Proceedings of the 2021 Winter Simulation Conference
S. Kim, B. Feng, K. Smith, S. Masoud, Z. Zheng, C. Szabo and M. Loper, eds.

DIGITAL TWIN BASED CYBER-ATTACK DETECTION FOR MANUFACTURING SYSTEMS

Chandrasekhar Sivasubramanian
Giulia Pedrielli
Georgios Fainekos

School of Computing, Informatics, and Decision Systems Engineering
Arizona State University- Tempe
699 S Mill Ave
Tempe, AZ 85281, USA

Petar Jevtic

School of Mathematical and Statistical Sciences
Arizona State University
900 S Palm Walk,
Tempe, AZ 85281, USA

Mani Janakiram

Intel Corporation
5000 W Chandler Blvd
Chandler, AZ 85226, USA

ABSTRACT

Breakthrough paradigms and technologies are up and coming across several sectors in manufacturing and semiconductor, as high-tech manufacturing is witnessing unprecedented opportunities. In fact, next generation fabs are Cyber-Physical Systems (CPS) which integrate the physical and the information layer using networks, sensors and data processing. In these connected systems, there are several interactions between the equipment and the information layer (Cloud storage). With unprecedented opportunities came unprecedented challenges. In this work, we focus on cyber-attacks in semiconductor smart manufacturing. While cyber-attacks have been formulated and analyzed for several critical infrastructures (power, water, gas, etc.) the development in the manufacturing sector in general and semiconductor in particular, are still nascent. In this paper, we formulize new attack categories, provide ways to deploy them and alternative ways to detect them. A preliminary empirical analysis is provided for a lithography system.

1 MOTIVATION AND PROPOSED WORK

Lithography is a vital process in semiconductor manufacturing and the associated equipment is highly expensive. The risk of cyber-attacks on the CPS of such a process, always attracts increased attention. Wu et al. (2020) proposes a zero-day attack on an additive manufacturing 3D printing process, while Cárdenas et al. (2011) implements data integrity attacks on the control system of a chemical process. Inspired by the CPS literature, in this work, our contribution is to propose a new family of data integrity attacks.

In our study, we focus on the Spin coating process. In order to implement a data integrity attack, we look into the relationship between the initial and final thickness of the product and assume the attacker is able to break in the sensing system of the coater to modify the initial thickness. In fact, a spin coater is responsible to set the angular velocity (ω) and the spin time (τ_s) in order to obtain a target thickness (h_f^*), given an initial thickness (h_0). In this work, we consider the simple relationship between those variables, namely (Lee et al. 2019): $h_f^* = h_0/\left(\sqrt{1+(4\rho W^2 h_0^2 \tau_s)/(3\mu)}\right)$, where h_f^* is the target thickness in micrometers [μm], h_0 the initial thickness of the part when it enters coating [μm], ρ is the density of the photoresist material (Kg/m^3), $W = \pi/30 \cdot \omega$, where ω is the angular velocity (RPM), τ_s is the spin time in seconds, and μ is the dynamic viscosity [cP]. However, the process is affected by noise.

2 PRELIMINARY ANALYSIS

We modeled the initial thickness as $H_0 \sim \mathrm{Tri}\left(h_0, h_0^u, h_0^\ell\right)$, $h_0 = 1050[\mu\mathrm{m}]$, $h_0^\ell = 1050 - 25\ [\mu\mathrm{m}]$ and $h_0^u = 1050 + 25\ [\mu\mathrm{m}]$. While the true h_0 is unknown, the attacker modifies the realization from H_0 with Δh_0. With desired thickness, $h_f^* = 60[\mu m]$, the spin speed Ω is calculated from the h_f^* relationship (returning ϖ), and, adding a noise term, we have $\Omega \sim \mathrm{Tri}(\varpi, \varpi \pm 41)$[rpm]. The actual thickness H_f is calculated using the h_f^* relationship (returning $\overline{H_f}$) and, adding noise $H_f \sim \mathrm{Tri}\left(\overline{H_f}, \overline{H_f} \pm 3\right)$[μm].

- Test I: effect of deviation on H_f. Figure 1 shows the results from several values of $\Delta H_0/h_0$. We can see that the relative change in the final thickness is always within 10% and especially for negative variations the plots tend to overlap making identification harder (the central plot refers to nominal in Figure 1).
- Test II: effect of deviation on the machine parameters (spin). In the second test, we perform a simulation where the $\Delta H_0/h_0$ is changed similar to the previous, but we observe the confidence regions exhibit less overlapping thus proving a potential for being used for attack identification. A sensor attack can be easily differentiated from a wrong sensor calibration since the issue of calibration produces a bias in the output.

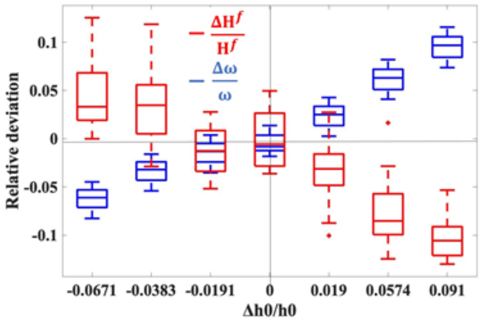

Figure 1: Box plot from 15 independent replications of relative deviation in final thickness and relative deviation in spin speed vs. relative change in initial thickness.

3 CONCLUSIONS AND FUTURE WORK

In this work, we propose for the first time the implementation of a data integrity attack to a smart manufacturing system focusing on the lithography process. We assume to be able to manipulate the reading of the initial thickness of the process, thus impacting the output control. We show the potential impact of the attack as well as the difficulty in detection through the sole output monitoring. We also show the potential of processing parameters in detection. Current and future work focus on widening the class categories and designing realistic test cases with the collaboration of our industry partner. We would also be relating the impact of an attack to a cost function in our future work.

REFERENCES

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*, March 22nd-24th, New York, USA, 355-366.

Lee, U. G., W.-B. Kim, D. H. Han, and H. S. Chung. 2019. “A Modified Equation for Thickness of the Film Fabricated by Spin Coating”. *Symmetry* 11(9): 1183.

Wu, M. and Y. B. Moon. 2020. “Alert Correlation for Detecting Cyber-Manufacturing Attacks and Intrusions”. *Journal of Computing and Information Science in Engineering* 20(1): 011004.