Tetra Industrial Security

Ing. Tijl Deneut
Lecturer Applied Computer Sciences/NMCT Howest
Researcher XiaK, Ghent University

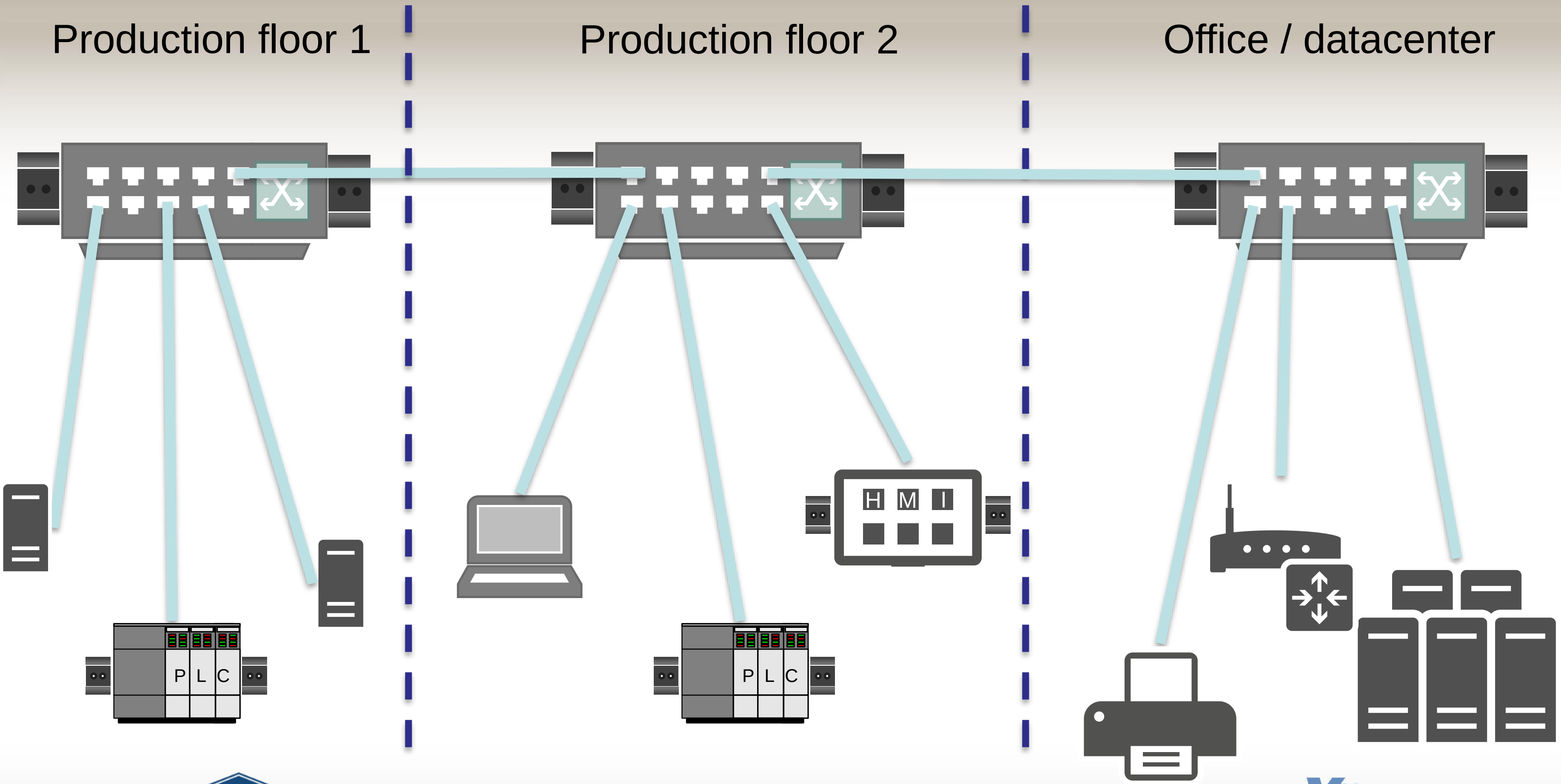
UNIVERSITEIT GENT

howest
De Hogeschool West-Vlaanderen
Lid van de Associatie Universiteit Gent

KU LEUVEN

XiaK

Demo cases



Production floor 1

Production floor 2

Office / datacenter

UNIVERSITEIT GENT

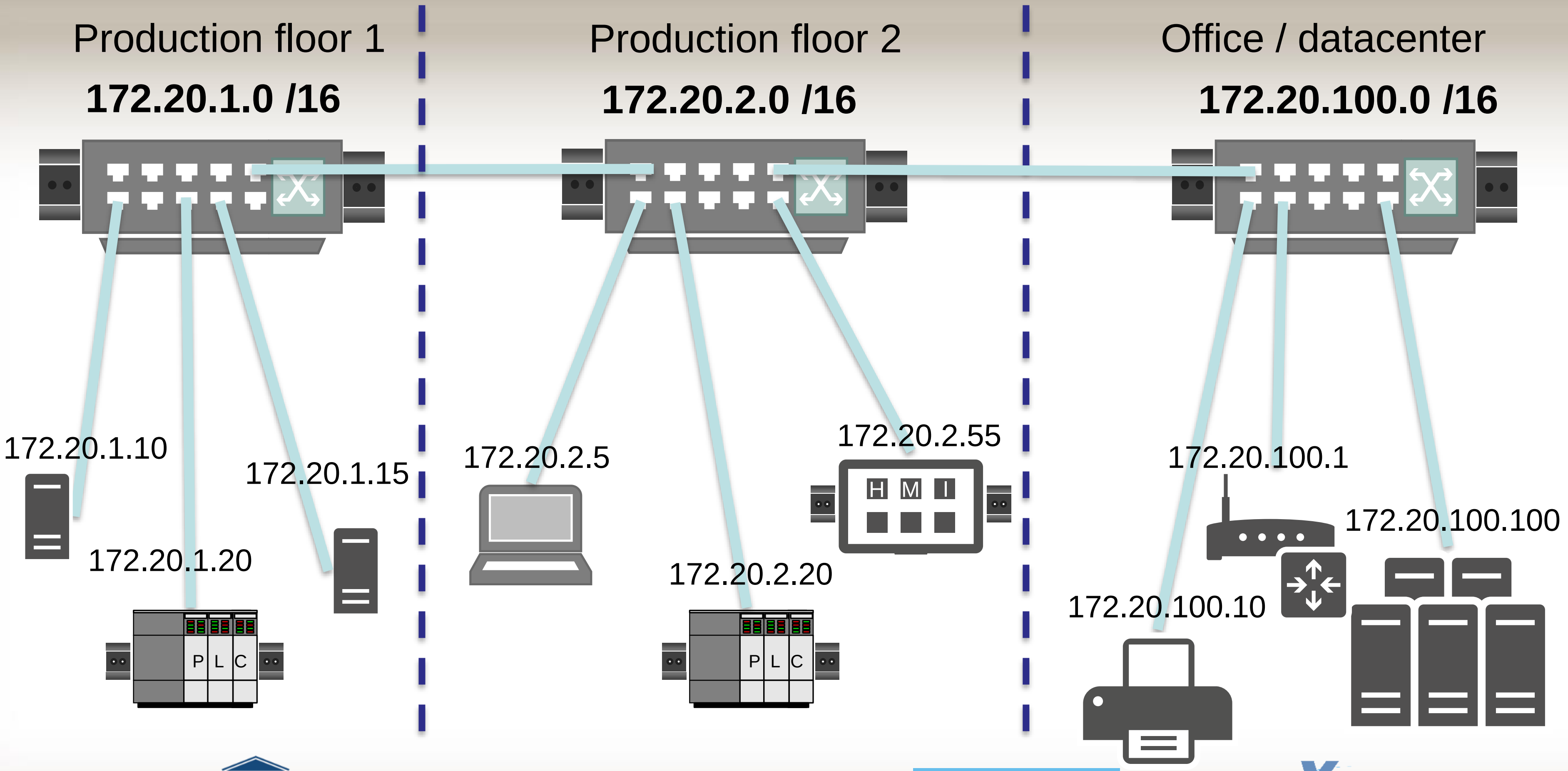
howest
De Hogeschool West-Vlaanderen
Lid van de Associatie Universiteit Gent

KU LEUVEN

Xiak

Network Example

172.20.0.0 /16



Production floor 1

172.20.1.0 /16

172.20.1.10

172.20.1.15

172.20.1.20

Production floor 2

172.20.2.0 /16

172.20.2.5

172.20.2.55

172.20.2.20

Office / datacenter

172.20.100.0 /16

172.20.100.1

172.20.100.100

172.20.100.10

UNIVERSITEIT GENT

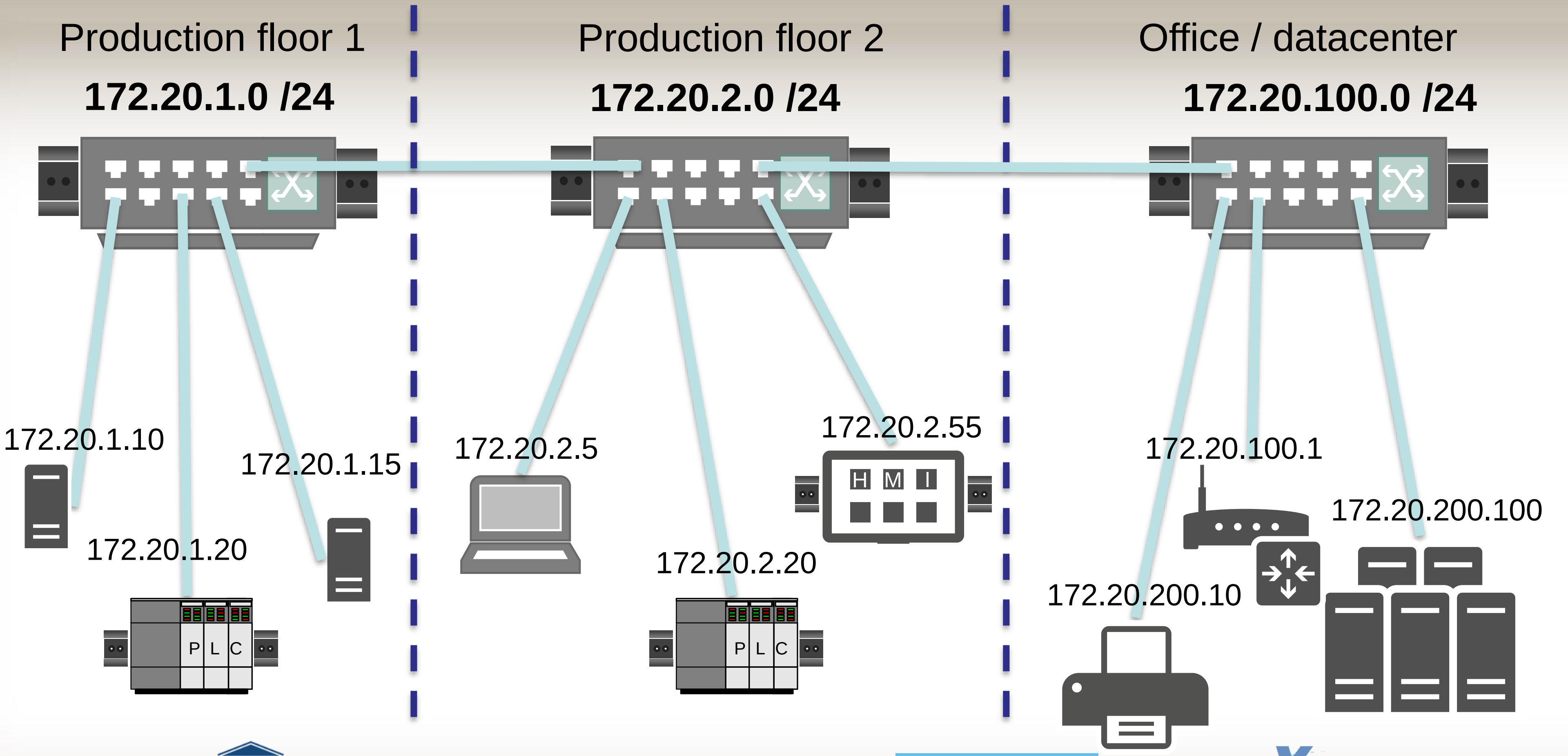
howest
De Hogeschool West-Vlaanderen
Lid van de Associatie Universiteit Gent

KU LEUVEN

Xiak

Network Example

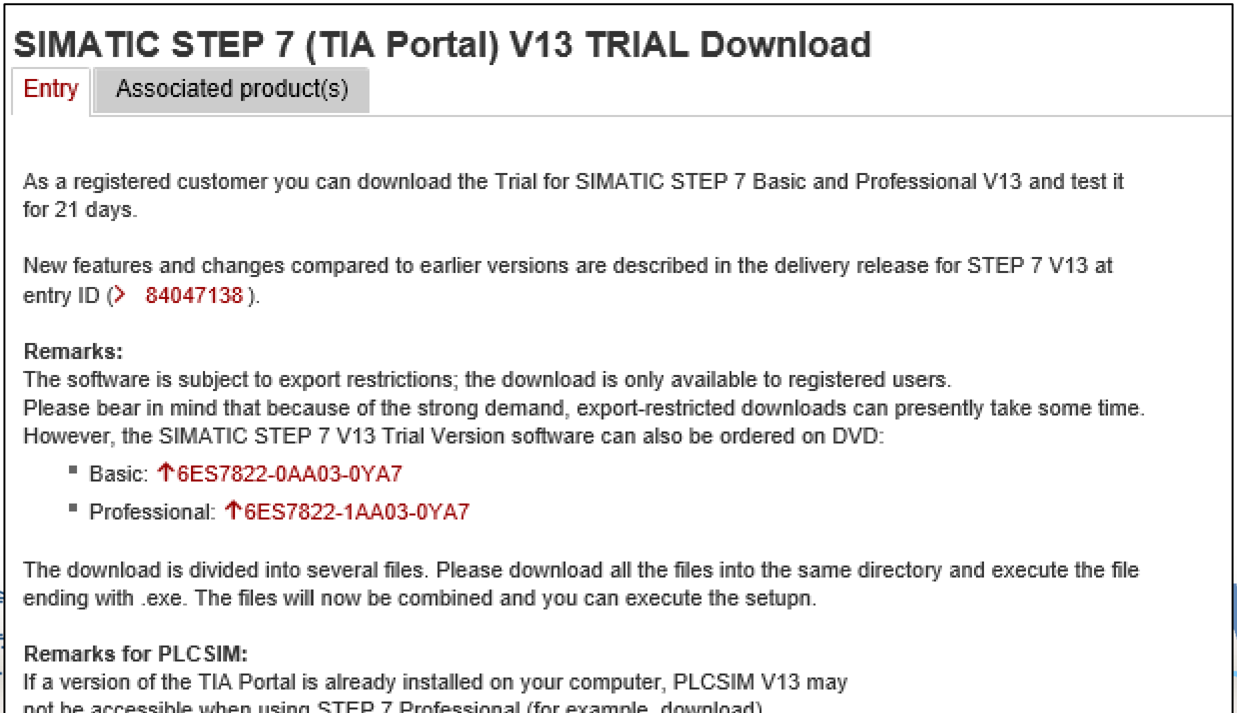
172.20.0.0 /16 but using real subnets



Siemens S7-1200 PLC

How do you program PLCs?

- In practice, quite a ‘simple’ problem
  - Everyone who has a Windows system can install the software *TIA Portal*
  - This can be downloaded as a trial here (6GB!)



SIMATIC STEP 7 (TIA Portal) V13 TRIAL Download

As a registered customer you can download the Trial for SIMATIC STEP 7 Basic and Professional V13 and test it for 21 days.

New features and changes compared to earlier versions are described in the delivery release for STEP 7 V13 at entry ID (84047138).

Remarks:
The software is subject to export restrictions; the download is only available to registered users.
Please bear in mind that because of the strong demand, export-restricted downloads can presently take some time.
However, the SIMATIC STEP 7 V13 Trial Version software can also be ordered on DVD:

- Basic: 6ES7822-0AA03-0YA7
- Professional: 6ES7822-1AA03-0YA7

The download is divided into several files. Please download all the files into the same directory and execute the file ending with .exe. The files will now be combined and you can execute the setupn.

Remarks for PLCSIM:
If a version of the TIA Portal is already installed on your computer, PLCSIM V13 may not be accessible when using STEP 7 Professional (for example, download).

TIA Portal

- In TIA Portal it is only a matter of creating an empty project, configuring the PLC IP address and start controling the PLC
- **NO AUTHENTICATION POSSIBLE**

- So what did we do?
  - We intercepted all traffic and (tried to) understand the protocol
  - After which we just programmed a tool (again in Python)

Protocol results

- All PLC scanning is done on **Layer2** (so only MAC addresses) using a protocol called Profinet-DCP
  - So we wrote a scanner
- This same protocol is used to **configure** things like IP addresses
- Then a proprietary protocol is used (S7Comm) on TCP Port 102 to get more information
  - **And to read and set outputs**

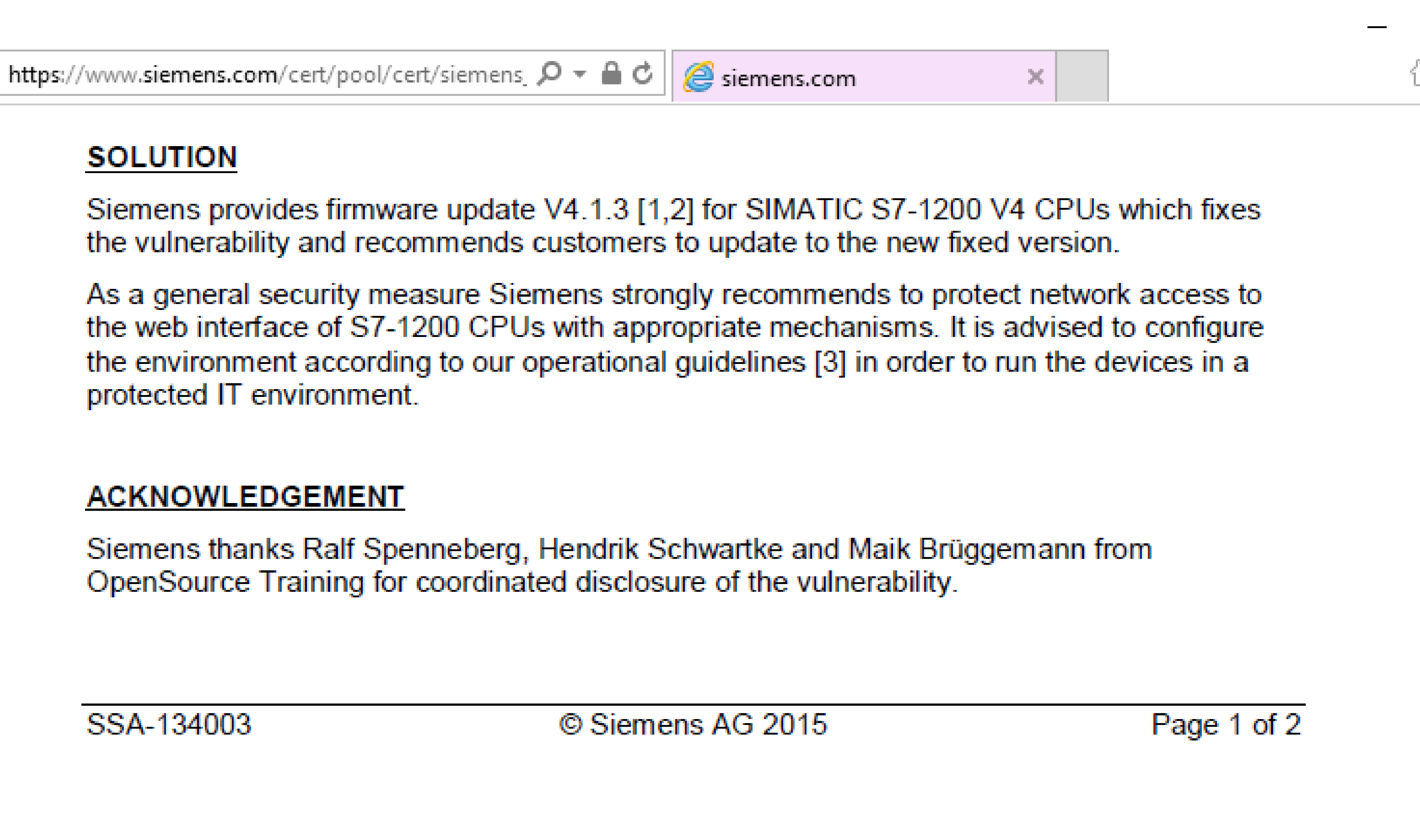
Demo Siemens PLC S7-1200

Solution?

- Firmware v3.1 adds authentication, but this firmware **does not exist** for this particular PLC
  - Furthermore, it is disabled by default

- Best solution: secure your network

- Or as Siemens puts it:



SOLUTION

Siemens provides firmware update V4.1.3 [1,2] for SIMATIC S7-1200 V4 CPUs which fixes the vulnerability and recommends customers to update to the new fixed version.

As a general security measure Siemens strongly recommends to protect network access to the web interface of S7-1200 CPUs with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks Ralf Spenneberg, Hendrik Schwartke and Maik Brüggemann from OpenSource Training for coordinated disclosure of the vulnerability.

SSA-134003 © Siemens AG 2015 Page 1 of 2