
XP LEVEL
600
PRISON ESCAPE 2
NIGHT BEFORE DAWN
LOADING... PLEASE WAIT IT MAY TAKE A MOMENT..

Operator Jail breakout

Dieter Sarrazyn
dieter@secudea.be
@dietersar
https://be.linkedin.com/in/dietersarrazyn

Frank Lycops
frank@asvalis.com
https://be.linkedin.com/in/franklycops

Operator Jail ?

- Applications running in ‘full screen’ mode
- No access to underlaying OS

- Examples:
  - ATM systems
  - HMIs
  - Kiosk systems in stores / hotels

Asvalis Secudea
Cybersecurity services for Industry

Why important?

We are trying to prevent THIS…

Asvalis Secudea
Cybersecurity services for Industry

Common issues with operator jailed systems

- Apps (often) running with admin levels
- Stored clear text credentials
- Access to config files
- Access to internal network
- Access to confidential information
- No / outdated antivirus
- No whitelisting used

Why would I care?

"My system is in a secure control room"

- Operators get bored
  - Play games
  - Watch videos (located on USB)
- Operators make unauthorized system changes
  - It makes their lives easier

Why would I care?

"Only clients use that system,

no company information is on it"

- Often connected to office network
- Clients don't always remove their PII data
- Negative press

Checking operator jails …

"Do whatever was told to be wrong or not to be done"

Click on everything, press every button or key combinations

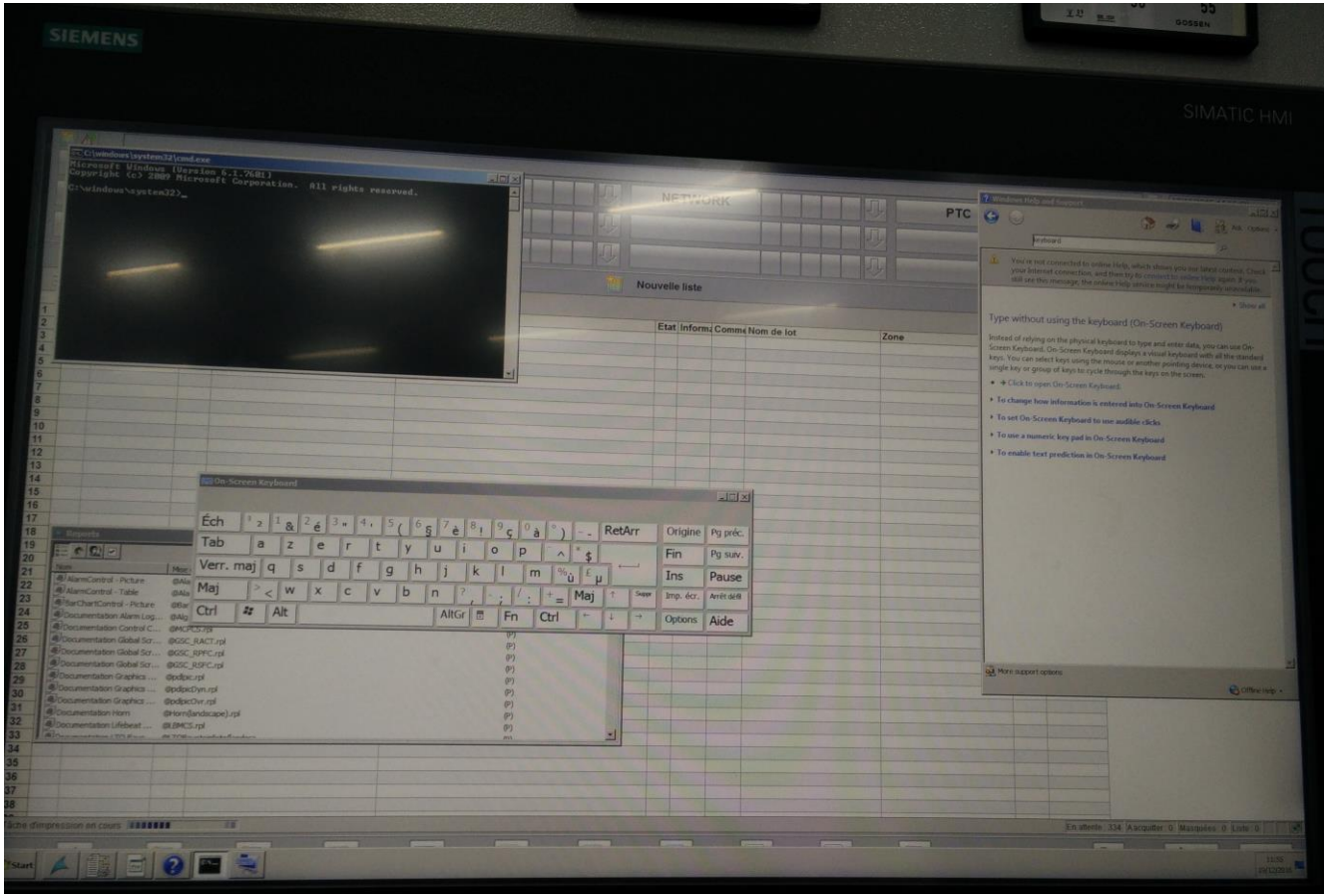
- "test" the mouse
- "test" the keyboard
- Provide incorrect input

Checking operator jails …

- Easy ways
  - Go to help (F1 or other)
    - Windows Help might be useful for once!
  - Sticky keys
  - Windows key combo's
  - Ctrl + key
  - Through installed software (internet explorer, AV, HMI or other)
- Harder ways
  - Network based

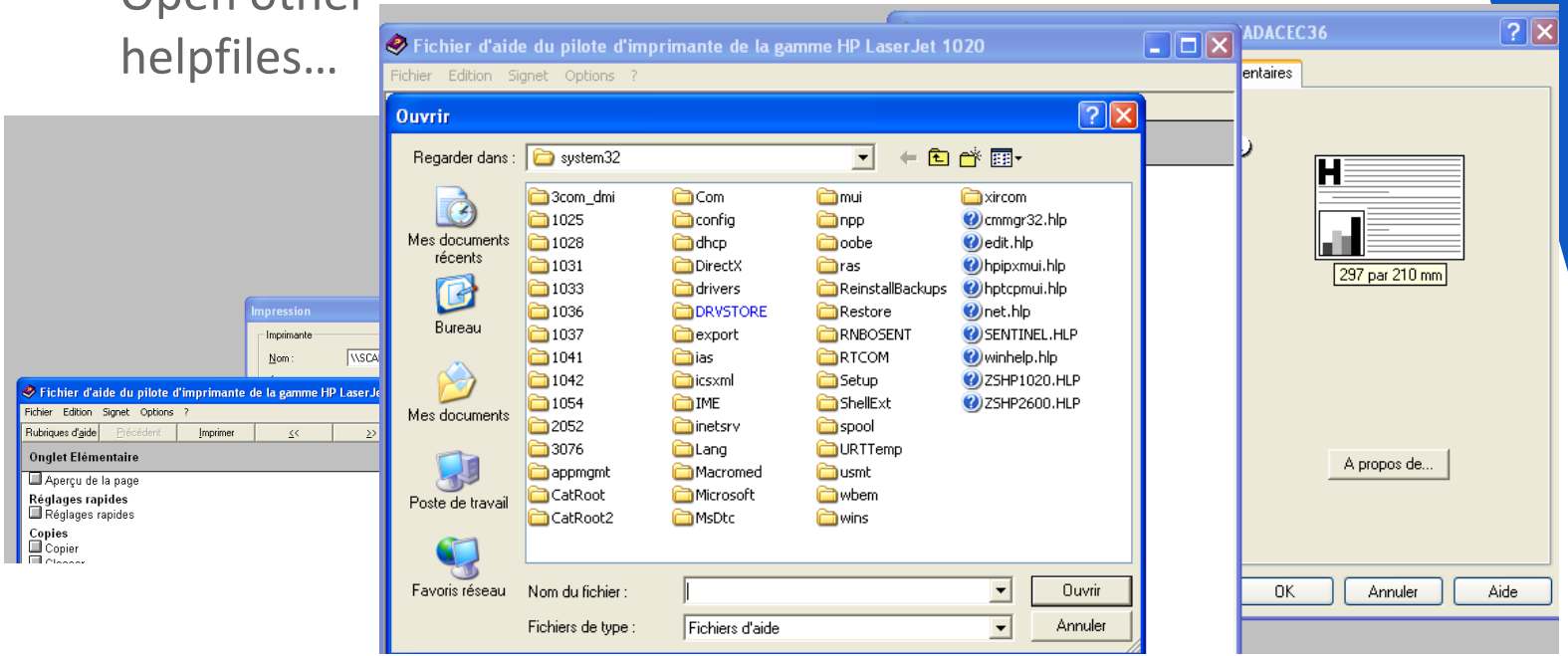
Checking operator jails … Go to hel(l)(p)

- Via the help window
  - Search & run: cmd.exe, task manager …
- Recent OS
  - Requesting help opens an Internet Browser

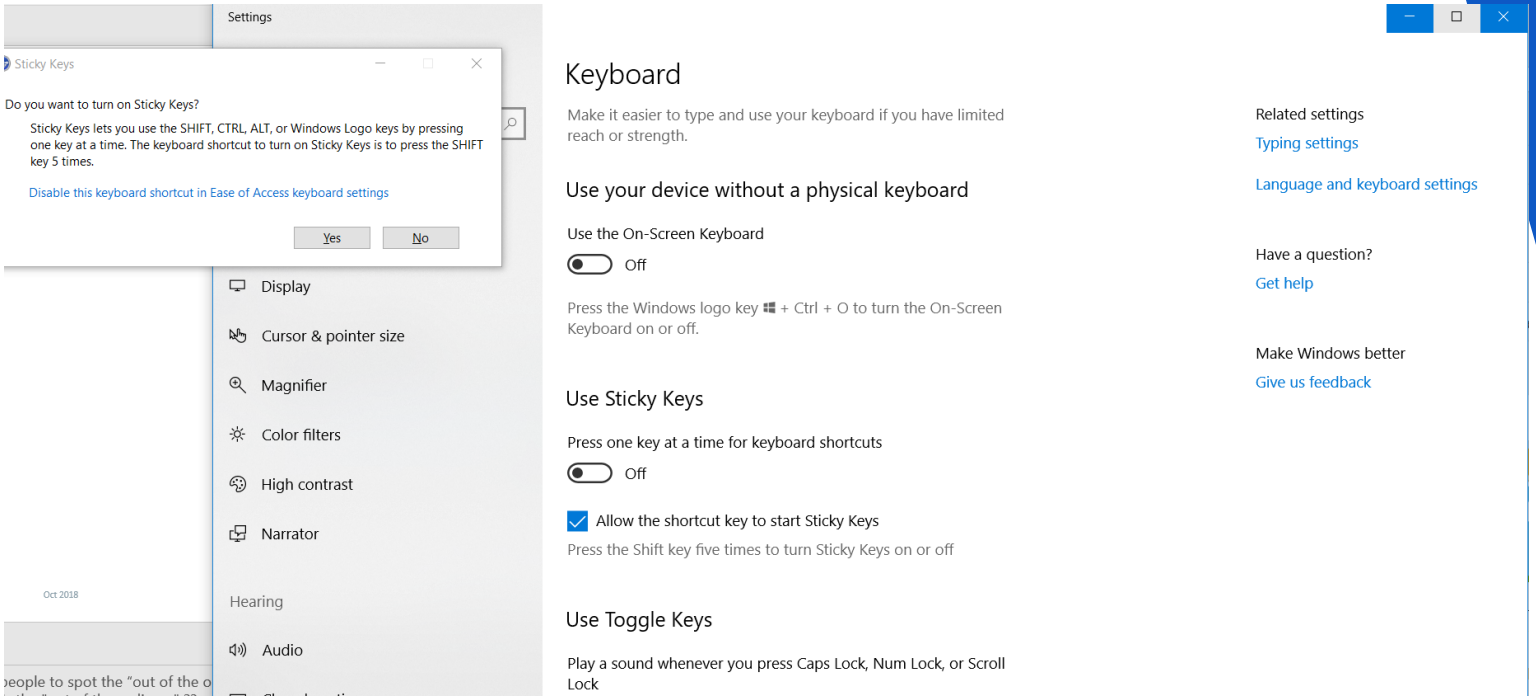

SIEMENS
SIMATIC HMI
NETWORK
PTC
Nouvelle liste
Etat
Nom de lot
Zone
On-Screen Keyboard
Type without using the keyboard (On-Screen Keyboard)

Checking operator jails … Go to hel(l)(p)

- Open other helpfiles…



Checking operator jails … sticky keys

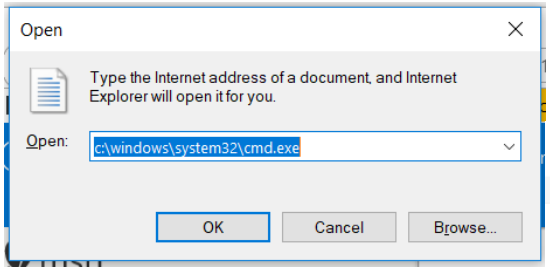


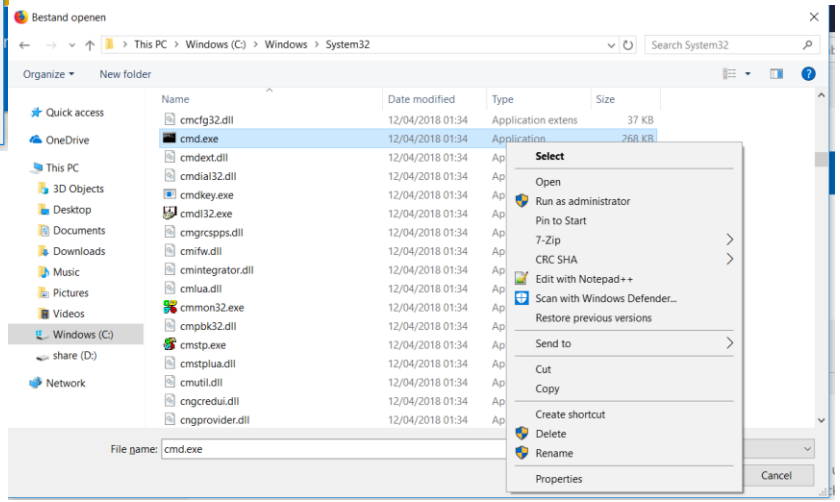
Checking operator jails … windows key combo's

Windows key

+ E => explorer
+ R => run
+ U / + I => (display) settings
+ Q => search
+ D => show desktop
+ A => show notifications sidebar
+ X => right click start menu

Checking operator jails … CTRL + key

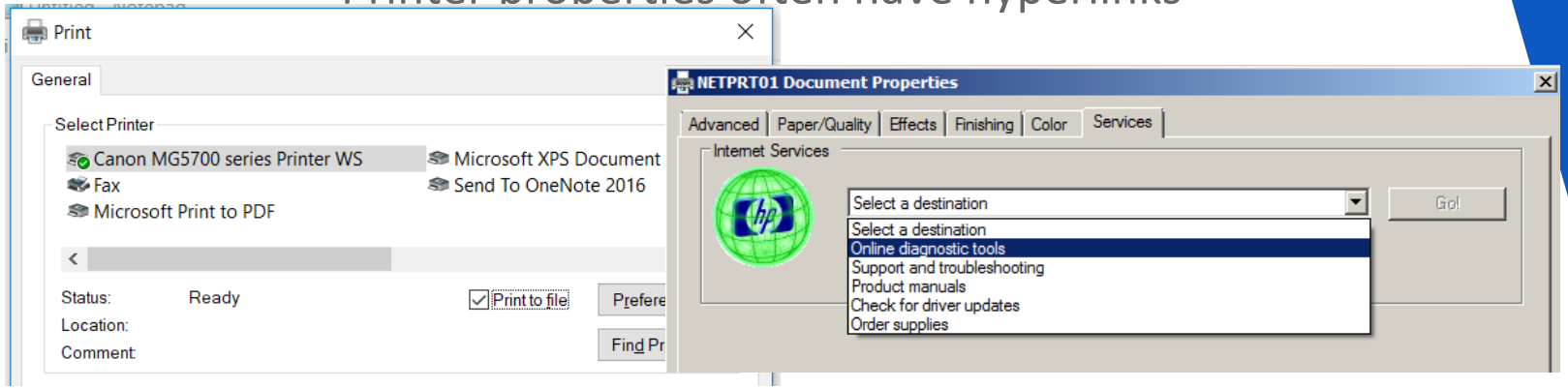




- CTRL + P
- CTRL + O
- CTRL + S
- …

Checking operator jails … Printing

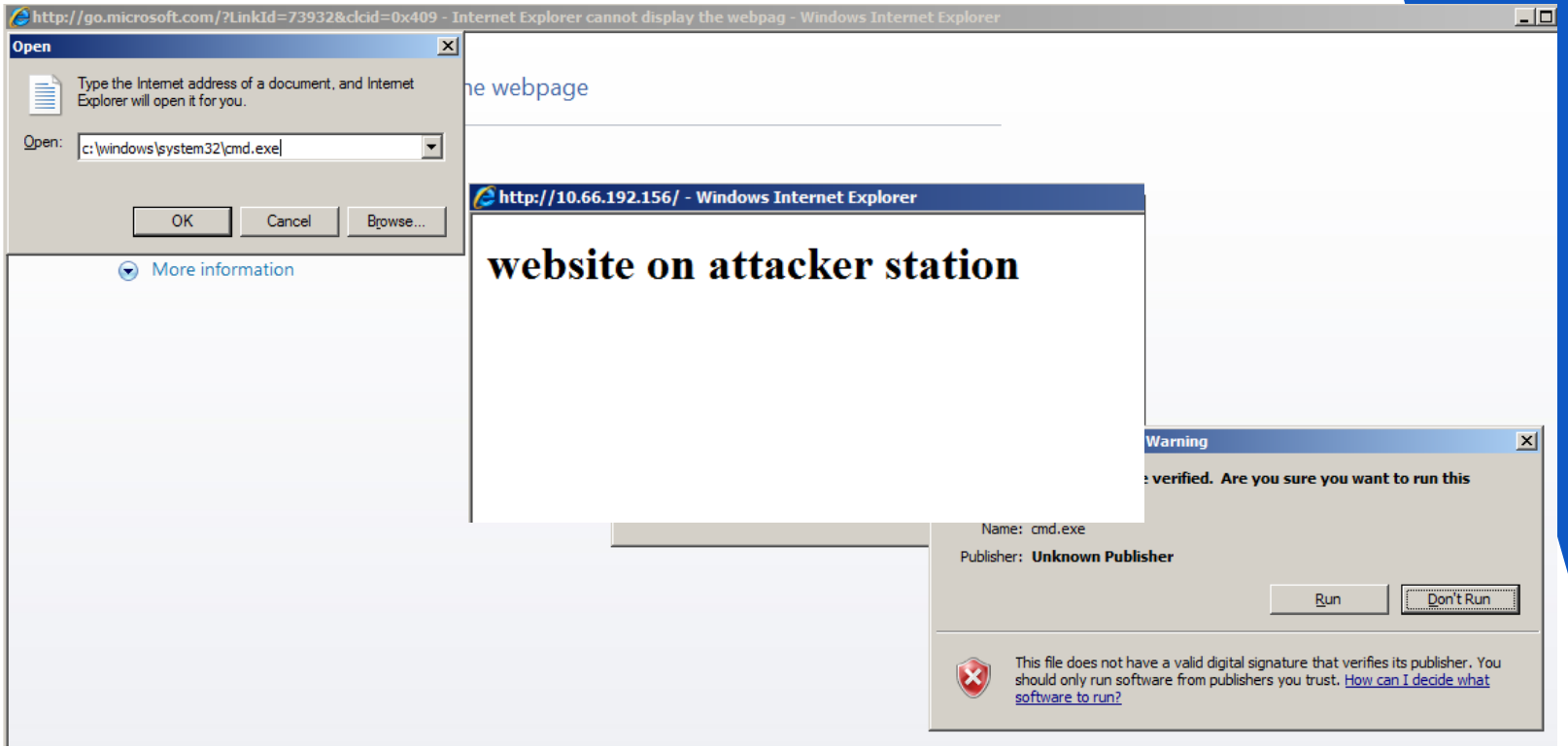
- Default Windows print dialog lets you break out
  - Print to (XPS) file
  - Find a printer
  - Printer properties often have hyperlinks



Checking operator jails … Internet explorer

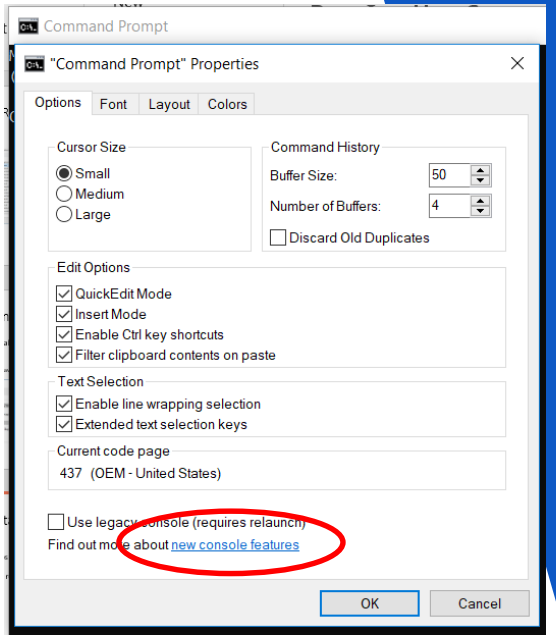
- Launched from any URL on the system / application
- Download your backdoor
- If internet connection exists: Ikatt

- “download” cmd.exe


http://go.microsoft.com/?LinkId=73932&clcid=0x409 - Internet Explorer cannot display the webpag - Windows Internet Explorer
Open
Type the Internet address of a document, and Internet Explorer will open it for you.
Open:
c:\windows\system32\cmd.exe
OK
Cancel
Browse...
More information
http://10.66.192.156/ - Windows Internet Explorer
website on attacker station
Warning
verified. Are you sure you want to run this
Name: cmd.exe
Publisher: Unknown Publisher
Run
Don't Run
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

Checking operator jails … other installed software

- Antivirus software popups in tray bar
  - Why not trigger the AV?
- Startup scripts that don't run 'silent'
  - Request properties
  - New hyperlink added in Windows 10
  - Opens with web browser…



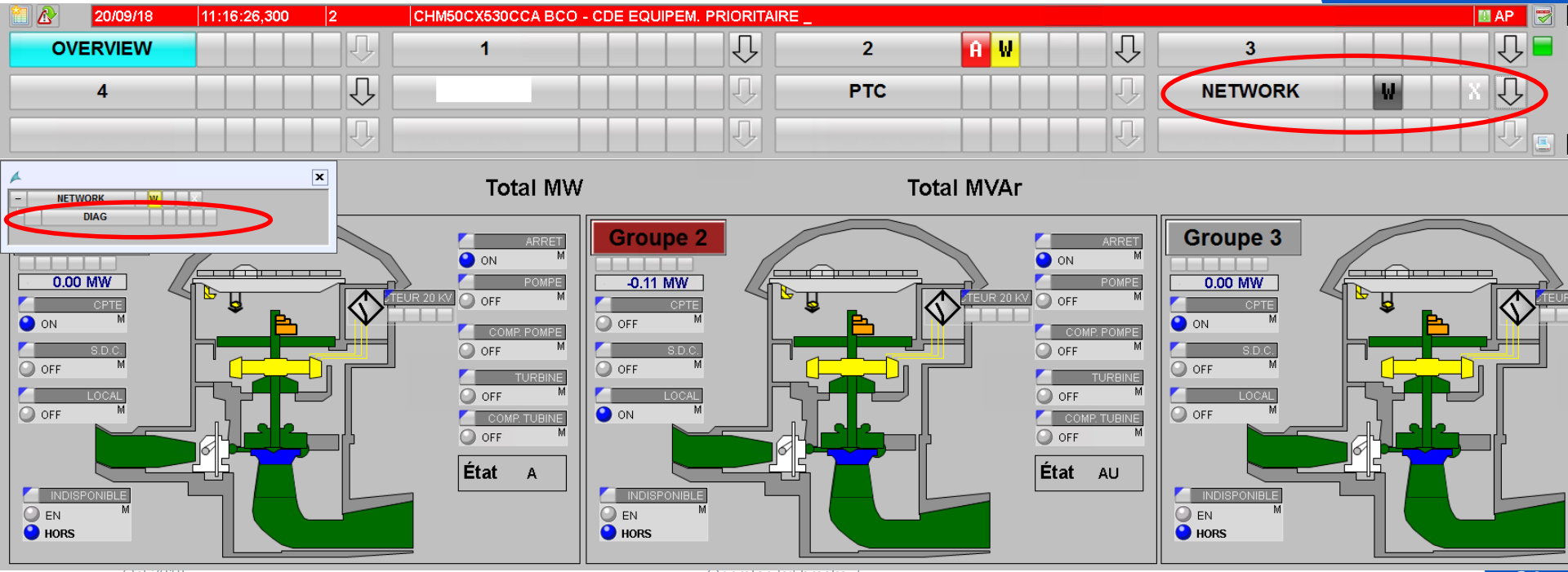
Asvalis Secudea

Checking operator jails … HMI Software

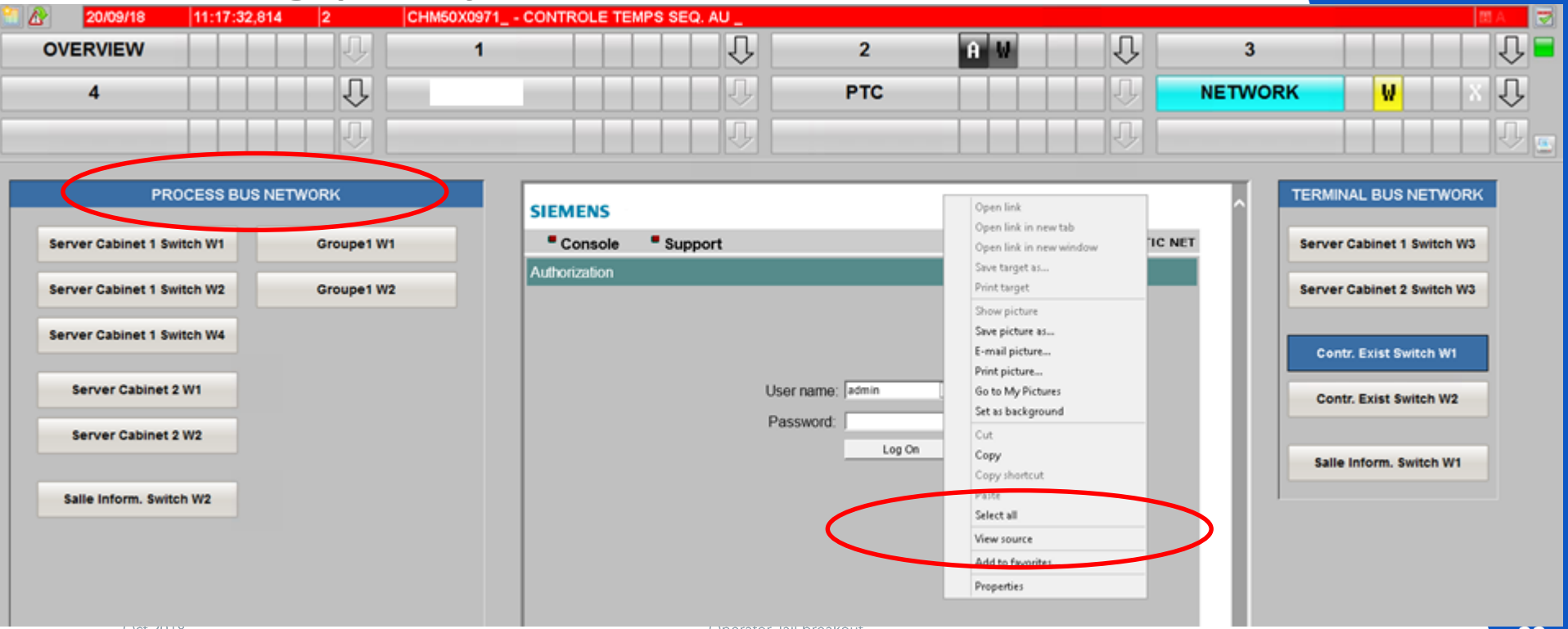
Siemens MM8000

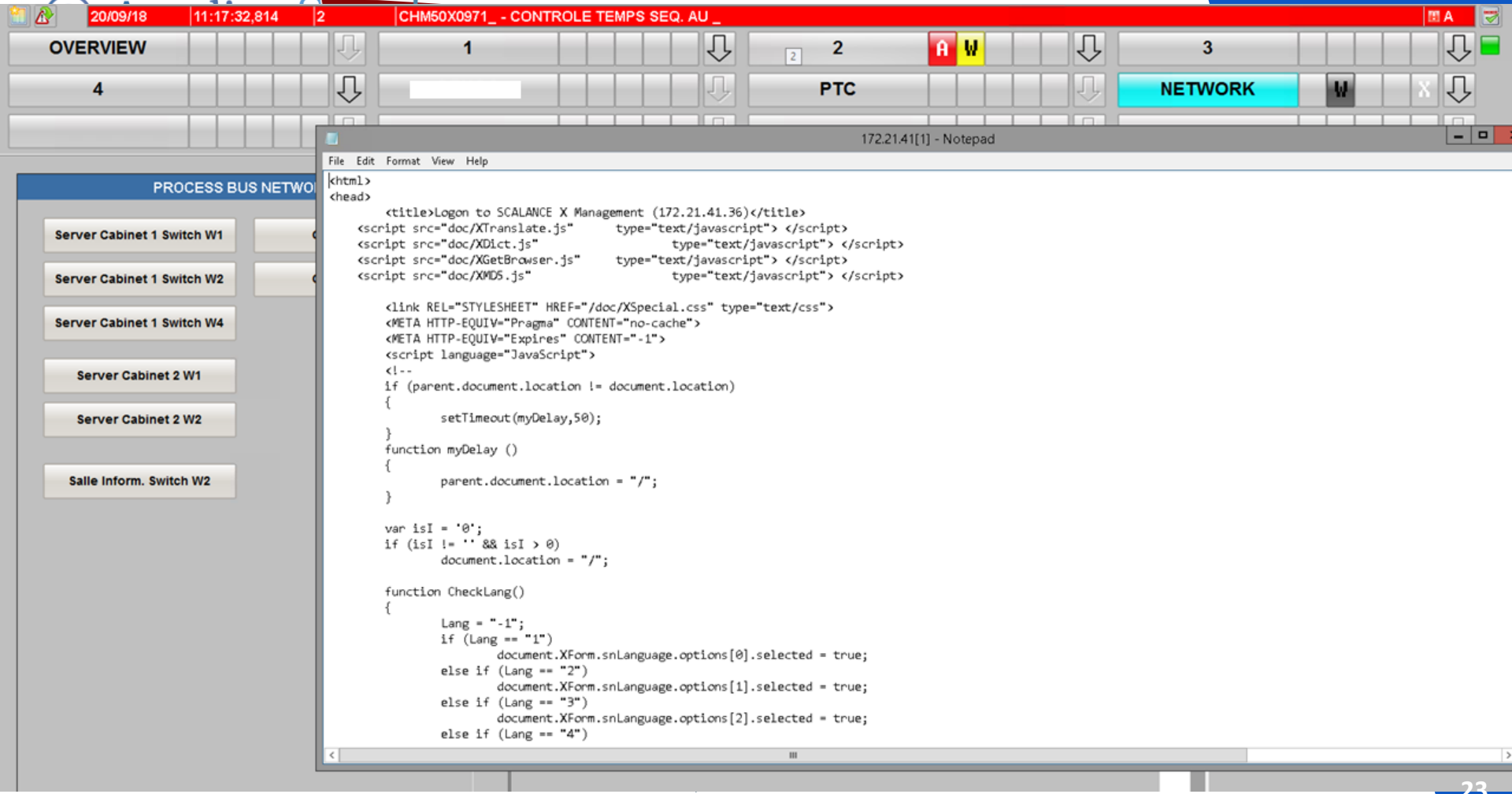
- Go to the MM8000 historic browser
- Choose to export the historic
- Click right in the new window & create a shortcut
  - Its a limited shortcut :-/
- Select “Cmd.exe” from c:\windows\system32, click right and request the properties
- Click on any link in the properties window
- Opens a windows help file

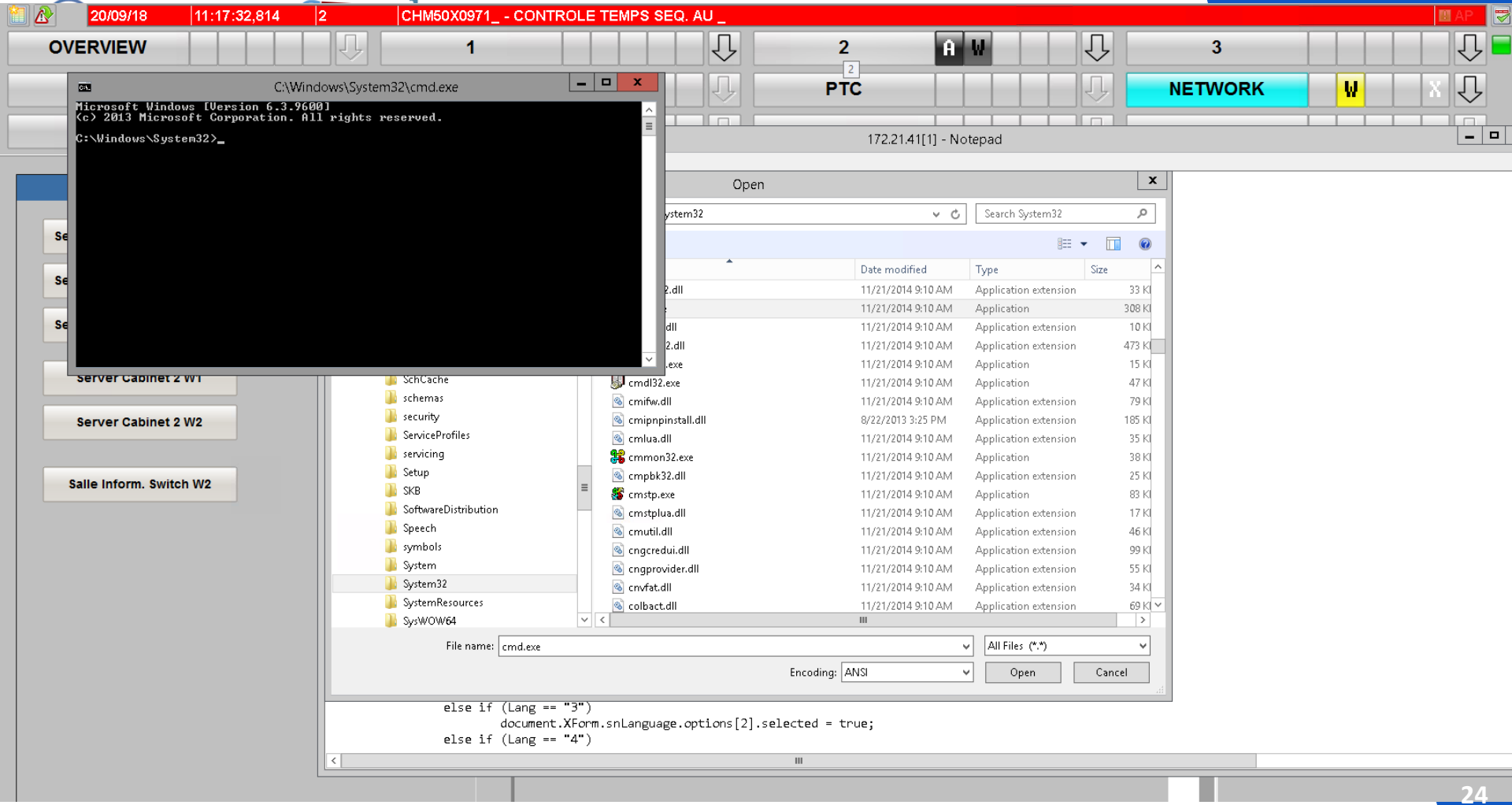
Checking operator jails … HMI Software



Checking operator jails … HMI Software

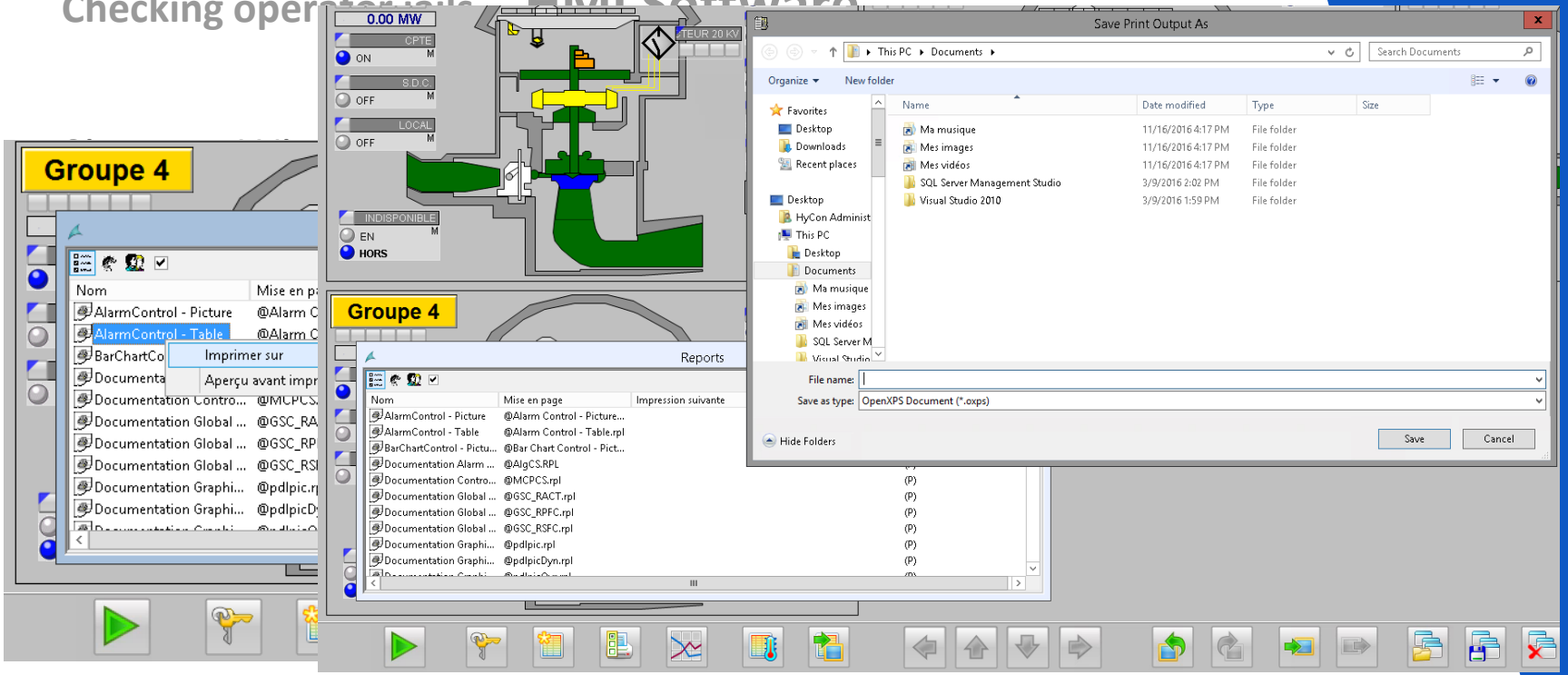



20/09/18
11:17:32,814
2
CHM50X0971_ - CONTROLE TEMPS SEQ. AU _
A
OVERVIEW
1
2
3
4
PTC
NETWORK
PROCESS BUS NETWO
Server Cabinet 1 Switch W1
Server Cabinet 1 Switch W2
Server Cabinet 1 Switch W4
Server Cabinet 2 W1
Server Cabinet 2 W2
Salle Inform. Switch W2
172.21.41[1] - Notepad
File Edit Format View Help
<html>
<head>
<title>Logon to SCALANCE X Management (172.21.41.36)</title>
<script src="doc/XTranslate.js" type="text/javascript"> </script>
<script src="doc/XDict.js" type="text/javascript"> </script>
<script src="doc/XGetBrowser.js" type="text/javascript"> </script>
<script src="doc/XMD5.js" type="text/javascript"> </script>
<link REL="STYLESHEET" HREF="/doc/XSpecial.css" type="text/css">
<META HTTP-EQUIV="Pragma" CONTENT="no-cache">
<META HTTP-EQUIV="Expires" CONTENT="-1">
<script language="JavaScript">
<!--
if (parent.document.location != document.location)
{
setTimeout(myDelay,50);
}
function myDelay ()
{
parent.document.location = "/";
}
var isI = '0';
if (isI != '' && isI > 0)
document.location = "/";
function CheckLang()
{
Lang = "-1";
if (Lang == "1")
document.XForm.snLanguage.options[0].selected = true;
else if (Lang == "2")
document.XForm.snLanguage.options[1].selected = true;
else if (Lang == "3")
document.XForm.snLanguage.options[2].selected = true;
else if (Lang == "4")


20/09/18
11:17:32,814
2
CHM50X0971_ - CONTROLE TEMPS SEQ. AU _
OVERVIEW
1
2
PTC
3
NETWORK
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Windows\System32>_
172.21.41[1] - Notepad
Server Cabinet 2 W1
Server Cabinet 2 W2
Salle Inform. Switch W2
Open
Search System32
Date modified
Type
Size
SchCache
schemas
security
ServiceProfiles
servicing
Setup
SKB
SoftwareDistribution
Speech
symbols
System
System32
SysWOW64
cmdl32.exe
cmifw.dll
cmipnpinstall.dll
cmlua.dll
cmmon32.exe
cmpbk32.dll
cmstp.exe
cmstplua.dll
cmutil.dll
cngcredui.dll
cngprovider.dll
cnvfat.dll
colbact.dll
File name: cmd.exe
All Files (*.*)
Encoding: ANSI
Open
Cancel
else if (Lang == "3")
document.XForm.snLanguage.options[2].selected = true;
else if (Lang == "4")

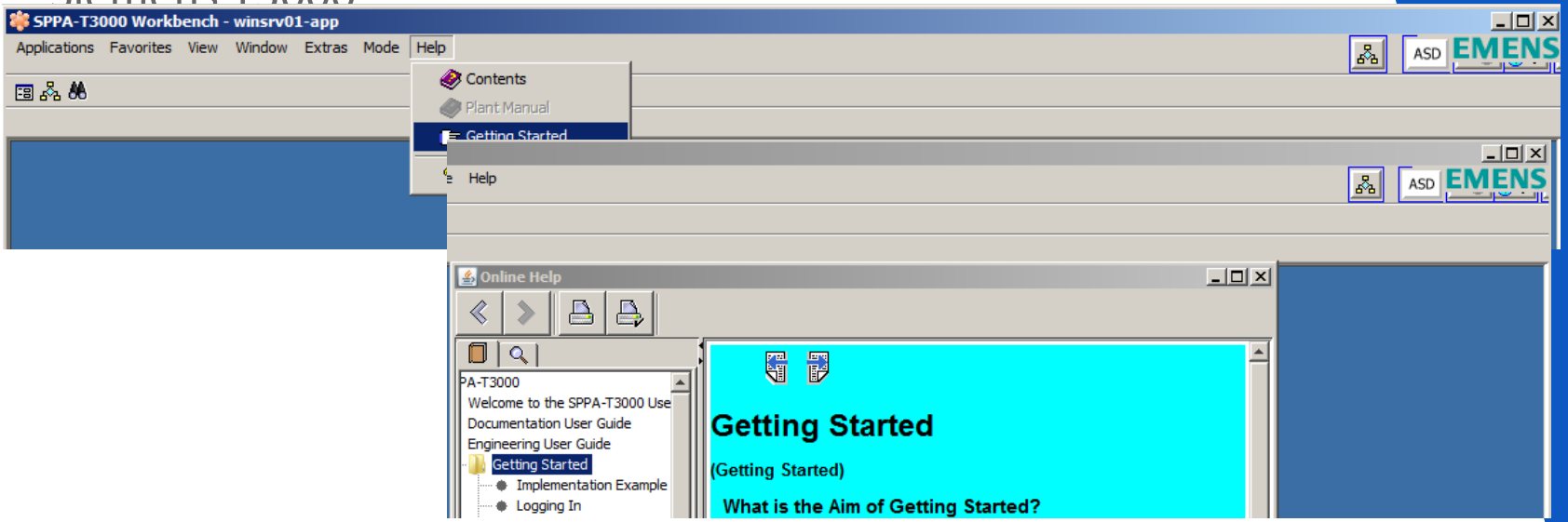
Asvalis Secudea

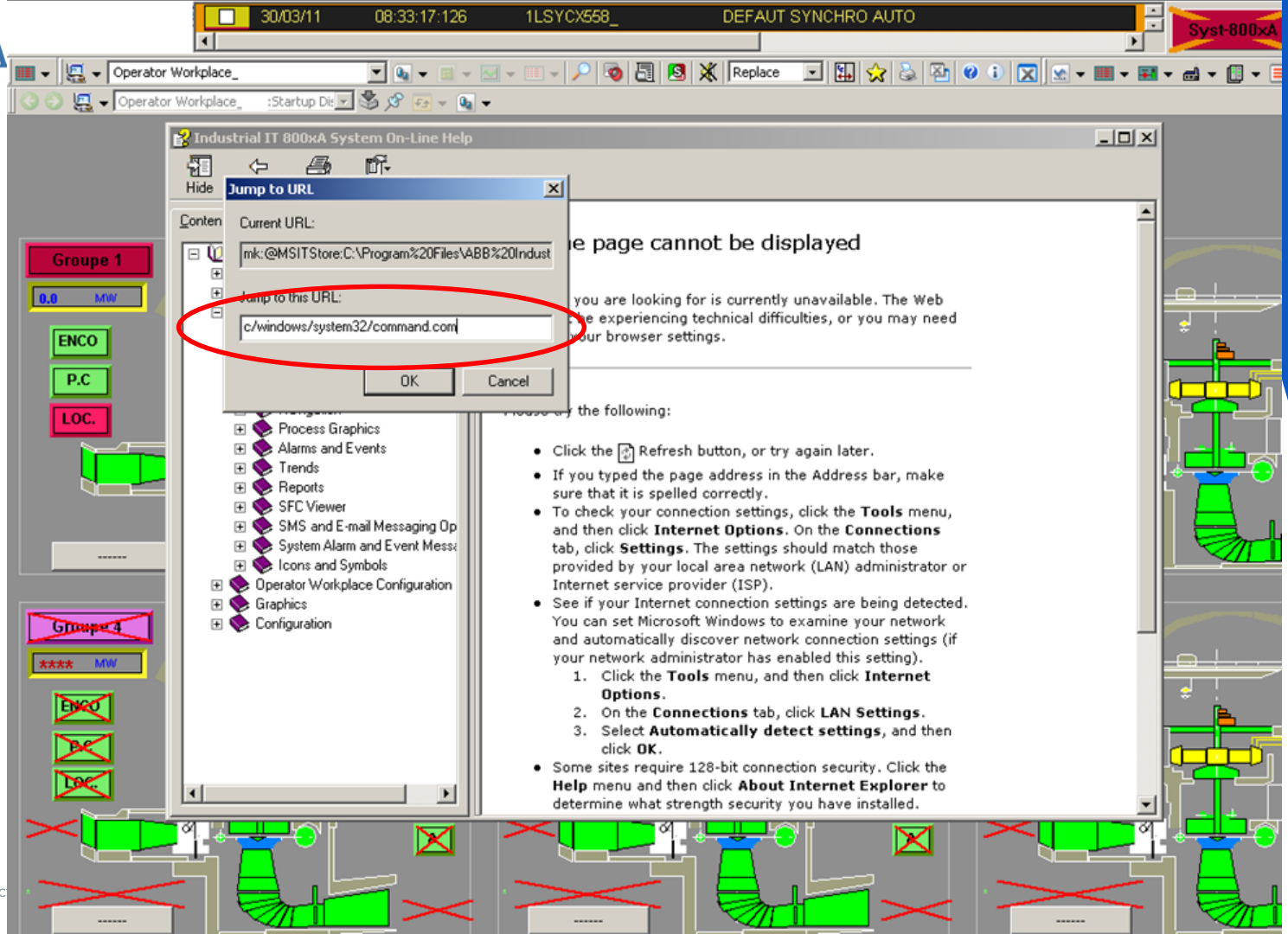
Checking operator jails HMI Software



Checking operator jails … HMI Software

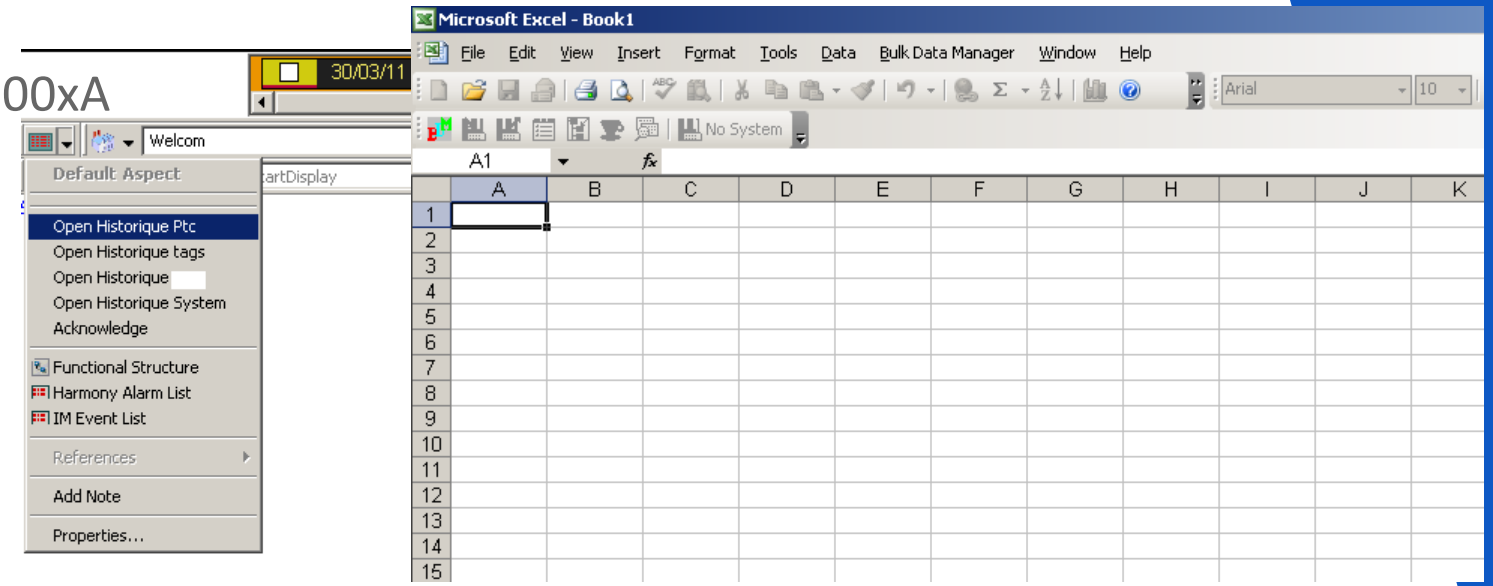
Siemens T3000

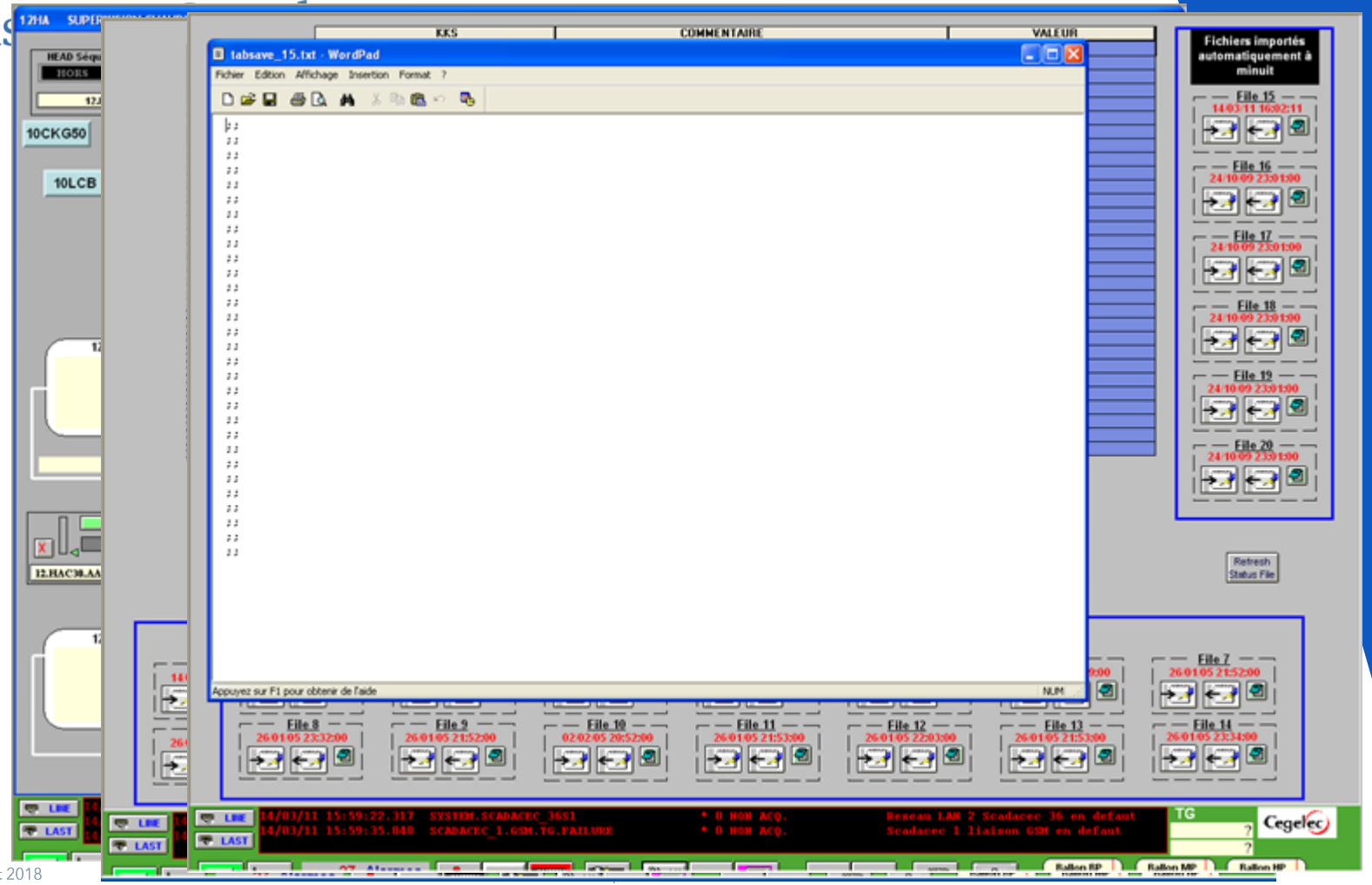



30/03/11 08:33:17:126 1LSYCX558_ DEFAUT SYNCHRO AUTO
Syst-800xA
Operator Workplace_
Replace
Operator Workplace_ :Startup Di
Industrial IT 800xA System On-Line Help
Hide
Jump to URL
Current URL:
mk:@MSITStore:C:\Program%20Files\ABB%20Indust
Jump to this URL:
c/windows/system32/command.com
OK
Cancel
Process Graphics
Alarms and Events
Trends
Reports
SFC Viewer
SMS and E-mail Messaging Op
System Alarm and Event Mess
Icons and Symbols
Operator Workplace Configuration
Graphics
Configuration
e page cannot be displayed
you are looking for is currently unavailable. The Web
e experiencing technical difficulties, or you may need
ur browser settings.
the following:
Click the Refresh button, or try again later.
If you typed the page address in the Address bar, make sure that it is spelled correctly.
To check your connection settings, click the Tools menu, and then click Internet Options. On the Connections tab, click Settings. The settings should match those provided by your local area network (LAN) administrator or Internet service provider (ISP).
See if your Internet connection settings are being detected. You can set Microsoft Windows to examine your network and automatically discover network connection settings (if your network administrator has enabled this setting).
1. Click the Tools menu, and then click Internet Options.
2. On the Connections tab, click LAN Settings.
3. Select Automatically detect settings, and then click OK.
Some sites require 128-bit connection security. Click the Help menu and then click About Internet Explorer to determine what strength security you have installed.
Groupe 1
0.0 MW
ENCO
P.C
LOC.
Groupe 4
**** MW

Checking operator jails … HMI Software

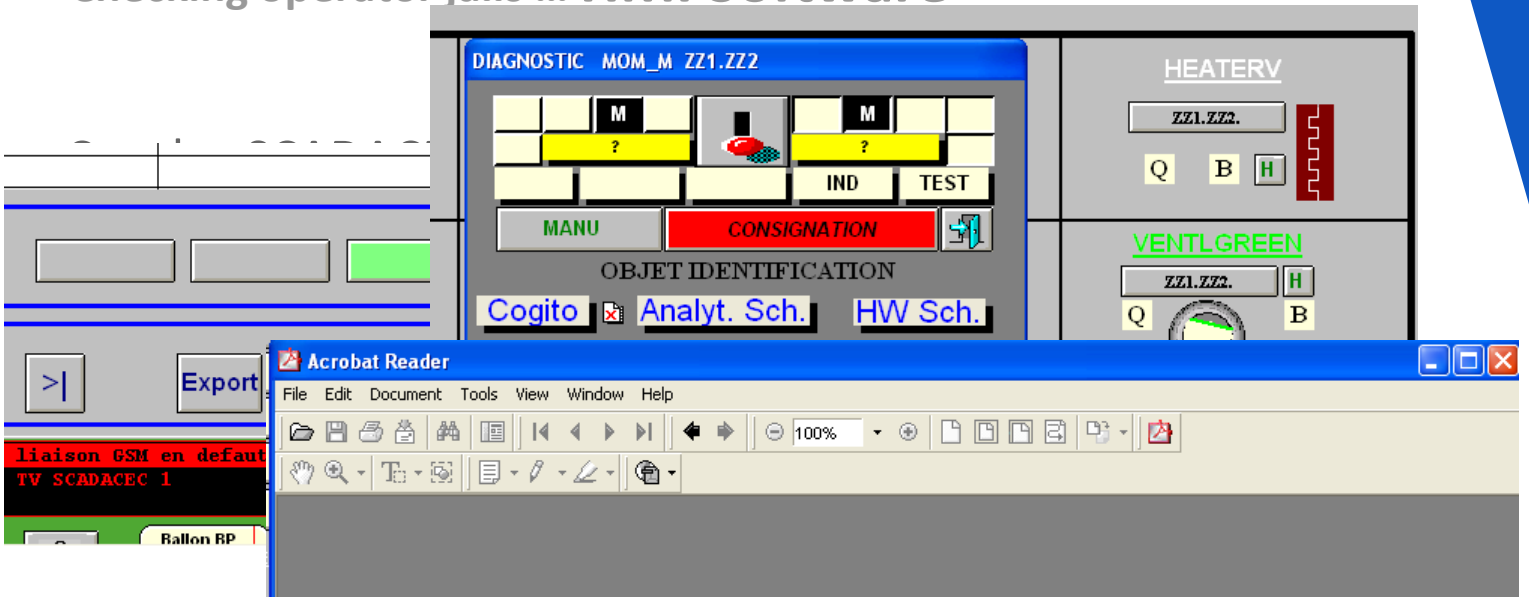
ABB 800xA




tabsave_15.txt - WordPad
Fichier Edition Affichage Insertion Format ?
Appuyez sur F1 pour obtenir de l'aide
NUM
KKS
COMMENTAIRE
VALEUR
Fichiers importés automatiquement à minuit
File 15
14/03/11 16:02:11
File 16
24/10/09 23:01:00
File 17
24/10/09 23:01:00
File 18
24/10/09 23:01:00
File 19
24/10/09 23:01:00
File 20
24/10/09 23:01:00
Refresh Status File
10CKG50
10LCB
12.HAC30.AA
File 7
26/01/05 21:52:00
File 8
26/01/05 23:32:00
File 9
26/01/05 21:52:00
File 10
02/02/05 20:52:00
File 11
26/01/05 21:53:00
File 12
26/01/05 22:03:00
File 13
26/01/05 21:53:00
File 14
26/01/05 23:34:00
14/03/11 15:59:22.317 SYSTEM.SCADACEC_36S1 * 0 NON ACQ. Reseau LAN 2 Scadacec 36 en defaut
14/03/11 15:59:35.848 SCADACEC_1.GSM.TG.FAILURE * 0 NON ACQ. Scadacec 1 liaison GSM en defaut
LINE
LAST
TG
Cegelec
Rafale RP
Rafale MP
Rafale HP

Asvalis Secudea

Checking operator jails … HMI Software



Checking operator jails … Uncommon behavior

- Crash the software
  - Overloading system
    - Opening “help” pdf 1000 times
    - Execute heavy queries
  - Unexpected input
    - Unexpected format
    - Unexpected timing (loading screens)
- Pull out network cable
- Reboot
  - Start in safe mode (works on phones as well)
  - Not advised in live environments

Protecting operator jails …

- System hardening
- Vendor fix
- Block key combo's
- Disable right-mouse click
- Implement custom print solutions
- Don't open additional soft within kiosk mode
- No notification popups …
- Restrict access to the network – restrictive firewalling
- Use Windows Applocker features


Do you have what it takes to escape?

Operator Jail breakout

Dieter Sarrazyn
dieter@secudea.be
@dietersar
https://be.linkedin.com/in/dietersarrazyn

Frank Lycops
frank@asvalis.com
https://be.linkedin.com/in/franklycops