optimization". In *Proceedings of the 2011 Winter Simulation Conference (WSC)*, pp. 3612–3622. ISSN: 1558-4305.

Morrice, D., R. Valdez, J. P. Chida, and M. Eido. 2005. "Discrete Event Simulation in Supply Chain Planning and Inventory Control at Freescale Semiconductor Inc". *Proceedings of the Winter Simulation Conference, 2005.*.

Park, M., H. Oh, and K. Lee. 2019. "Security Risk Measurement for Information Leakage in IoT-based Smart Homes from a Situational Awareness Perspective". *Sensors* vol. 19 (9), pp. 2148.

Platzer, M. D., J. F. S. Jr, and K. M. Sutter. 2020. "Semiconductors: U.S. Industry, Global Competition, and Federal Policy". *Global Competition*, pp. 58.

Prinsloo, J., S. Sinha, and B. von Solms. 2019, January. "A Review of Industry 4.0 Manufacturing Process Security Risks". *Applied Sciences* vol. 9 (23), pp. 5105. Number: 23 Publisher: Multidisciplinary Digital Publishing Institute.

Rawat, D. B., R. Doku, and M. Garuba. 2019. "Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security". *IEEE Transactions on Services Computing*, pp. 1–1. Conference Name: IEEE Transactions on Services Computing.

Rose, O. 2000, December. "General Simulation Applications in Semiconductor Manufacturing: Why do simple wafer fab models fail in certain scenarios?". In *Proceedings of the 32nd conference on Winter simulation*, WSC '00, pp. 1481–1490. San Diego, CA, USA, Society for Computer Simulation International.

Shinde, A. 2018. "Modeling and Simulation of Semiconductor Manufacturing Fab for Cycle Time Analysis". pp. 103.

Sobb, T., B. Turnbull, and N. Moustafa. 2020, November. "Supply Chain 4.0: A Survey of Cyber Security Challenges, Solutions and Future Directions". *Electronics* vol. 9 (11), pp. 1864. Number: 11 Publisher: Multidisciplinary Digital Publishing Institute.

Valente, S., E. Christiano Cecone, L. Alvim, and D. Cassiano. 2015, August. "Optimization of a Semiconductor Manufacturing Process Using a Reentrant Model". *Exacta* vol. 13.

Werling, J., C. Yugma, A. Soukhal, and T. Mohr. 2020, December. "An Agent-Based Simulation Model with Human Resource Integration for Semiconductor Manufacturing Facility". In *2020 Winter Simulation Conference (WSC)*, pp. 1801–1812. Orlando, FL, USA, IEEE.

Yaacoub, J.-P. A., O. Salman, H. N. Noura, N. Kaaniche, A. Chehab, and M. Malli. 2020, September. "Cyber-physical Systems Security: Limitations, Issues and Future Trends". *Microprocessors and Microsystems* vol. 77, pp. 103201.

AUTHOR BIOGRAPHIES

BUSRA EZICI is a Ph.D student at the systems engineering and operations research department at George Mason University. She received M.Sc. degree in industrial engineering department from Istanbul University, the B.Sc. degree in industrial engineering department from Gaziantep University in Turkey. Her research interests include secure supply chain management, cyber security applications in smart manufacturing, energy-saving techniques, digitalization with Industry 4.0, risk management, and evaluation and simulation techniques. Her email is bozoglu@gmu.edu.

PAULO COSTA is an Associate Professor at the systems engineering and operations research department, Associated Chair of the cyber security engineering department, and Director of the C4I & Cyber Center at George Mason University. He received his Ph.D. degree in information technology and his M.Sc. degree in systems engineering from George Mason University, and his B.Sc. degree in aeronautical engineering from the Brazilian Air Force Academy. His research interests include multi-sensor information fusion, probabilistic reasoning, and security of cyber physical systems with applications in advanced manufacturing, transportation, and supply chain systems. His email is pcosta@gmu.edu.

JIE XU is an Associate Professor at the systems engineering and operations research department at George Mason University. He received the Ph.D. degree in industrial engineering and management sciences from Northwestern University, the M.S. degree in computer science from The State University of New York, Buffalo, the M.E. degree in electrical engineering from Shanghai Jiaotong University, and the B.S. degree in electrical engineering from Nanjing University. His research interests are data analytics, stochastic simulation and optimization, with applications in cloud computing, healthcare, manufacturing, power systems, and supply chain. His email is jxu13@gmu.edu.