Security Challenges and Requirements for Control Systems in the Semiconductor Manufacturing Sector

Malek Ben Salem
CyberSecurity Lab
Accenture Technology Labs
Reston, Virginia 20190
Email: malek.ben.salem@accenture.com

(Extended Abstract)

I. Introduction

Moore's Law and the market requirements for higher performance chips are driving the production of increasingly smaller transistors, and therefore, are forcing more stringent controls on semiconductor manufacturing processes and equipment, with a very small room for error.

The second trend in the semiconductor industry is the adoption of the e-Manufacturing paradigm [1]. With the rise of fully-automated factories and the new technology size requirements for chips, new security challenges arise as the control systems are becoming increasingly more complicated. The need for high manufacturing yields using these systems is driving more Advanced Process Controls (APC). Control systems, already ubiquitous in the industry, are becoming more and more sophisticated. And complexity, as is widely acknowledged, is the enemy of security.

The last trend in the industry is the tendency for manufacturers to form joint production ventures. The highly cyclic demand for various consumer electronic products is causing cyclical fluctuation in the manufacturing load of semiconductor factories. The high costs of development and production facilities for different technology node sizes is driving semiconductor companies to form join manufacturing partnerships instead of building new factories. Production of parts may be distributed among manufacturing partner facilities if the manufacturing load in one factory is too high, and part delivery deadlines cannot be met. This new manufacturing model is known the Manufacturing Grid. The goal is to utilize all the manufacturing resources that are distributed between different manufacturing partners and factories different chip parts.

This paper presents threats to controls systems in the semiconductor manufacturing sector that are driven by the above trends in Section II. In Section III, we review recent research work related to the most important threat faced by these control systems. Section IV presents the research priorities and security requirements needed to mitigate these threats. Finally, Section V concludes the paper by summarizing its main points.

II. Threats and Security Challenges to Control Systems in the Semiconductor Manufacturing Sector

We distinguish between targeted attacks to control systems such as Stuxnet [2], and non-targeted attacks. We also distinguish between two types of threats: threats to equipment sensors and controllers, and threats to the IT systems and networks that support these sensors and controllers. For completeness, we cover the major threats of both types in this Section.

A. Equipment Control and Recipe Integrity

Recipes are specifications of equipment processing used to control manufacturing equipment, including processing tool chamber temperature, pressure, and cooling/heating rates. A critical security (and potentially safety) challenge is trusted recipe content, which guarantees that the recipe on the equipment is exactly the one that the factory approved and selected. Another challenge is the traceability of recipe items and parameter usage. A third challenge is preventing DoS attacks, where the adversary prevents the tool controller from receiving recipe parameters and values or sensor measurements by blocking the communication channels between them.

B. Process Data Integrity

The industry applies feed-forward and feedback control, as well as automated fault detection to equipment and to the automated factory, in order to improve process performance and factory yield. These techniques, known as APC rely on the integrity of the data measured by equipment sensors.

Accurate alarm reporting also relies on the accuracy of sensor readings. Alarm reporting is critical to the safety of the equipment, the product, and the factory in general. Alarm reports must be accurate and timely.

One type of targeted attacks against the sensors is the *False Data Injection Attack* where a malicious third party compromises the integrity of the control systems by controlling the readings of one or more sensors, such as the sensors measuring the ambient temperature inside a chamber on an ion implantation tool.

C. Privilege Over-Entitlement

With the establishment of the Manufacturing Grid, distributed teams are being formed from different companies to collaborate on the development and production of various products. This along with the high job rotation rates among

process engineers through various product wafer processing steps, is increasingly complicating the access controls management process. Many engineers quickly accumulate privileges that they do not need to perform their current job functions.

Although this security problem is not strictly related to cyber-physical devices, highly-privileged access to equipment sensors and controllers is a serious threat, knowing that the control systems are increasingly becoming remotely accessible and linked to the corporate networks or to other factories through the Manufacturing Grid. The threat is exacerbated by the open specifications used for process equipment design. This make it easy for malicious users, potentially from a business/manufacturing partner, to launch their attacks and compromise equipment sensors or controllers.

D. Sample Attack

An attacker may develop Stuxnet-like malware [2], featuring zero-day exploits, rootkits, anti-virus evasion techniques, and process injection and hooking code, to target a specific process step within the entire chip manufacturing process.

One of the critical steps in chip manufacturing is the lithography step, where lithography masks or reticles are used to print the pattern of transistors and wires on a microchip. An attacker may substitute a mask with another and use it to print additional transistors and wires on a microchip. Printing as few as a 1000 additional transistors (to the millions of transistors on a chip) may introduce a kill switch or a backdoor to the chip [3]. A kill switch on a chip allows the attacker to stop the chip at any time when he or she sends a specific sequence of bits. All chips on wafers processed using this tool will carry the backdoor or kill switch. The damage may be catastrophic if the chip is installed on a plane for instance. A backdoor may allow the attacker to disable any cryptographic functions that the chip may be running for example. Hardware backdoors create a significant security vulnerability, since hardware is the root of trust, which software builds on.

This is an example of a targeted and very sophisticated attack enabled by the next-generation factory model, where all manufacturing operations are automated and controllers are reachable remotely. The attacker may be able to compromise the controllers of the equipment and have the lithography process tool load the wrong mask. He or she may also compromise the sensors of the tool and/or the software running on the tool so that the wrong process data is reported, thus preventing the detection of the attack through log analysis. The resulting "compromised" chips are hard to detect even during the chip testing phase. Chip makers are not able to test every unspecified function of the device in order to find potential backdoors [3], nor are they able to test all possible sequences of data that might trigger, and therefore discover, a kill switch during testing.

III. Related Research

One of the major attacks against control systems, including process tools used for chip manufacturing, is the *False Data Injection Attack*. Process tools in this sector are perhaps more vulnerable to these attacks, due to the highly stringent process requirements that have to be met as transistors and technology nodes get smaller. Any false data injected into the control data may drive the process tool "out of control" or irreversibly damage the product.

Mo and Sinopoli studied this type of attack targeting control systems in general. They defined the required and sufficient conditions under which an adversary is able to destabilize a control system that is used to monitor a Linear Time Invariant (LTI) Gaussian system. Linear dynamical systems are one of the most common models for physical systems. The researchers assumed that the control system is equipped with a Kalman filter used to estimate the state of the system from different sensor observations, a LGQ controller used to stabilize the system, and a failure detector [4]. They formulated the action of the attacker as a constrained control problem and showed that, if the attacker knew the variables of the controlled systems and controlled a subset of the sensors, then the attack is feasible. As a defense mechanism, they proposed adding redundant sensors to measure all unstable modes in order to improve the resilience of the control system.

Cárdenas *et al.* reviewed different types of false data injection attacks against control systems, such as bias attacks, surge attacks, and geometric attacks. They experimentally tested these types of attacks against a chemical reactor process. They concluded that it was more important to protect against integrity attacks than DoS attacks. They also found that the proposed data injection attacks could be detected thanks to the slow dynamics of the process. This, probably, does not hold true for semiconductor manufacturing processes.

IV. Research Priorities and Security Requirements

As we have pointed out, some of the threats targeting control systems are CPS-specific, while others apply to all IT systems. Below, we highlight the security research priorities for control system security in the semiconductor manufacturing sector.

A. Detecting False Data Injection Attacks and Sensor Compromise

The adversary can launch these attacks by obtaining the secret key or by compromising some sensors or controllers. Preventing or at least detecting these attacks is critical. Collecting accurate data is one of the most important conditions for the secure manufacturing of chips. Engineers rely on quality data to make critical decisions related to the availability of manufacturing tools, to the integrity of the specifications of the the manufactured product, and to the reliability and repeatability of the manufacturing process [5].

As the industry embraces the e-Manufacturing model, data integrity becomes even more critical. This requires the protection of the sensor readings and sensor software, eliminating message and data latency and ensuring accurate timestamps. For example, at the equipment controller level, it is important to have accurate readings of the process speed and cooling response rates, the process chamber status, as well as calibration data, and sensor settings. Similarly accurate process data are

critical to equipment setup, qualification, process control, and process monitoring.

Data must also be made available in a timely manner to support process control. False data may be an incorrect measurement, an incorrect sender id, or an incorrect timestamp sent with the measurement. Semiconductor processing has stringent timing controls. Distributed factory environments also rely on accurate time in order to coordinate manufacturing processes. So, the time synchronization system used should be fault-tolerant using diverse time sources, so that if one source fails or is inaccessible, others may be reached.

B. Trusted Recipe Management and Fine-Grained Access Control Management

Trusted recipe are a critical security requirement [6]. The management of equipment configuration is of vital importance because configuration changes can cause differences in process capability and outcomes. Trusted recipe management is not a research priority, as much as a security requirement. Security measures that can be used to enforce trusted recipe management are available but cannot easily implemented. Existing access control mechanisms, as previously underlined, do not easily meet the requirements of the industry. New fine-grained access control models to equipment and product recipes are needed in order to help reduce the privilege over-entitlement problem, while allowing design, process, equipment, industrial and integration engineers to solve problems together, especially in cases of manufacturing line emergencies.

C. Dynamic Patching

Control systems are not typically suitable for frequent software patching and updates due to their high availability requirements. Software patches and updates are usually deployed on a fixed, calendar-based schedule, although there is a call to move to condition-based and predictive preventive maintenance [7]. While this may not be the top research priority, we believe that there needs to be more work on dynamic patching for software running on control systems with high uptime requirements.

V. Conclusion

In this extended abstract, we gave an overview of the security challenges driven by three trends in the semiconductor manufacturing sector: e-Manufacturing, Moore's Law, and the Manufacturing Grid. We briefly reviewed recent research related to one of the most serious attacks against control systems used by chip makers, namely false data injection attacks. Then, we highlighted the security-related research priorities for the industry.

Control systems are subject to non-targeted attacks and targeted attacks, such as Stuxnet [2]. Attacks against control systems may be directed at the sensors of the control systems, their actuators or controllers, or the IT systems and networks supporting the information processing and communication. Techniques for detecting tampering, and validating the inputs provided by the sensors are of paramount importance.

Besides their unique security requirements, control systems share many of the security requirements with traditional IT systems. However, if we are to achieve secure control systems in this sector, we need to model the security implications of the physical interactions in semiconductor processing tools. Design of the equipment, including hardware components and the software that it runs, as well as the factory automation platform, should consider security as part of system architecture and software development. Information flow and control paths have to be identified during the design phase, so that the operational security requirements of the system may be met..

References

[1] T. Walker and D. Stark, "Next-generation factory publications by the semiconductor manufacturing consortium (sematech)." [Online]. Available: http://sematech.org/docubase/wrappers/33s.htm

[2] N. Falliere, L. O. Murch, and E. Chien, "W32.stuxnet dossier version 1.4," New York, NY, USA, February 2011.

[3] S. Adee, "The hunt for the kill switch," *Spectrum, IEEE*, vol. 45, no. 5, pp. 34 –39, may 2008.

[4] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Proceedings of the First Workshop on Secure Control Systems*, ser. SCS '10. Team for Research in Ubiquitous Secure Technology (TRUST), April 2010. [Online]. Available: http://www.cse.psu.edu/ smclaugh/cse598e-f11/papers/mo.pdf

[5] G. Crispieri, "Data quality guidelines: Version 1," July 2008. [Online]. Available: http://sematech.org/docubase/document/4843ceng.pdf

[6] L. Rist, "Recipe management system: Common requirements and benchmark 2007," May 2008. [Online]. Available: http://sematech.org/docubase/document/4930atr.pdf

[7] T. Walker and D. Stark, "Ismi predictive preventive maintenance implementation guideline," October 2010. [Online]. Available: http://sematech.org/docubase/document/5119atr.pdf

Malek Ben Salem, PhD, CISSP Dr. Ben Salem has an extensive background in process controls. She has worked for 9 years as an IT systems developer and integrator and as a Controls engineer at IBM's East Fishkill chip manufacturing factory. Dr. Ben Salem earned a PhD degree in Computer Science from Columbia University in 2012. Her research interests include intrusion detection, network security, and secure dependable systems.