Hacking Industry 4.0 With CNC Vulnerabilities

Sergey Sidorov from @kl_secservices

Disclaimers

- Everything mentioned **has been reported** to respective vendor a long time ago
- **Not** a one-vendor problem, it’s an industry wide challenge
- Remember, **defenders are always behind** attackers

http://addxorrol.blogspot.com/2019/08/rashomon-of-disclosure.html

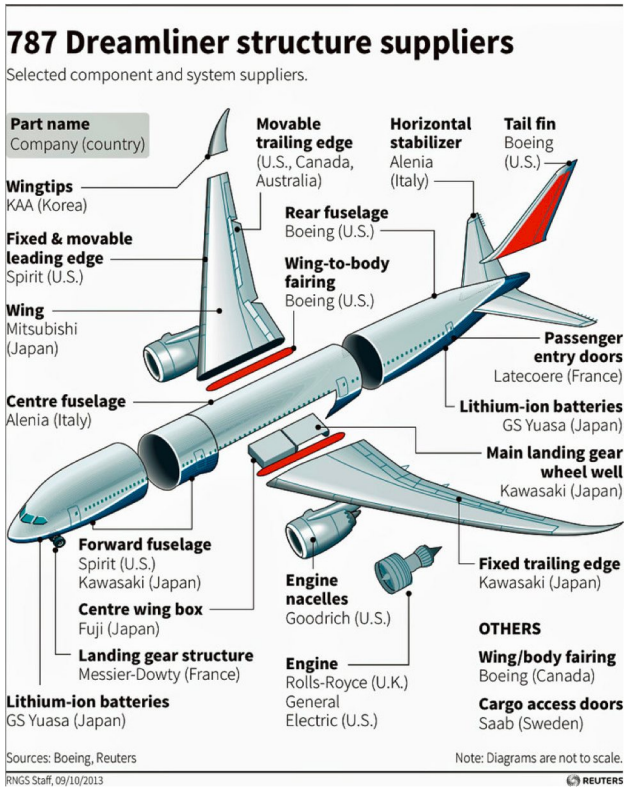
Manufacturing intro

Product design

Producing CAD/CAM of components

Factory

With CNC machines producing components: from screws/bolts to body parts



Manufacturing intro (almost PLM)

Product design

Producing CAD/CAM of components

Factory

With CNC machines producing components: from screws/bolts to body parts

Manufactured components “assembled” view

G-code

- G-code (= *RS-274*) – numerical control programming language
- A set of instructions for machine instruments (e.g. milling tool)
- CAD/CAM converted to G-code
- Same as in 3d printers

G00 X-25 Y20
G91 X-10
G02 X10 Y-10 I10 J0 F200 M3
G02 X-10 Y10 I0 J10;
G90 G00 M5 X0 Y0;
G00 X25 Y20
G91 X-10
G02 X10 Y-10 I10 J0 F200M3
G02 X-10 Y10 I0 J10;
G90 G00 M5 X0 Y0;
G00 X40 Y0
G02 X-40 Y0 I-40 J0 F200 M3
G90 G00 M5 X-55 Y0;
G02 X0 Y-55 I55 J0 F200 M3
G02 X-55 Y0 I0 J55

https://roboticsandautomationnews.com/2018/01/26/how-to-become-a-g-code-master-with-a-complete-list-of-g-codes/15807/

CNC machines

Lots of vendors vendors

Ethernet networks inside

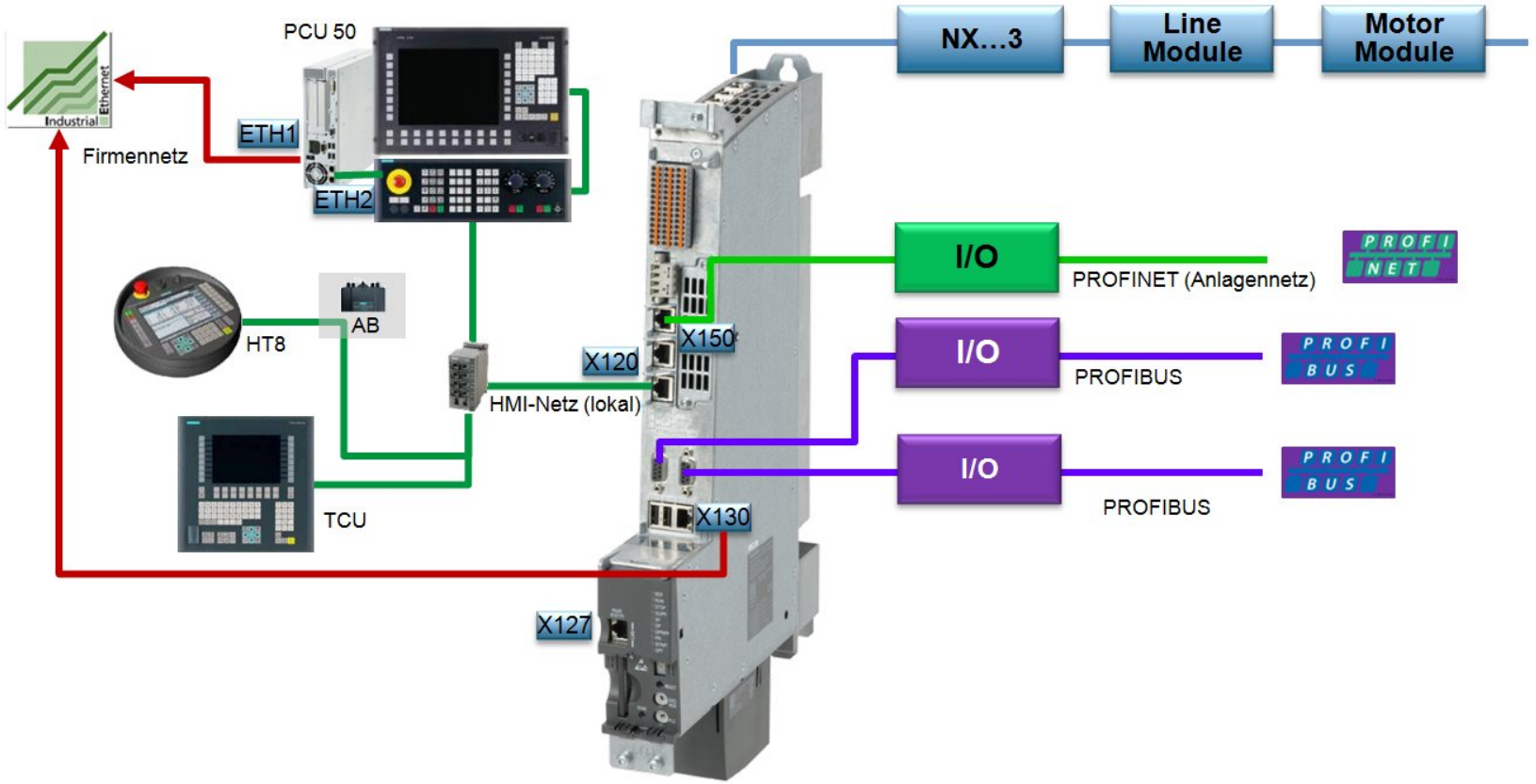
CNC is a “PLC”

Execute G-code

Siemens Sinumerik 840D sl CNC

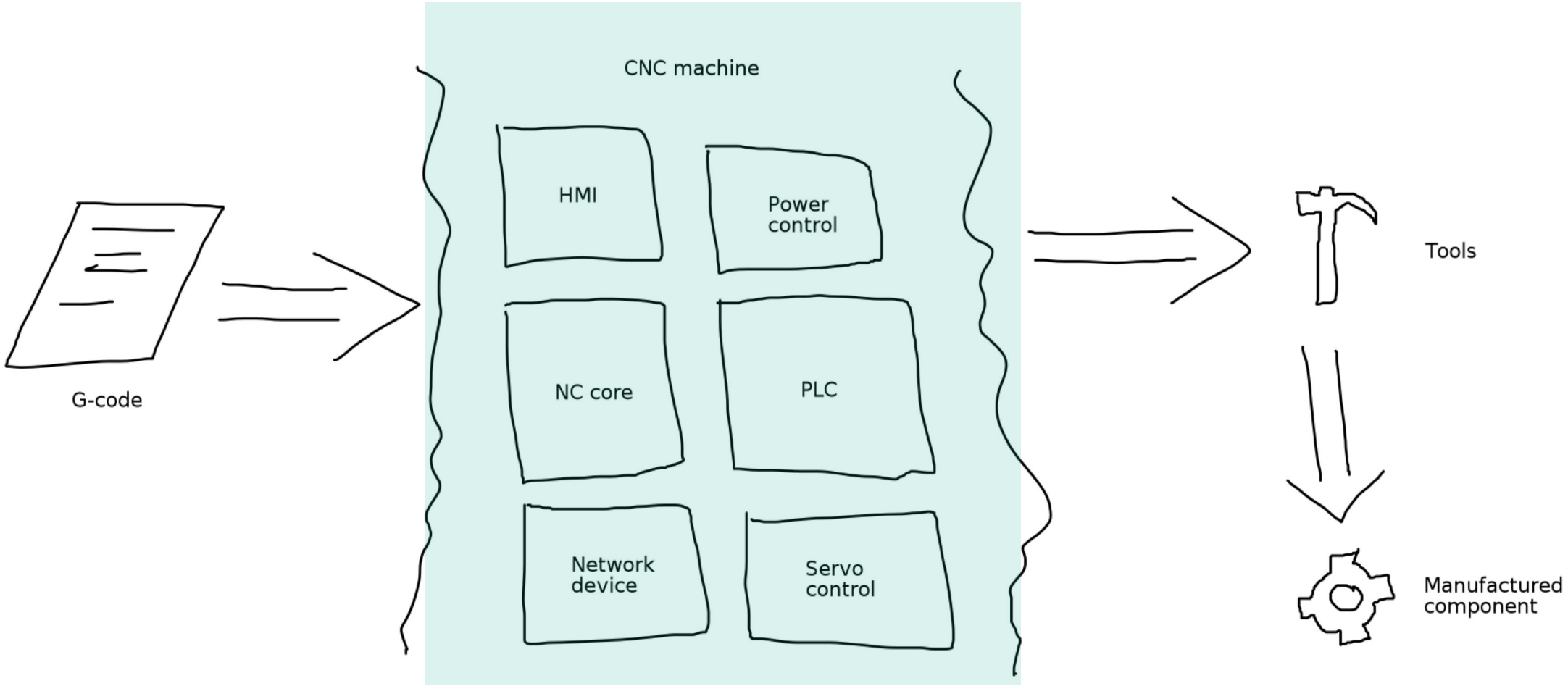
NCU (Numerical control Unit) - **central processing unit** of the 840D controller. This contains the following main modules:

- **NC-CPU:** Linux-based system for executing NC program
- **PLC-CPU:** SIMATIC S7-300 controller for safety functions (borders limits)

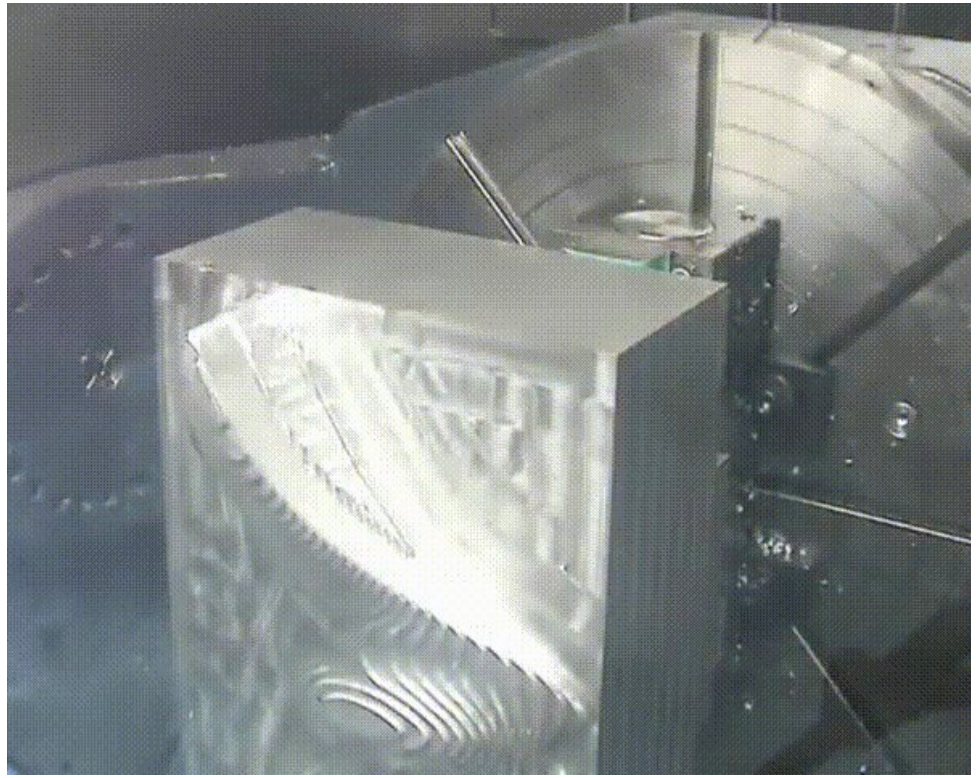


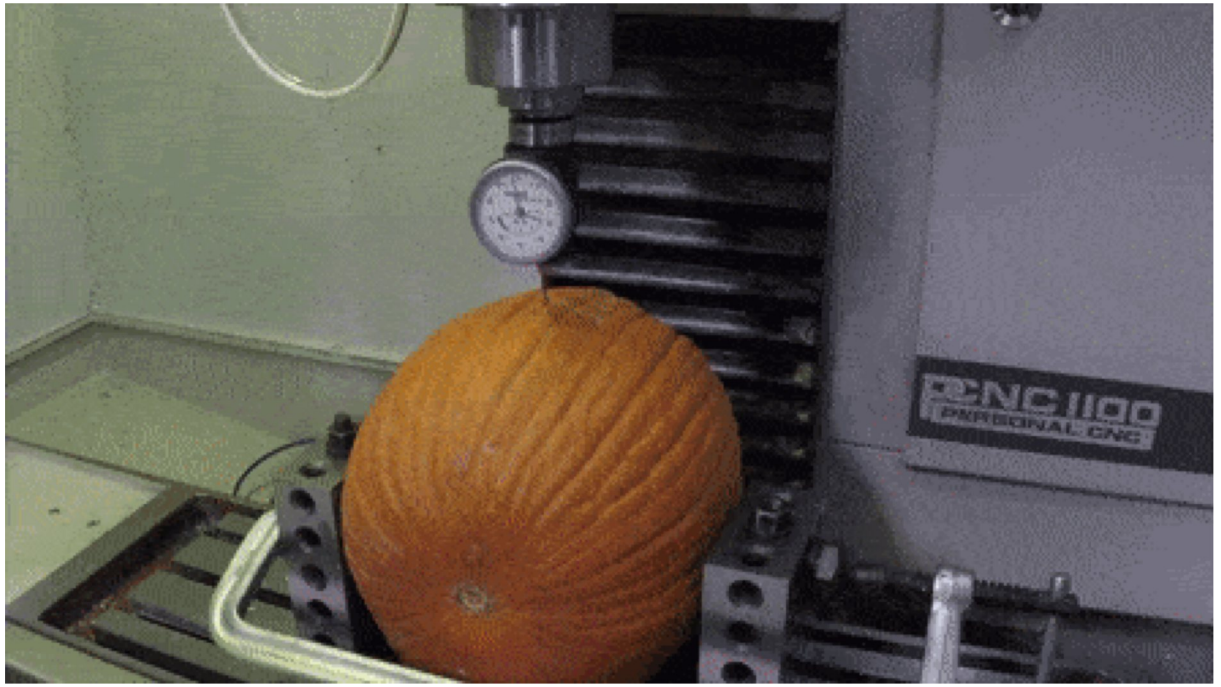
https://support.industry.siemens.com/cs/document/109481158/scalance-s615-with-sinumerik-840d-sl?dti=0&lc=en-ES

Inside CNC


CNC machine
HMI
Power control
NC core
PLC
Network device
Servo control
G-code
Tools
Manufactured component

CNC and what could possibly go wrong





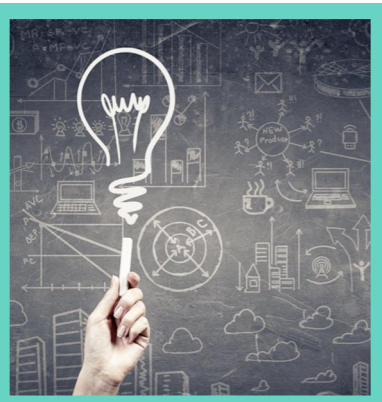
https://zippy.gfycat.com/JadedFlatBoutu.webm

https://giant.gfycat.com/SorrowfulIllegalIguanodon.gif

CNC related threats (threat modelling)

Damage of CNC components, products and instruments

Denial of Service attack, Remote Code Execution, Spoofing attack, etc.



Intellectual property theft, information disclosure

G-code (also CAD/CAM) have IP value

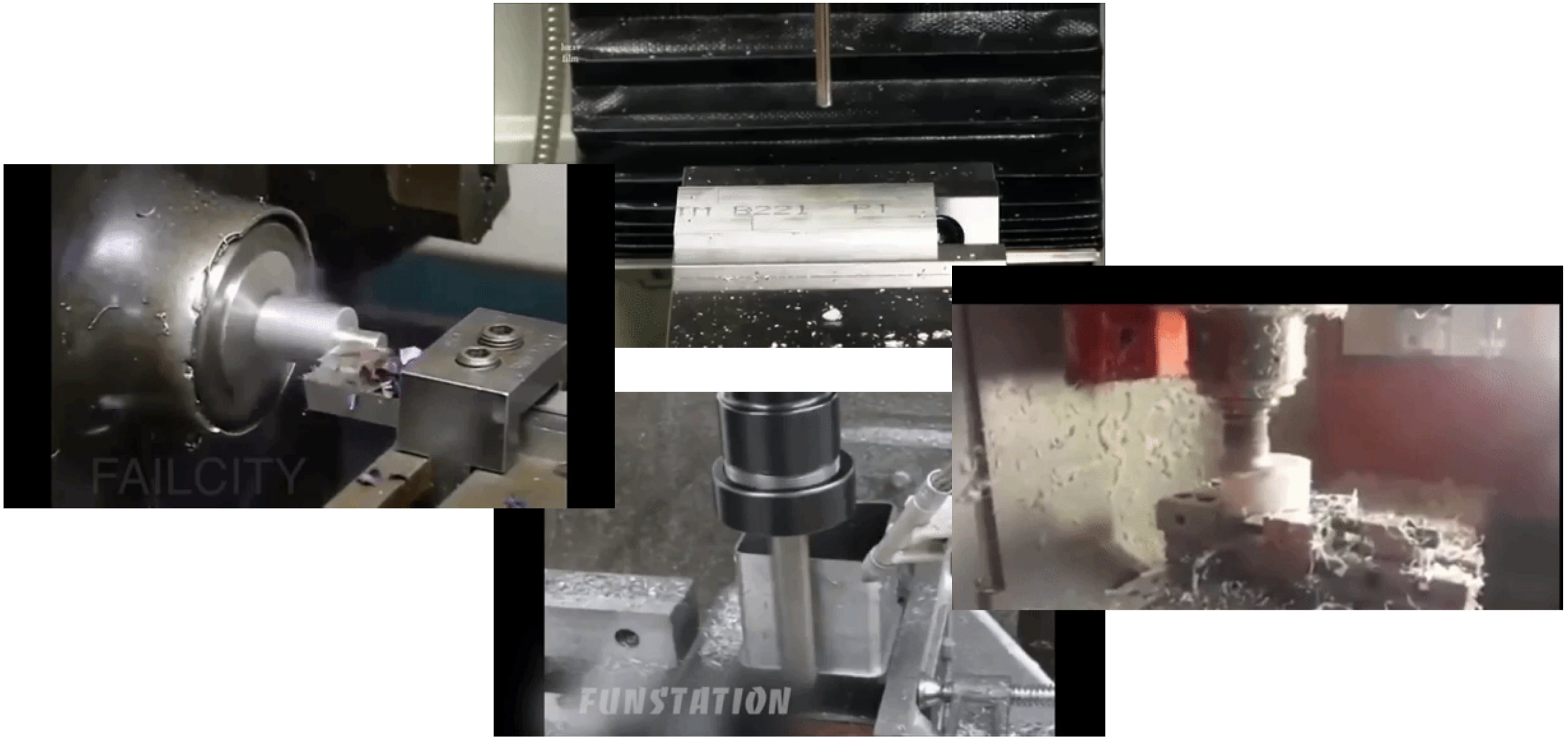
Introducing flaw in the development

Minor modifications of produced components to lower its MTBF (mean time between failures) or causing eventual damage to assembled product

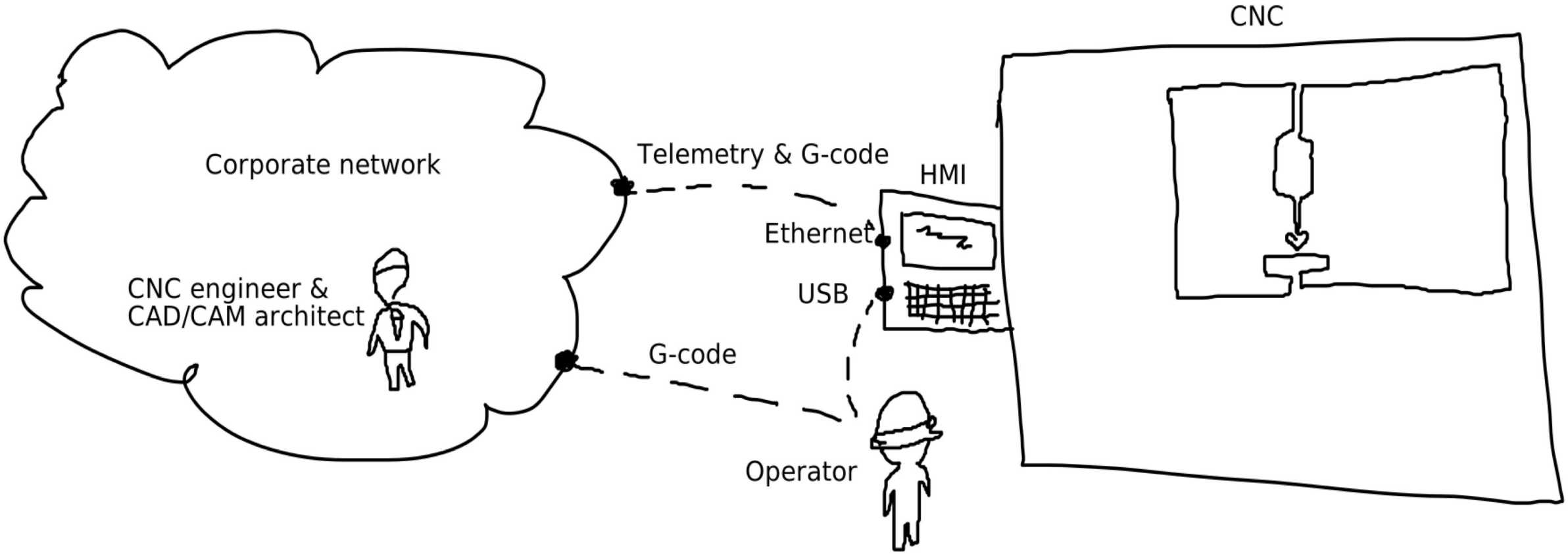
Operator safety

Most of the CNCs are in secured containers, but still can be dangerous to employees.

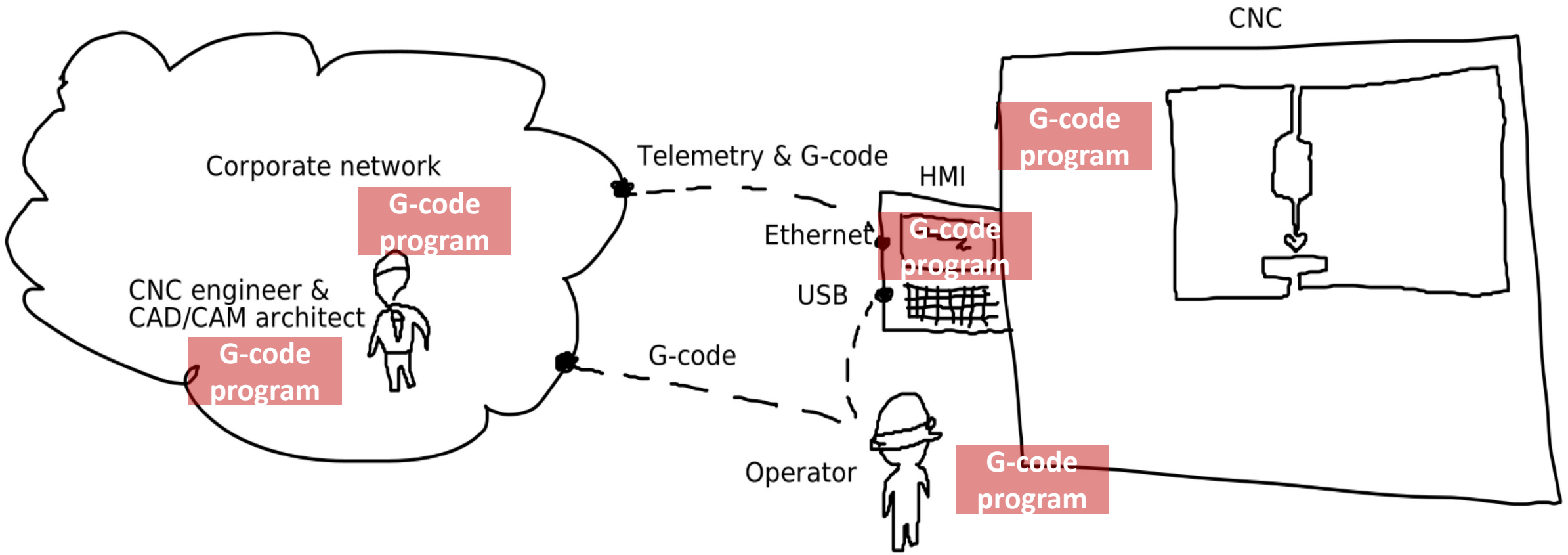
CNC fail compilations



Outside CNC


CNC
Corporate network
Telemetry & G-code
HMI
Ethernet
USB
CNC engineer &
CAD/CAM architect
G-code
Operator

Outside CNC: where is my G-code?



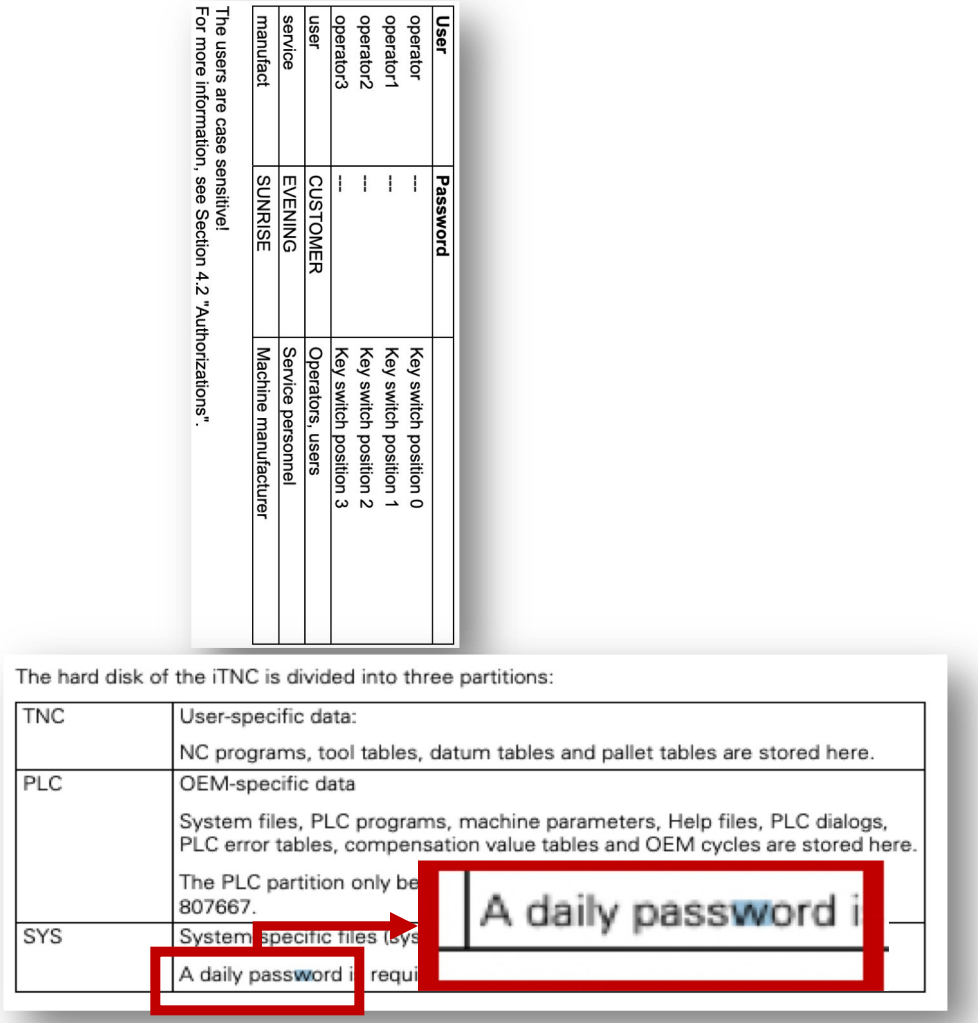
Important note

No vendors were harmed *Everything discussed is fixed* ONLY COORDINATED DISCLOSURE **Siemens, Fanuc, Mitsubishi, Heidenhain and others are alike security-wise**

(C) KATIE CAREY

Helping hand on user management

- No policies, instruments, integration for identity/password management
- All passwords in user and commissioning guides available publicly
- Lots of hardcodes - not possible to change those
- Applicable to FANUC, Heidenhahn, Sinumerik, etc.



The users are case sensitive!
For more information, see Section 4.2 "Authorizations".

User	Password	
operator	---	Key switch position 0
operator1	---	Key switch position 1
operator2	---	Key switch position 2
operator3	---	Key switch position 3
user	CUSTOMER	Operators, users
service	EVENING	Service personnel
manufact	SUNRISE	Machine manufacturer

The hard disk of the iTNC is divided into three partitions:

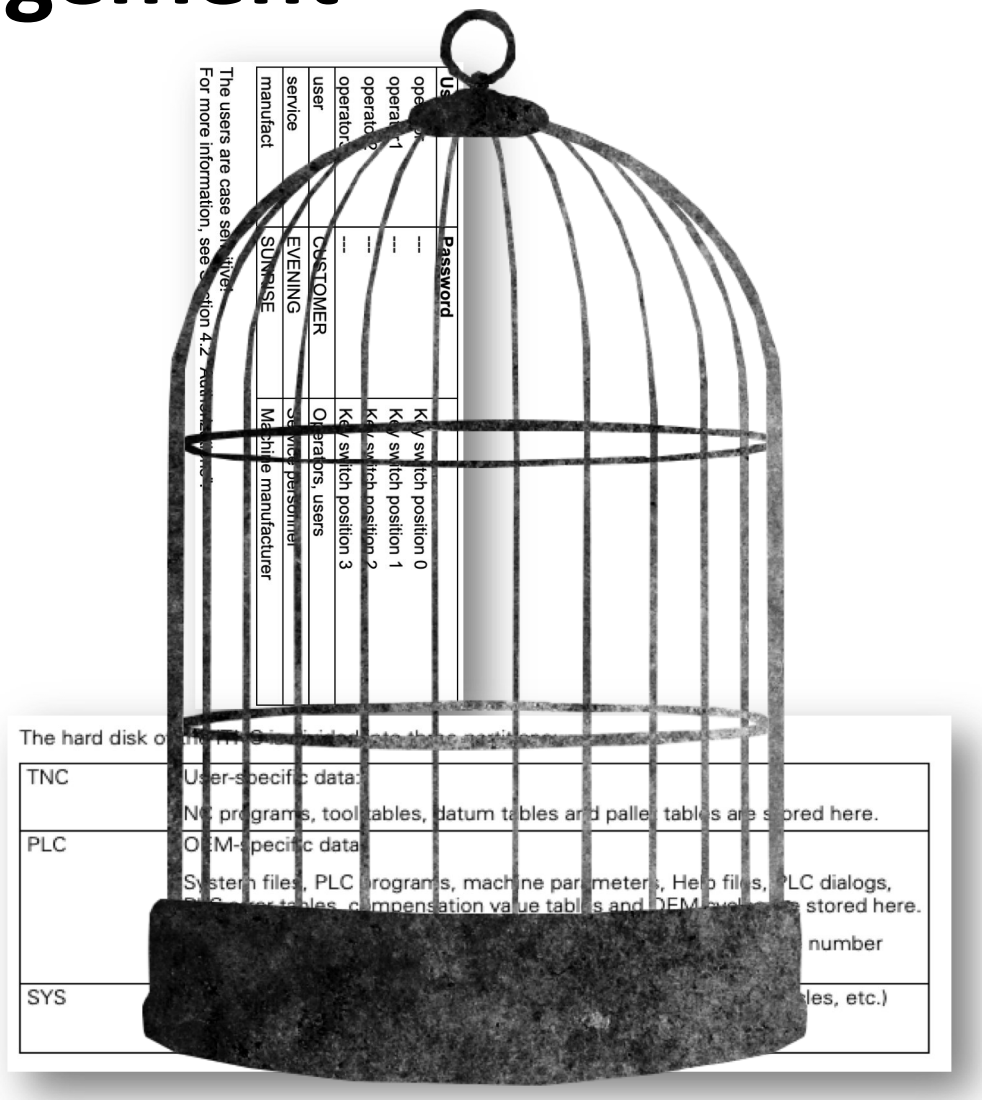
TNC	User-specific data: NC programs, tool tables, datum tables and pallet tables are stored here.
PLC	OEM-specific data System files, PLC programs, machine parameters, Help files, PLC dialogs, PLC error tables, compensation value tables and OEM cycles are stored here. The PLC partition only be 807667.
SYS	System specific files (sys A daily password i requi

A daily password i

Helping hand on user management

- No policies, instruments, integrati
  identity/password managem
- All passwords in user a ssioning
  guides available p
- Lots of hard t possible to change
  those
- A to FANUC, Heidenhahn,
  erik, etc.

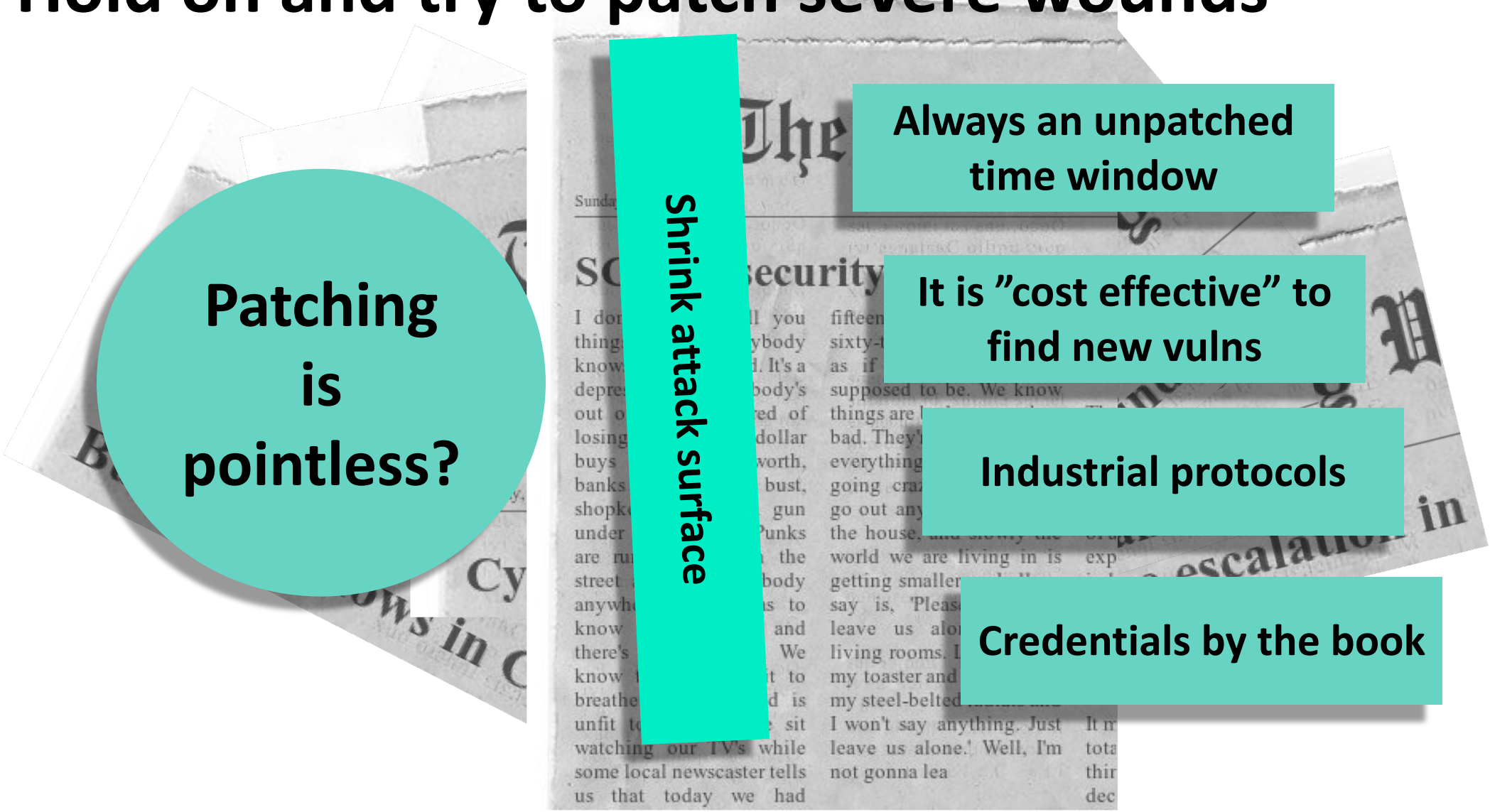
Remediation: It is all isolated, so don't panic



Hold on


Sunday, August 2, 2019
Buffer overflows in
Remote
Cy
The Daily
Sunday, August 2, 2019
SCADA security! Potato bicy
I don't have to tell you things are bad. Everybody knows things are bad. It's a depression. Everybody's out of work or scared of losing their job. The dollar buys a nickel's worth, banks are going bust, shopkeepers keep a gun under the counter. Punks are running wild in the street and there's nobody anywhere who seems to know what to do, and there's no end to it. We know the air is unfit to breathe and our food is unfit to eat, and we sit watching our TV's while some local newscaster tells us that today we had fifteen homicides and sixty-three violent crimes, as if that's the way it's supposed to be. We know things are bad - worse than bad. They're crazy. It's like everything everywhere is going crazy, so we don't go out anymore. We sit in the house, and slowly the world we are living in is getting smaller, and all we say is, 'Please, at least leave us alone in our living rooms. Let me have my toaster and my TV and my steel-belted radials and I won't say anything. Just leave us alone.' Well, I'm not gonna lea
industrial
anisms in S
ge escalation in

Hold on and try to patch severe wounds

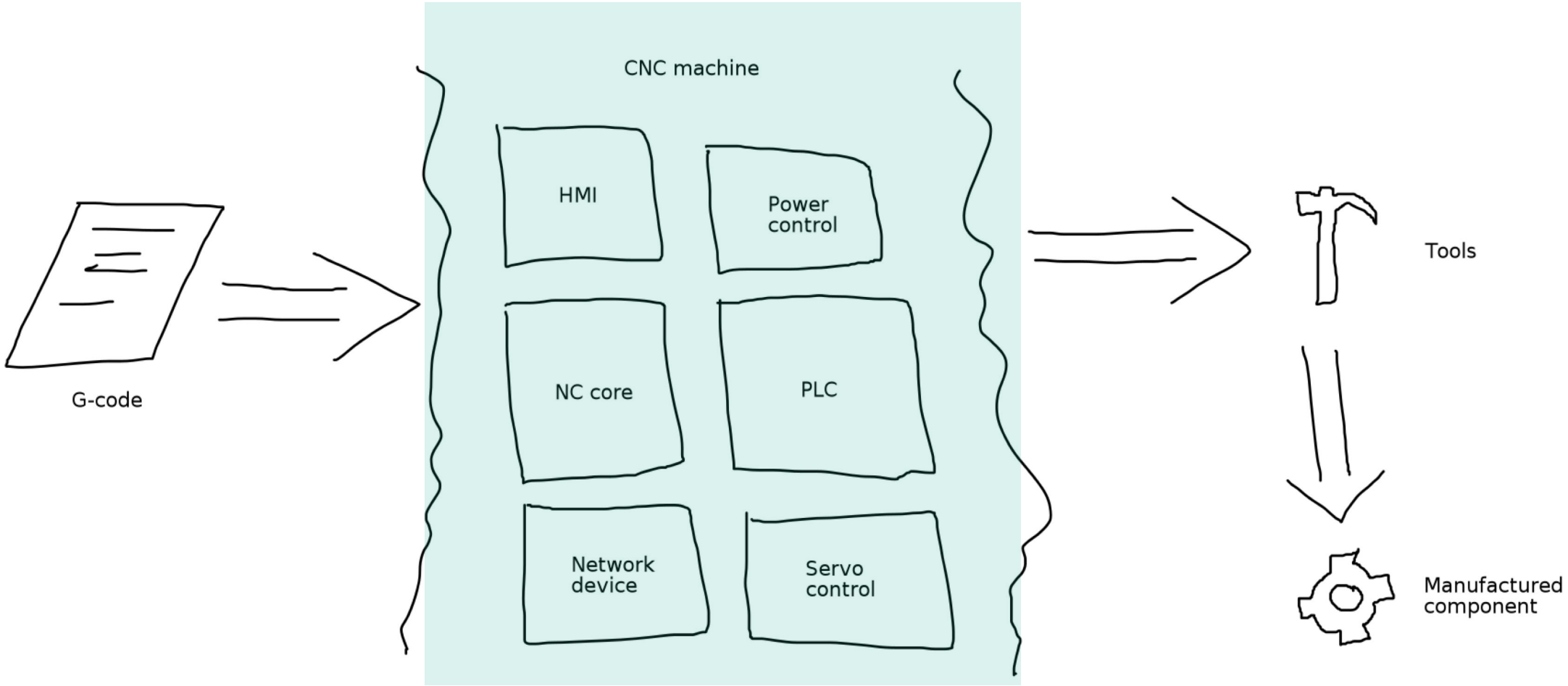


Vulnerabilities in Sinumerik CNC

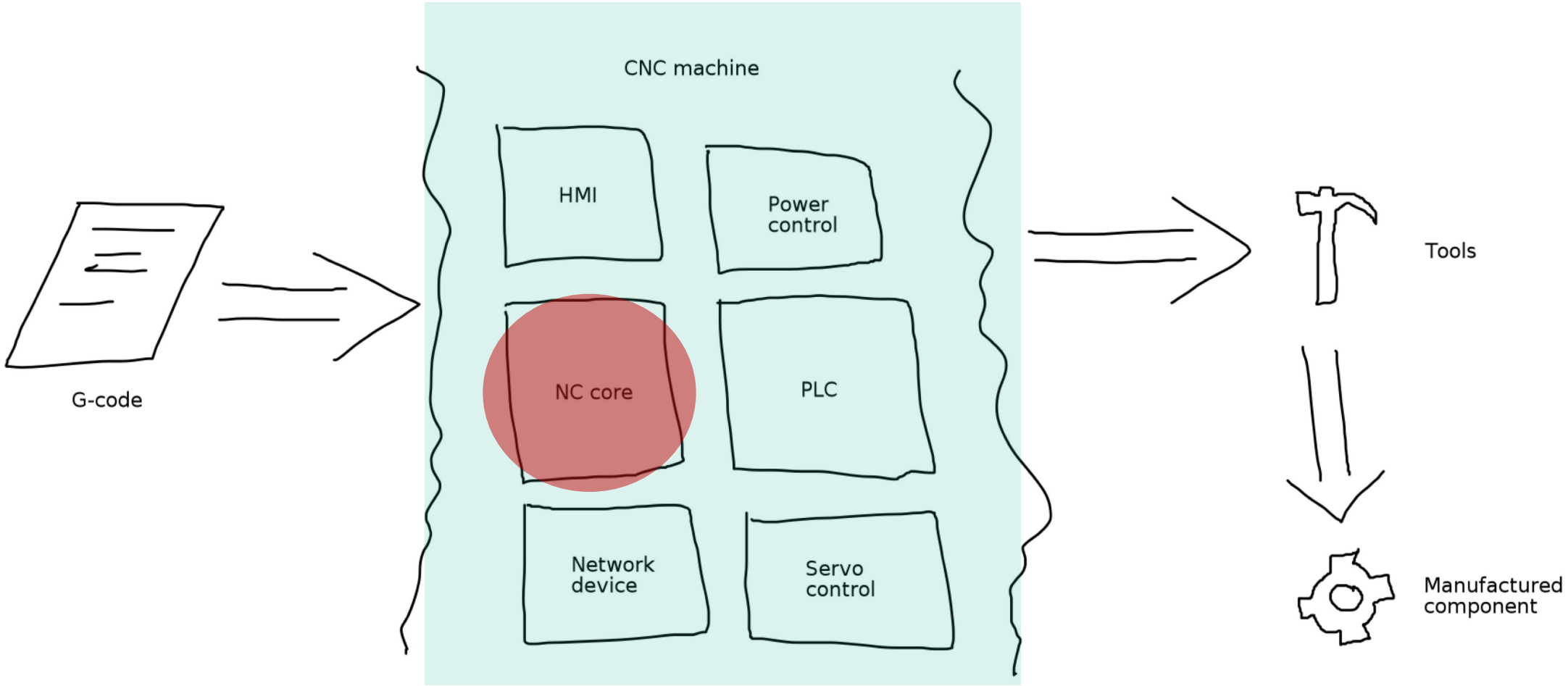
Remote vectors for host facing corporate network	Local vectors for host facing corporate network
CVE-2018-11457 **9.8**	CVE-2018-11459 **7.0**
CVE-2018-11458 **9.8**	CVE-2018-11460 **6.7**
CVE-2018-11464 **5.3**	CVE-2018-11461 **6.6**
CVE-2018-11466 **10.0**	CVE-2018-11463 **7.8**
Hardcodes not a vulnerability	CVE-2018-11465 **7.8**
	Hardcodes not a vulnerability

Siemens thanks Kaspersky for reporting the vulnerabilities and for coordinated disclosure. Siemens released updates for the affected devices
https://cert-portal.siemens.com/productcert/pdf/ssa-170881.pdf

CNC attack surface



CNC attack surface



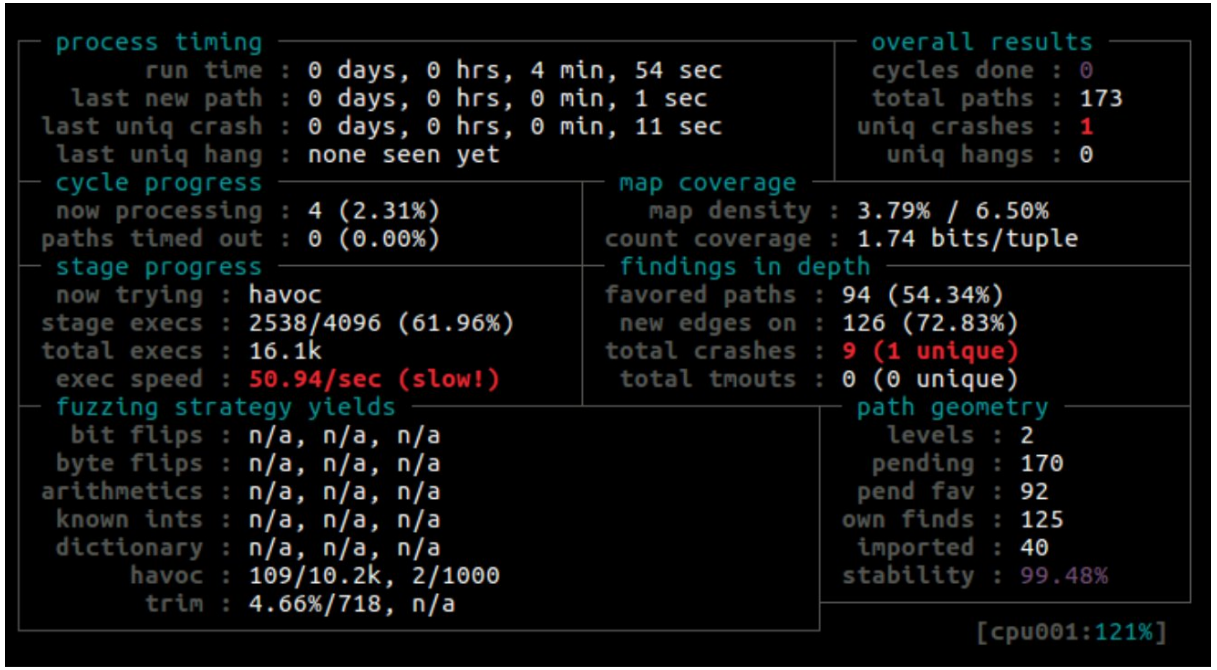
NC attack surface

- NC-CPU: Linux-based system for executing NC program
- X86 CPU
- Network services
  - miniweb
  - VNC
  - S7
  - OPC UA
- Ordinary Linux box from attacker perspective

OPC UA

ICS-CERT Research

- Open protocol
- Various implementation
- Good target for fuzzing



https://ics-cert.kaspersky.com/reports/2018/05/10/opc-ua-security-analysis/

Possible remote code execution

CVE-2018-11457:

- **miniweb.exe** application listens on port 4842/TCP
- **FindServerRequest** in UA Secure Conversation Message

Vulnerability:

- Integer Overflow that leads to Heap Corruption
- Other requests are also vulnerable: ServerOnNetwork, GetEndpointsRequest, ApplicationDescription, etc.

Impact:

- Potential remote code execution.

```
buf_ptr = (*(int (__cdecl **)(int, signed int, const char *))(MWEB_UASTACK_g_pMem +
12))(4 * array_len, 176, "Generated/MWEB_OpcUa_StackService_FindServersRequest.c");
if (!buf_ptr)
{
 v7 = (unsigned __int16)v7 | 0xE6870000;
 if ( MWEB_g_pCoreContext )
  (*(void (__cdecl **)(int, const char *, int, signed int, const char
*))(MWEB_g_pCoreContext + 120))((unsigned __int16)v7 | 0x2BC0000,"\"%s\" BAILED
OUT with code: %08X: %s", achScope_23008_1, v7, " Memory Error:a_pValue-
>LocaleIds\n");
 goto LABEL_37;
}
```

```
for ( i = 0; array_len > i; ++i )
  *(_DWORD *)(4 * i + buf_ptr) = 0;
for ( j = 0; array_len > j; ++j )
{
 v3 = MWEB_String_Read(a2, 4 * j + buf_ptr);
 LOWORD(v3) = 0;
 v7 = (unsigned __int16)v7 | v3;
 if ( v7 < 0 )
   goto LABEL_37;
}
```

VNC CNC HMI VNC HMI

Just so you know:
HMI on CNC is mostly VNC

https://www.industry.siemens.com/topics/global/en/cnc4you/tips_and_tricks/Documents/SINUMERIK_HMI_to_External_Monitor.pdf

Remote code execution

CVE-2018-11458, CVE-2018-11459, CVE-2018-11464:

- Slsmsystemmanager application - VNC server

Vulnerability example:

- Buffer overflow in GiiDevice::handle_rfbGIIEventInjection() function.
- Possiblity to write beyond buffer boundry and rewrite return address on the stack.

Impact:

- Potential remote code execution.

```
do
{
  v14 = 4LL;
  savedregs = v14 >> 32;
  v81 = v14;
  QIODevice::read(*((QIODevice **)this + 34), (char *)&v49 + 4 * v13, *(__int64 *)&v81);
  v80 = (char *)*((unsigned __int8 *)this + 156);
  v79 = (GiiDevice *)*(&v49 + v13);
  LOWORD(v15) = GiiDevice::endian(v79, (char)v80);
  v12 = this;
  *(&v49 + v13++) = v15;
  *((_WORD *)v12 + 83) -= 4;
}
while ( v47 > v13 );
//The *(&v49 + v13++) = v15 value writes to the stack and the loop count is controlling
//by data from TCP packet.
//Code 13. Loop count calculation
  v80 = (char *)*((unsigned __int8 *)this + 156);
  LOWORD(v9) = GiiDevice::endian(*(GiiDevice **)&sHeader[8], (char)v80);
  v41 = v9;
  v80 = (char *)*((unsigned __int8 *)this + 156);
  LOWORD(v10) = GiiDevice::endian(*(GiiDevice **)&sHeader[12], (char)v80);
  v47 = v10 / v41;
```

S7 protocol

S7comm well known:

Text introduction http://gmiru.com/article/s7comm/

Open source library https://sourceforge.net/projects/snap7/

Information gathering https://github.com/klsecservices/s7scan

Remote code execution

CVE-2018-11466:

- cp_710 application is responsible for s7comm

Vulnerability example:

- Lots of bugs were leading to crashes or exit()'s of the application
- Possibility to write beyond buffer boundary and rewrite return address on the stack.

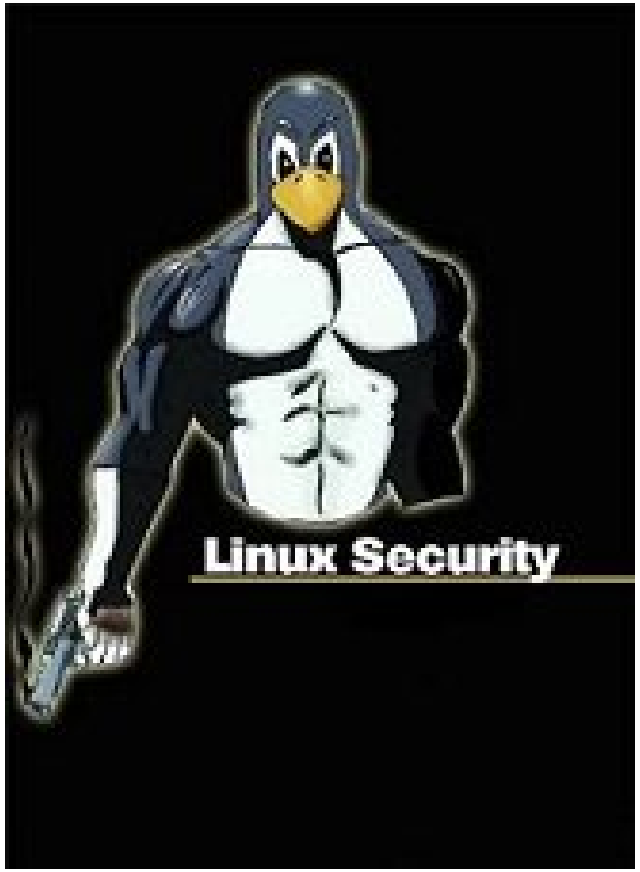
Impact:

- Potential remote code execution.

```
void L7_Init_Download_Element(L7_DOWNLOAD_LIST_EL
*Download_List_Ptr)
{
 /* Download_List_Ptr = 0x081ZZZZZ */
 Download_List_Ptr->In_Use = 1;
 Download_List_Ptr->State = 7;
 Download_List_Ptr->Appl_Id = L7_Cb.Dst_Appl;
 Download_List_Ptr->Cn_Id = L7_Cb.Cn_Id;
 memcpy(
  /* 0x081ZZZZZ */
  Download_List_Ptr->Dom_Name,
  /* offset from start of S7 protocol header in received packet (0x12
+ 7 = 0x19 => data block is copied)*/
  (char *)&L7_Cb.Pdu_Ptr->Q.Wr + 0x12,
  /* first data block byte (in this case it is 0xFF) plus 1 = 0x100 */
  L7_Cb.Pdu_Ptr->Q.Ds.Dat.Begin_Ladedaten + 1);
}
```

Post-remote exploitation

- Linux can be a problem for local privilege escalation
- How hard is path from www-data to root?



Unsafe file permissions (LPE)

CVE-2018-11459:

- R/W access for unprivileged user to the system configuration files (**/etc/basesys.ini)**

CVE-2018-11460:

- R/W access for engineering user to CNC software packages that are located in a variety of CRAMFS archives (**find /card -name '*.cfs'**)

Exploitation:

- Original value:

```
FirewallOpenPorts=TCP/4842 TCP/8080 TCP/102 TCP/5900 TCP/22
```

- Replace with:

```
FirewallOpenPorts=TCP/4842 TCP/8080 TCP/102 TCP/5900 TCP/22 `sed -i //
-- <OLD_PASSWORD_HASH>//<NEW_PASSWORD_HASH> /etc/shadow`
```

- Reboot

Local privilege escalation

- CVE-2018-11465, CVE-2018-11466
- drvslhwrt driver – internal bus
- Read arbitrary memory (see example of reading 0x0 –> ECX register)
- Write to arbitrary memory (see example of writing 0xf000f000 to 0x123)
- Execute arbitrary commands
- Custom drivers are made for LPE

```
if (request < 0x4...7)
{
    (args)();
    return 0;
}
```

NC attack vectors

- Network services
  - Miniweb (CVE-2018-11457)
  - VNC (CVE-2018-11458, CVE-2018-11459, CVE-2018-11464)
  - S7 (CVE-2018-11466)
  - OPC UA
- Ordinary Linux box from attacker perspective
  - Custom drivers (CVE-2018-11465, CVE-2018-11466)
  - Configuration files (CVE-2018-11459, CVE-2018-11460)

Prioritization: howto hazard analysis

Bucket of vulnerabilities

CNC related threats (threat modelling)

Damage of CNC components and products

Denial of service for software components of CNC

Broken parts of CNC (e.g. instrument)

Intellectual property theft, information disclosure

G-code (also CAD/CAM) have IP value

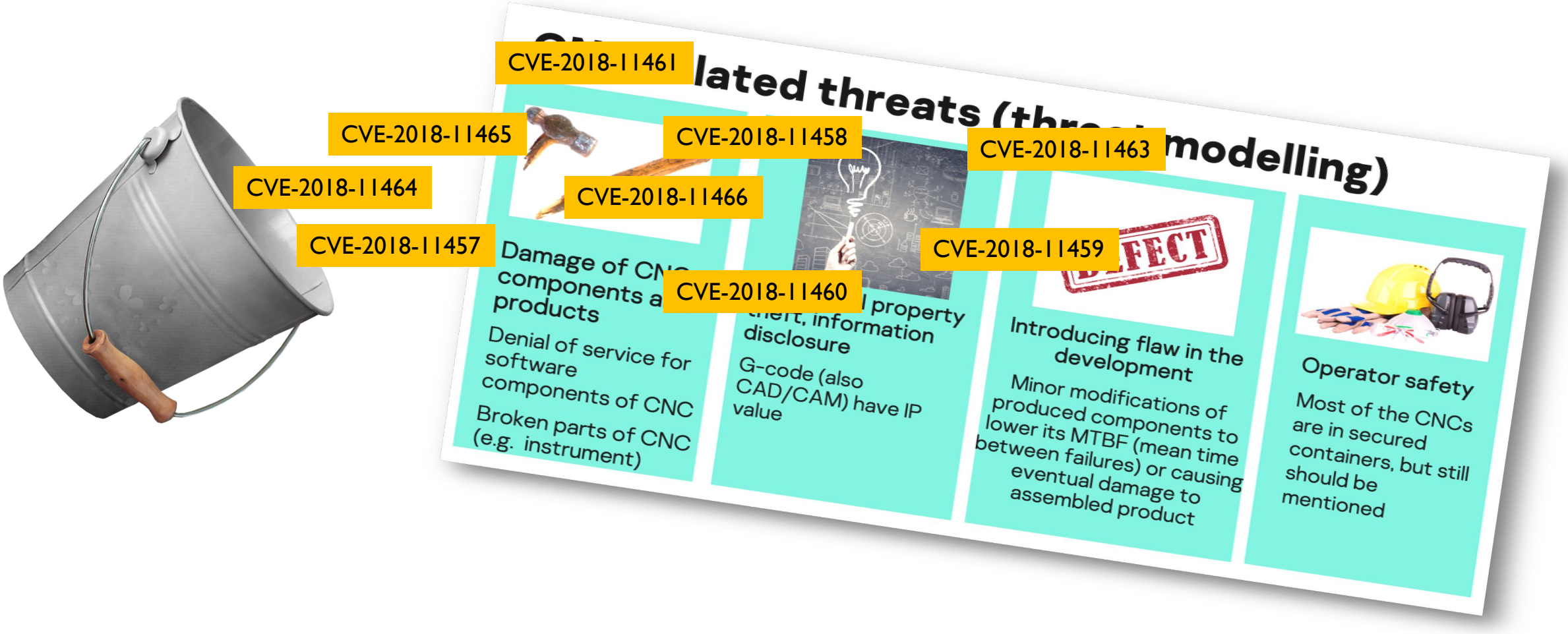
Introducing flaw in the development

Minor modifications of produced components to lower its MTBF (mean time between failures) or causing eventual damage to assembled product

Operator safety

Most of the CNCs are in secured containers, but still should be mentioned

Prioritization: howto hazard analysis



Recommendations

- Remove corporate network visibility, unless OPC UA or S7 is required for chosen hosts
  - That’s two firewall rules + deny any to any
- Malware scan company USB flash drives and never allow employees own removable media
  - Forbid USB at all and provide more security-wise control with network connection
  - Use USB if security maturity is low
- Implement jump host to connect anything to CNC as it would be usual Windows box where one can extensively audit events or EDR things

Recommendations

- Implicitly log-audit access to the G-code files on shares and introduce specific rules into your SOC to track security events and anomalies around those
- Do penetration testing of your manufacturing sites and request pentesters to assess process from CAD/CAM to G-code to CNC
- Request 3rd party proof of security posture for CNC vendor (Secure SDL report, security assessment/penetration testing report, etc.)
- Request security guide from vendor and force system integrator to follow it

Thanks!

Whitepaper & slides will be available
on https://github.com/klsecservices

@574rz Sergey Sidorov

Gleb Gritsai, Radu Motspan, Danila Parnishchev , Kirill Nesterov, Dmitry Sklyar, Dmitriy Zhuzhgov