An Empirical Evaluation of CNC Machines in Industry 4.0 (short paper)

Marco Balduzzi[1], Francesco Sortino[2], Fabio Castello[2], and Leandro Pierguidi[2]

[1] Trend Micro Inc.
[2] Celada SpA.

Abstract. CNC machines are largely used in production plants and constitute a critical asset for organizations globally. The strong push dictated by the Industry 4.0 paradigm led to the introduction of technologies for the wide connectivity of industrial equipment. As a result, modern CNCs resemble more to fully fledged systems rather than mechanical machines, offering numerous networking services for smart connectivity. This work explores the risks associated with the strong technological development observed in the domain of CNC machines. We performed an empirical evaluation of four representative controller manufacturers, by analyzing the technologies introduced to satisfy the needs of the Industry 4.0 paradigm, and conducting a series of practical attacks against real-world CNC installations. Our findings revealed that malicious users could abuse of such technologies to conduct attacks like denial-of-service, damage, hijacking or data theft. We reported our findings to the affected controller vendors and proposed mitigation. This work wants to be an opportunity to raise awareness in a domain in which, unfortunately, security doesn't seem to be, yet, an important driver.

1 Introduction

The last decade has seen a surge in popularity in the adoption of network-enabled systems, including devices that historically were not offering such capabilities for several reasons. In the industrial world, for example, several kinds of such systems are largely used nowadays to support the manufacturing process in a smart, modern paradigm. The evolution observed on devices such as programmable logical controllers (PLCs), computer numerical controls (CNCs), industrial robots, automated guided vehicles (AGVs) applied to logistics etc.., heads to models of interconnection, according to the general paradigm of the Industry 4.0, and is pushing manufacturing companies toward networked shop floors.

Although the need of connecting such modern machinery to wide networks, including the Internet, represents an important opportunity to create new business intelligence, for example to the collection and analysis of production data, it also opens the doors to potential threats impacting on security and privacy of organizations worldwide. This is further emphasized by reasons like: first, the heterogeneity of the technologies used in the industrial domain, with few standards available and far from being widely adopted yet; second, the lack of

awareness in the domain, for example in adopting security best practices in the development or use of the machines; third, the lack of prior art showing in practice how such machines could be attacked; last, but not least, the strong push dictated by the market to rapidly reposition legacy machinery in form of modern, smart solutions.

Given these considerations, some previous research (even though very limited) looked into the risks connected with the introduction of the Industry 4.0. Quarta et al. [3] conducted a security analysis of an industrial robot. Maggi et al. [2] reported several practical issues related to smart manufacturing systems in general. Balduzzi et al. [1] looked at industrial gateways, i.e. gateways considered as IIoT equipment used in smart factories for enabling the communication between modern and legacy devices.

While these studied technologies are related to smart manufacturing, none of them deal with computer numerical controls. In this respect, we believe being the first to tackle this topic from a security standpoint. Modern CNCs consist of sophisticated machines that can be programmed with domain-specific languages and configured to operate autonomously in a fully-remote fashion, for example with networking frameworks and libraries made available by the vendors. The same machines can be extended in features by installing add-ons that act as software extensions, similarly to the mobile apps available on the app stores for download. These, and other domain-specific functionalities, make modern CNCs closer to fully fledged systems like an IT server rather than hardware-centric machines as it was to be. In fact, although under the hood they are still operating well-established automation routines, for example used to engrave raw material, they are ran by operating systems together with several layers of complicated software and technologies.

As security researchers, and given the complexity of this technological ecosystem, we believe there are wide possibilities for security abuses. For this reason, we conducted an assessment of the domain of CNC machines, by investigating CNCs offered by four representative vendors, in particular by focusing on the technological aspects needed to make such machines easy to be connected and operated remotely in a smart manufacturing environment.

The contributions of our work consist of: 1. We investigate the domain of CNC machines in term of security and privacy. To the best of our knowledge, we are the first to conduct a depth empirical analysis in this direction. 2. We identify four vendors as representative of this domain and conduct practical assessments on the technologies offered by their controllers. 3. We report security problems related to the abuse of such technologies that can result in attacks like denial-of-service, leak of sensitive information, hijack of the production, introduction of micro-defects, damage of machines and pieces, and safety. 4. We communicate our findings to the affected vendors in a responsible way, and do our best to raise awareness in this domain.

2 Evaluation

Our investigation began by identifying representative controller manufacturers, in particular manufacturers that: 1. are geographically distributed (i.e., with headquarters and subsidiaries spread across the world) and that resell on a global scale; 2. are on the market since decades already; 3. have a large estimated side, for example with a total a revenue topping a billion dollar; 4; use technologies widely adopted in the domain, and are present in different manufacturing sectors. In addition, we made sure that the manufacturers we identified offered controllers that we could use for our evaluation, i.e. either in form of simulators (i.e. a controller attached on simulated peripherals) or real machines.

(a) Example of simulator used for preliminary testing

(b) Example of machine used for final testing

Table 1 provides a summary of the selected manufacturers together with the relative controllers we used in our research. For one vendor (Fanuc) we made use of two machines. Figure 1a provides an example of simulator we used in preliminary analysis of the controller, while Figure 1b shows a machine employed for the final testing.

For all vendors, we conducted an equal evaluation of their machines – that we summarize in:

– We first identified the technologies adopted by the vendors to be "Industry 4.0 ready". This set of technologies consists of the interfaces (and related protocols) used to interconnect the machines so to serve in smart environments. These interfaces allow the machine to transmit outbound information to centralized systems such as production data for better management and

Vendor	**Haas**	**Okuma**	**Heidenhain**	**Fanuc**
Country	USA	Japan	Germany	Japan
Establishment	1983	1898	1889	1972
Estimated size	>$1B and 1,300 employees (2018)	$1.41B and 3,812 employees (2020)	$1.3B and 8,600 employees (2020)	$4.18B and 8,260 employees (2020)
Market	Controllers and machines	Controllers and machines	Controllers	Controllers and simple machines
Simulator	100.19.100.1123	OSP-P300S	TNC 640 v. 10.00.04	Not used
Controller	100.20.000.1110	P300MA-H	TNC 640	31iB5 iHMI and 32i-B
Machine	Super Mini Mill	GENOS M460V-5AX	HARTFORD 5A-65E	YASDA YMC 430+RT10 and STAR SR 32JII
Type	3-axis vertical machining center	5-axis vertical machining center	5-axis vertical machining center	5-axis vertical micro machining center and Swiss lathe

Table 1: Summary of the selected controller manufacturers and related CNC machines used in the research.

Vendor	**Default Technologies**	**Optional Technologies**
Haas	MTConnect, Ethernet Q Commands	NaN
Okuma	NaN	THINC-API , MTConnect
Heidenhain	RPC and LSV2 (DNC)	OPC-UA
Fanuc	FOCAS	OPC-UA , MTConnect

Table 2: Summary of the Industry 4.0 technologies adopted by the vendors.

cost reduction. They also enable remote management, for example for an operator to change the executed program or the configuration of the tooling in an easy way. A summary is provided in Table 2.

– We conducted a security assessment in a black-box fashion, which consisted of using automated vulnerability scanners like Nessus to identify potential known vulnerabilities or misconfigurations in the exposed services. Note that since the goal of our research is on domain specific technologies, we ignored all problems related to generic software like Windows services and moved forward looking for abuses in CNC interfaces.
– In this respect, we then went deep into the CNC-specific technologies previously identified, by analyzing the risks of abuses and conducting practical attacks on the controllers. For this, we developed attacking tools that leverage the weaknesses we identified in the domain specific interfaces with the help of proprietary APIs we got access to.
– We collected evidence of our concerns and collaborated with the vendors suggesting mitigation. All evidence has been conducted on real world instal-

lations, but we also used the simulators for preliminary testing or when the machines were not available in the immediate.

We now give a short introduction on the domain specific technologies that we identified and discuss the related macro problems.

MTConnect is an effort to standardize the different protocols used in the industrial domain to collect machinery data like telemetry on production. The goal is indeed to provide guidelines for converting old and proprietary information to a common language. This will help organizations to handle machinery from different brands in an easier form. Along with our evaluation, we confirmed that 3 of the tested vendors support MTConnect, in particular Haas provides such feature on all default installations. In our analysis, we investigated the data that an attacker could reconstruct (or leak) from a machine exposing MTConnect over its network interface. A common scenario is, for example, the number of pieces that are produced, together with the associated program's name. In other cases, an attacker could infer the source code as well, making the attack very severe.

Proprietary protocols seem to be widely used in the CNC domain, in which manufacturers develop their own technologies for enabling their controllers to network. Some example of such protocols are Haas's Ethernet Q Commands, Heidenhain's RPC (also known as DNC / Option 18), or Fanuc's FOCAS. Unfortunately, our analysis reported major issues with these implementations: 1. authentication is rarely available, or not offered as default feature, which makes a malicious user able to log into the networking service and abuse it, 2. encryption is not adopted and data confidentiality is not guaranteed. Another important issue is the lack of authorization, making a malicious user able to tamper with privileged resources.

Okuma stands out from the market of the CNC controllers for one interesting feature: the modularity of the controller. In fact, while this vendor seems offering a controller with limited features, it instead provides a mechanism (called THINC-API) to highly customize a machine's functionalities. With this technology, any developer can implement a program that – once installed – runs in the context of the controller, in the form of add-on. From our analysis, it turned out that very simple security mechanisms that are nowadays very common on other platforms like mobile applications, for example resource control access, are not yet supported. As a result, if a miscreant manages to install a malicious application, she will be able to access all information stored internally in the controller, and – worse than that – to maliciously tamper with the behavior of the controller. The malicious application we developed for testing mimics a malware reaching out the attacker and waiting for commands to be prompted to the backdoored CNC.

Attack Class	Attack Name	Haas	Okuma	Heidenhain	Fanuc	Total
Compromise	RCE	y	y	y		3
Damage	Disable feed hold	y				1
	Disable single step	y		y		2
	Increase the tool life	y	y	y		3
	Increase the tool load	y	y		y	3
	Change of tool geometry	y	y	y	y	4
	Decrease the tool life	y	y	y		3
DoS	Decrease the tool load	y	y		y	3
	Change of tool geometry	y	y	y	y	4
	DoS via parametric program	y	y	y	y	4
	Trigger custom alarms	y		y		2
	Ransomware	y	y	y		3
Hijacking	Change of tool geometry	y	y	y	y	4
	Hijack of parametric program	y	y	y	y	4
	Program rewrite		y	y	y	3
Theft	Leakage of production information	y	y	y	y	4
	Leakage of program code		y	y	y	3
	Screenshot			y		1
	Total	15	14	15	10	

Table 3: Summary of the attacks identified in our research.

3 Findings

Overall, as depicted in Table 3, our evaluation identified 18 attacks (or attack variations[3]) that we grouped in 5 attack classes namely compromise, damage, denial-of-service, program hijacking, and theft.

Among the different controllers that we tested, we observed a consistency on the number of problems: Haas, Okuma and Heidenhain reported a similar amount of issues (15), with Fanuc confirming 10 attacks. This is a symptom that security doesn't seem to be yet a priority for controller manufacturers with our research showing that this domain lacks of awareness with respect to privacy and security. This, together with the possibility that CNC machines can be misconfigured or exposed to corporate networks (or to the Internet) creates serious and compelling problems.

When looking at the same table on a line basis, the scenario doesn't look better. Among all attacks, only two are confirmed to apply to a single vendor only (i.e., disable feed hold and screenshot). Vice versa, 6 attacks are confirmed on all

[3] Some attacks are reported multiple times because consisting of attack variations. For example, a malicious user can modify the geometry of a tool to achieve damage, hijacking, or denial-of-service – depending on the type of machine and manufacturing process. Vice versa, the same user can conduct several attacks to achieve the same goal. For example, an attacker can take control of the production of an exposed CNC by hijacking a parametric program, by modifying the geometry of a tool to introduce a micro-defect, or by changing the executed program.

vendors. Features like the remote configuration of a tool's geometry, or the ability to influence the parameters of a program with values fetched remotely (via network) are needed when dealing with complex automation and unsupervised process. However, although these requirements are nowadays more common in manufacturing, vendors don't seem to take into account the unwanted consequences of these features, thus raising concerns about security.

In this work, we conducted an evaluation on the technologies introduced by representative controller manufacturers to adhere to the Industry 4.0 paradigm. We identified common problems across the different vendors, namely the possibility of abusing of such technologies to perform attacks like denial-of-service, damage, hijacking, and data theft.

We conducted real-world attacks against CNC machines and documented our findings in a full blown paper (currently under development) and with this one being a preliminary and shorter version. We reported our findings to the vendors, together with a discussion on the countermeasures that prevent our attacks to happen and will improve the current situation.

References

1. Balduzzi, M., Bongiorni, L., Flores, R., Lin, P., Perine, C., Vosseler, R.: Lost in translation: When industrial protocol translation goes wrong. Trend Micro (2020)
2. Maggi, F., Balduzzi, M., Vosseler, R., Rösler, M., Quadrini, W., Tavola, G., Pogliani, M., Quarta, D., Zanero, S.: Smart factory security: A case study on a modular smart manufacturing system. Procedia Computer Science **180**, 666–675 (2021)
3. Quarta, D., Pogliani, M., Polino, M., Maggi, F., Zanchettin, A.M., Zanero, S.: An experimental security analysis of an industrial robot controller. In: 2017 IEEE Symposium on Security and Privacy (SP). pp. 268–286. IEEE (2017)