Control-System Cyber-Security (CS)^2

- ►The Fact: Controls goes IT
- ►The Problem: No Inherent PLC Security
- ►The Mitigation: You, CNIC and CERN

Stefan.Lueders@cern.ch (CERN IT/CO)
ATC/ABOC Days – January 22nd, 2007

Controls goes IT

► Controls networks mate business networks

- Proprietary field busses (PROFIBUS, Modbus)
  replaced by Ethernet & TCP/IP (PROFINET, Modbus/TCP)
- PLCs & field devices connect directly to Ethernet & TCP/IP
- Real time applications based on TCP/IP

► Use of IT protocols & gadgets:

- eMailing, FTP, Telnet, HTTP (WWW), … directly from the PLC

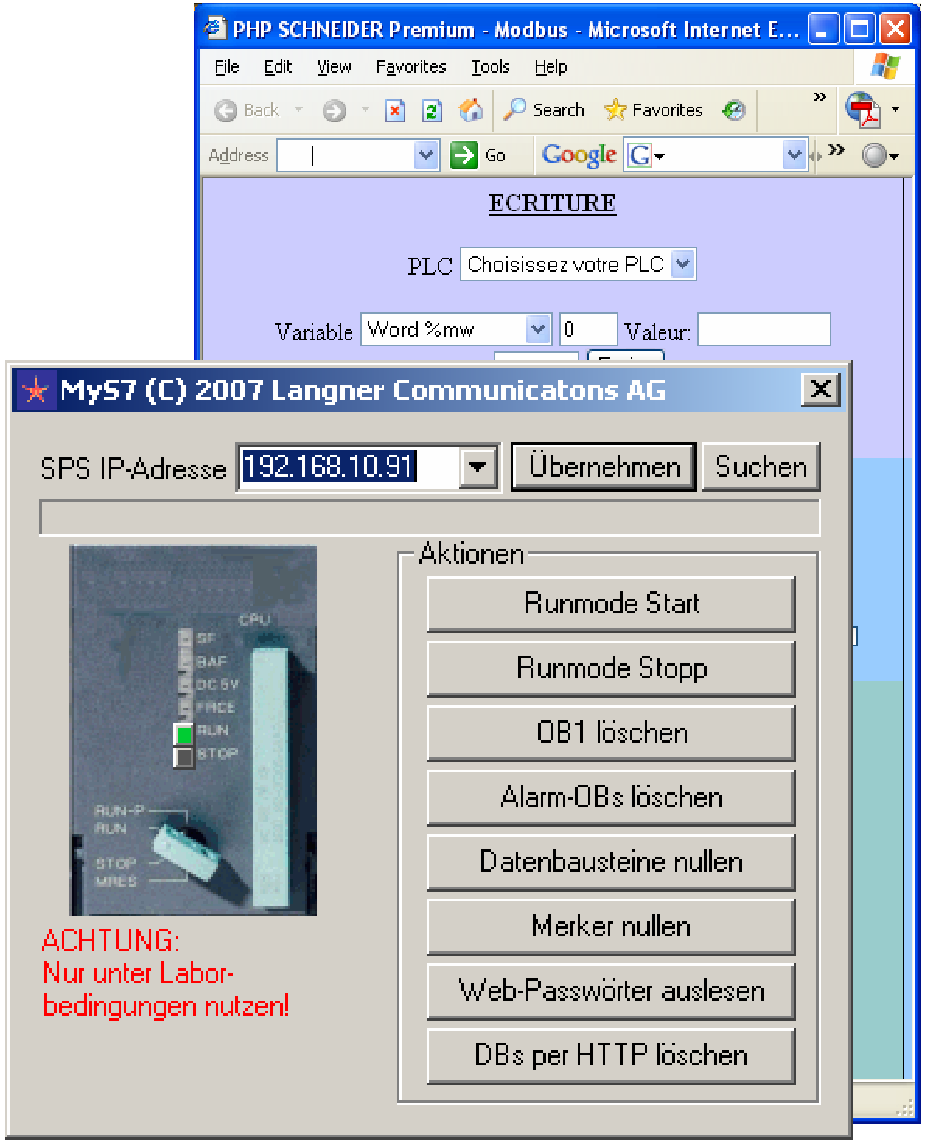
► Migration to the Microsoft Windows platform

- STEP7, PL7 Pro, UNITY, WINCC, …
- Windows not designed for Industrial / Control Systems
- OPC/DCOM runs on port 135 (heavily used for RPC)

Attacking PLCs

- I can stop *any* PLC at CERN.
- I can modify its contents.
- I just need
  an Ethernet connection to it.

- I (engineer, operator)
  might have finger-trouble.
- I (virus)
  do not care that it's a PLC.
- I (attacker)
  might do this on purpose.



PHP SCHNEIDER Premium - Modbus - Microsoft Internet E...

ECRITURE

PLC: Choisissez votre PLC

Variable: Word %mw 0 Valeur:

MyS7 (C) 2007 Langner Communicatons AG

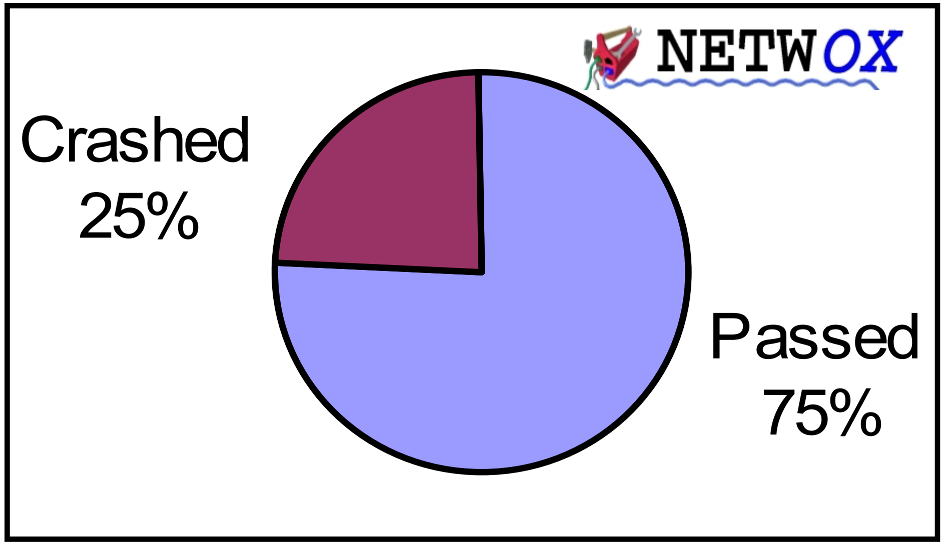
SPS IP-Adresse: 192.168.10.91

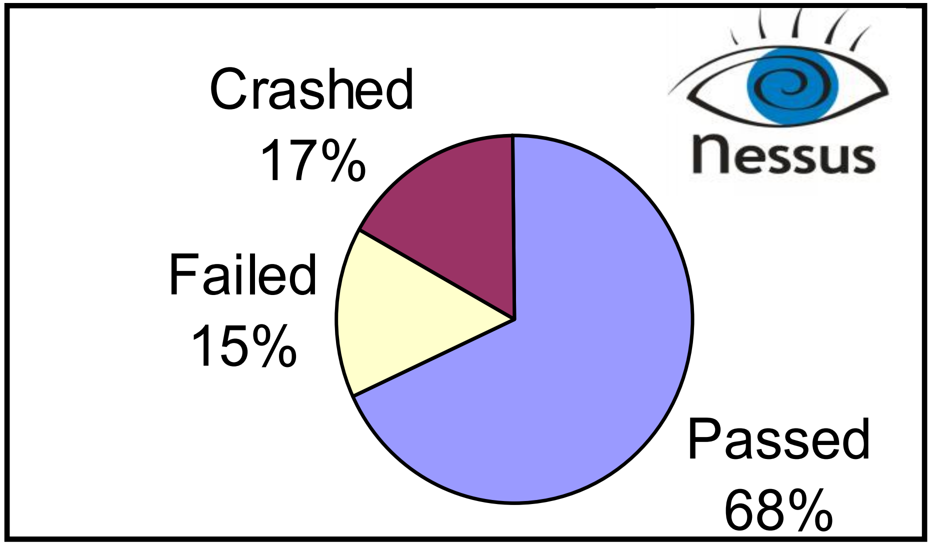
ACHTUNG:
Nur unter Labor-
bedingungen nutzen!

TOCSSiC: PLCs under Attack !

► 31 devices from 7 different manufacturers **(53 tests in total)**

► All devices fully configured <u>but running idle</u>



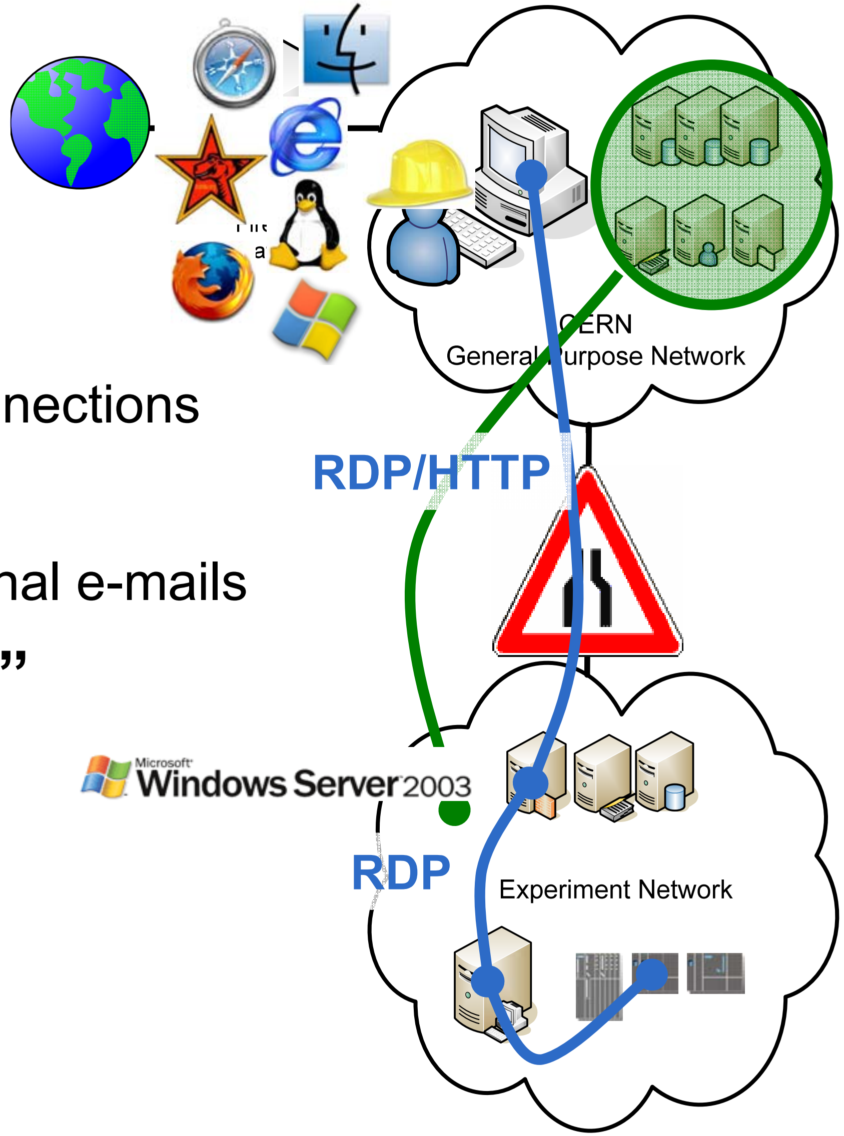


► ***…PLCs <u>under load</u> seem to** fail even more likely **!!!***

► ***…**results improve **with more recent firmware versions** ☺*

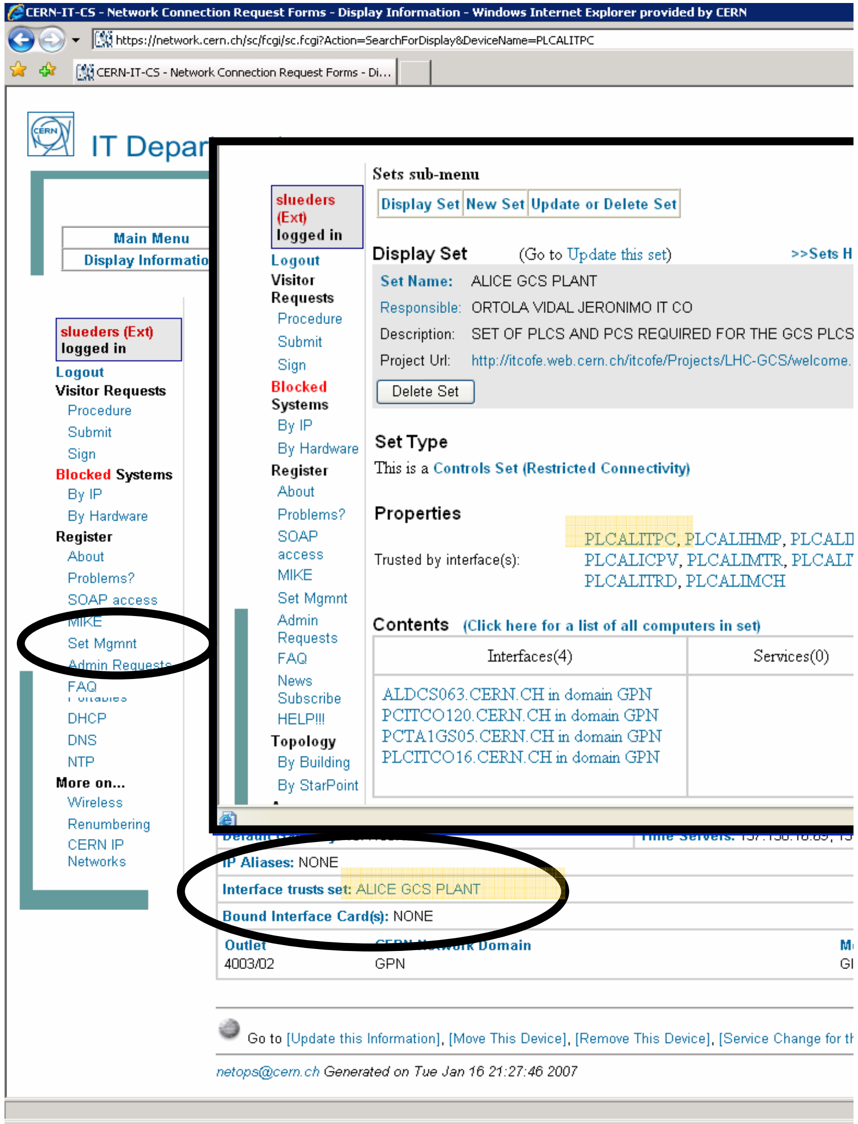
CNIC Network Segregation

- **Technical Network (TN)**
  - Domain Manager with technical responsibility
  - Only operational devices (development & testing on GPN)
  - Authorization procedure for new connections
- **Restricted connectivity**
  - No Internet web-browsing, no personal e-mails
- **Essential services are “trusted”**
  - DFS, NTP, Oracle, Castor, …
- **Remote access from “office”, “home”, “wireless”**
  - Using Terminal Servers
  - Keep engineering-station on TN



Your LANDB “Control Sets”

- **Restrict connectivity defined on a per-device level…**
- **…to a sub-set of devices**
  - engineering stations
  - SCADA terminals
  - other PLCs
- **Implemented inside the TN routing**



Display Set (Go to Update this set) >>Sets H

Set Name: ALICE GCS PLANT

Responsible: ORTOLA VIDAL JERONIMO IT CO

Description: SET OF PLCS AND PCS REQUIRED FOR THE GCS PLCS

Project Url: http://itcofe.web.cern.ch/itcofe/Projects/LHC-GCS/welcome.

Set Type

This is a Controls Set (Restricted Connectivity)

Properties

Trusted by interface(s): PLCALITPC, PLCALIHMP, PLCALI PLCALICPV, PLCALIMTR, PLCALI PLCALITRD, PLCALIMCH

Contents (Click here for a list of all computers in set)

Interfaces(4)	Services(0)
ALDCS063.CERN.CH in domain GPN PCITCO120.CERN.CH in domain GPN PCTA1GS05.CERN.CH in domain GPN PLCITCO16.CERN.CH in domain GPN	

IP Aliases: NONE

Interface trusts set: ALICE GCS PLANT

Bound Interface Card(s): NONE

Outlet	CERN Network Domain	M
4003/02	GPN	GI

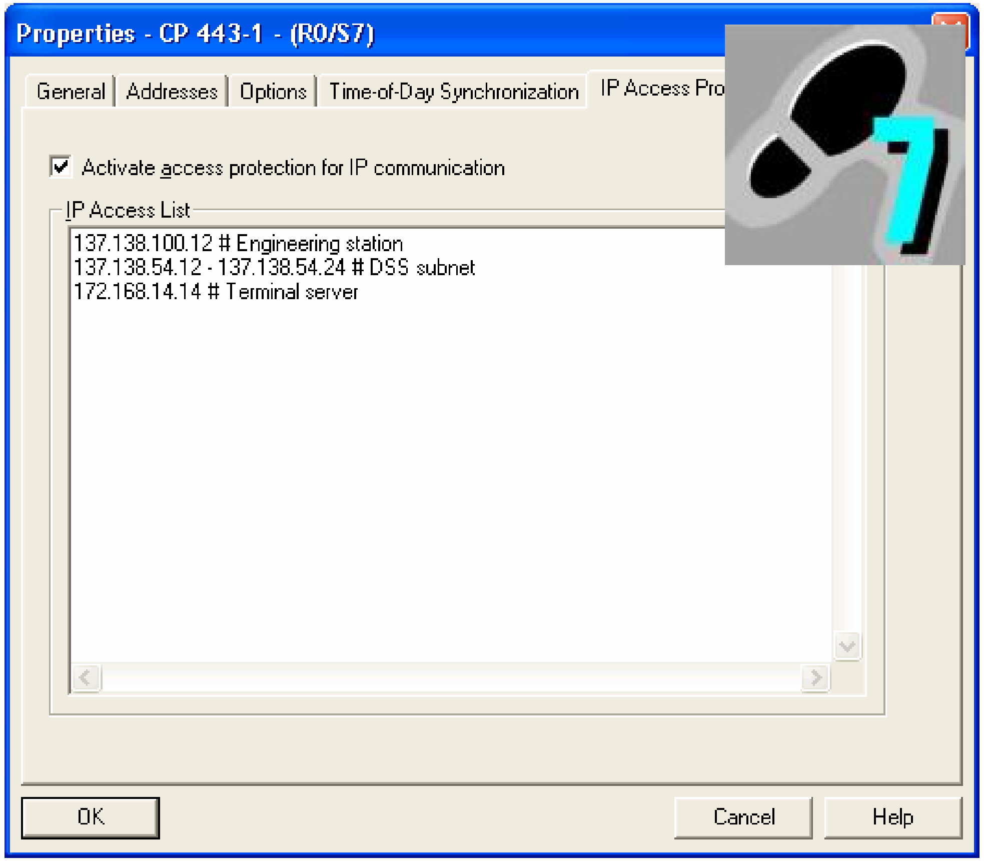
Go to [Update this Information], [Move This Device], [Remove This Device], [Service Change for th

netops@cern.ch Generated on Tue Jan 16 21:27:46 2007

Your PLC “IP Access Protection”

► Restrict communication partners

- Possible through Siemens STEP7, Schneider PL7 Pro & UNITY
- Permit access to IP addresses and address ranges

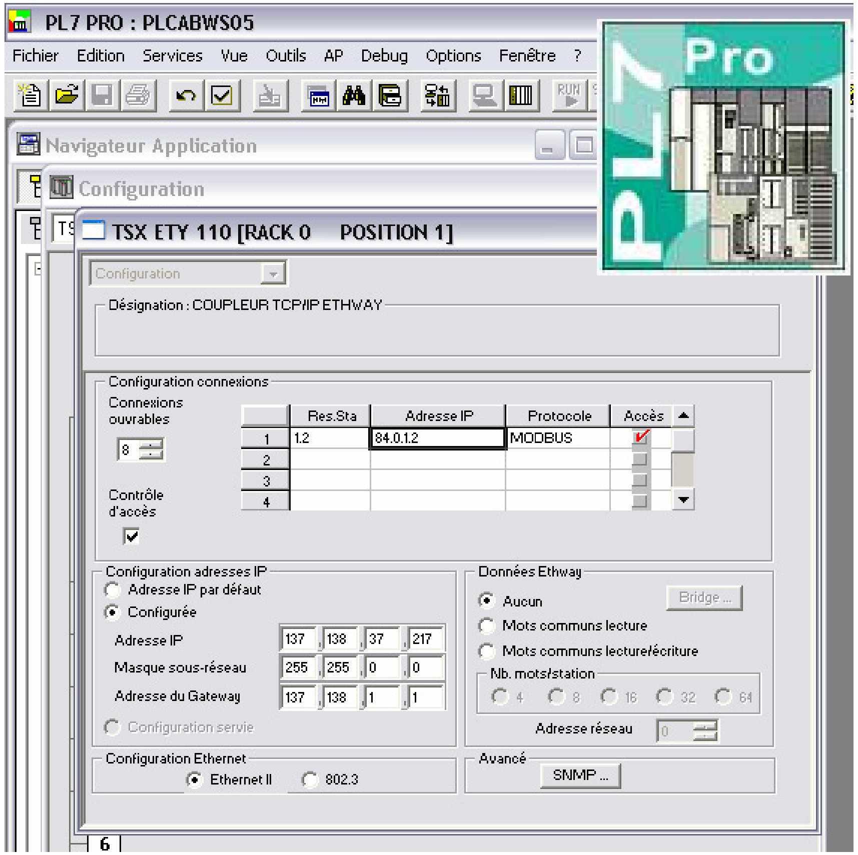


Properties - CP 443-1 - (R0/S7)

☑ Activate access protection for IP communication

IP Access List

```
137.138.100.12 # Engineering station
137.138.54.12 - 137.138.54.24 # DSS subnet
172.168.14.14 # Terminal server
```



PL7 PRO : PLCABWS05

TSX ETY 110 [RACK 0 POSITION 1]

Configuration

Désignation : COUPLEUR TCP/IP ETHWAY

Configuration connexions

Connexions ouvrables: 8

Contrôle d'accès: ☑

	Res.Sta	Adresse IP	Protocole	Accès
1	1.2	84.0.1.2	MODBUS	☑
2				□
3				□
4				□

Configuration adresses IP
○ Adresse IP par défaut
● Configurée
Adresse IP: 137 . 138 . 37 . 217
Masque sous-réseau: 255 . 255 . 0 . 0
Adresse du Gateway: 137 . 138 . 1 . 1
○ Configuration servie

Données Ethway
● Aucun
○ Mots communs lecture
○ Mots communs lecture/écriture
Nb. mots/station: ○ 4 ○ 8 ○ 16 ○ 32 ○ 64
Adresse réseau: 0

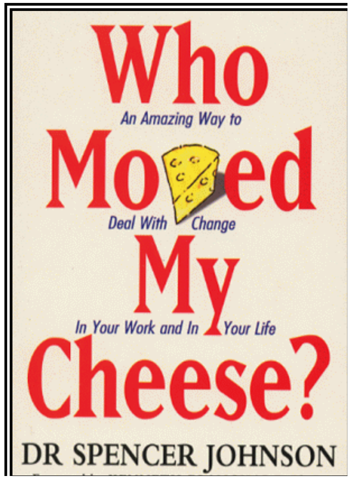
Configuration Ethernet: ● Ethernet II ○ 802.3

Avancé

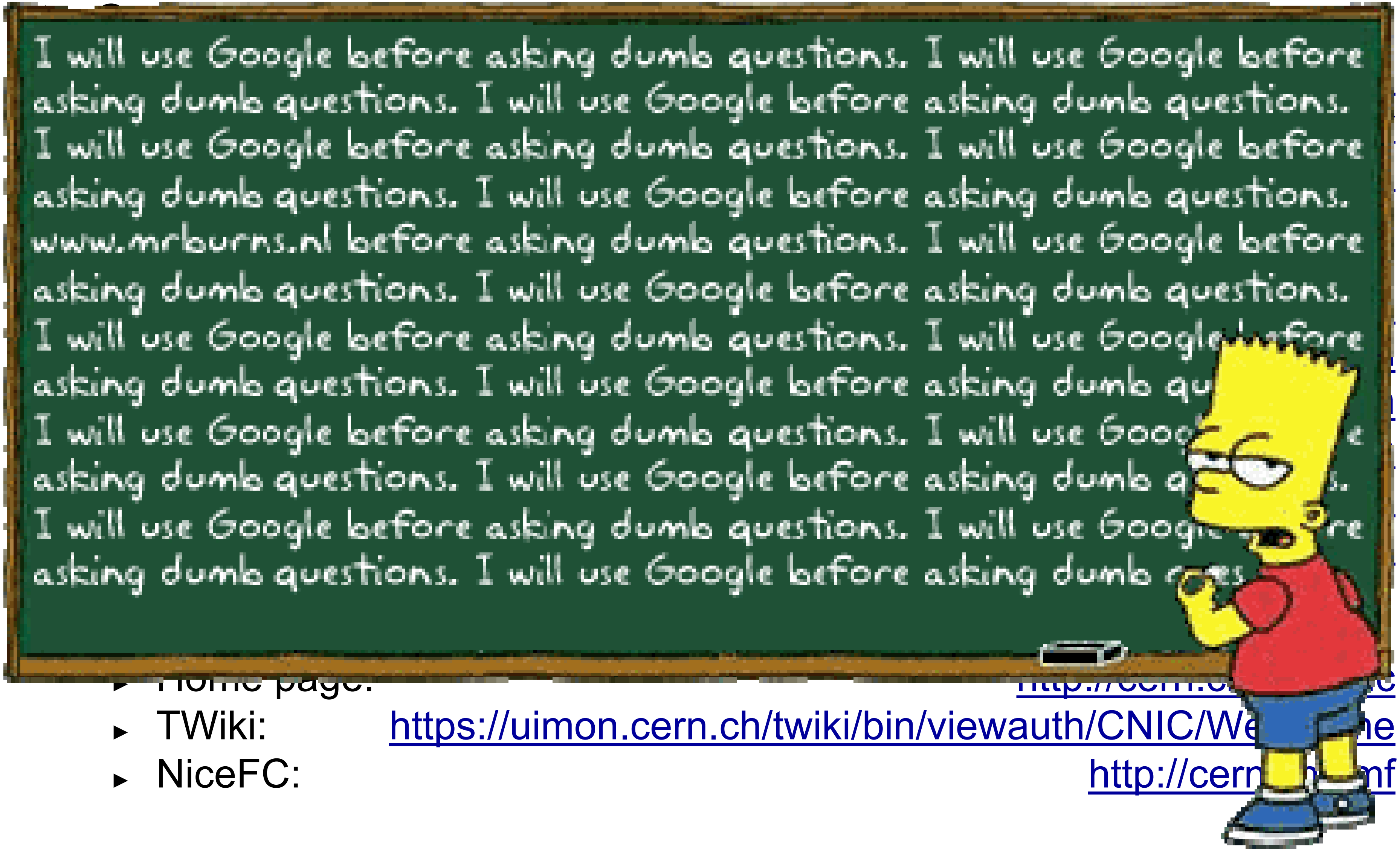
Summary

- **PLCs are interconnected to the Ethernet**
- **PLCs have no inherent security**
  - Use most recent firmware versions to improve
- **The CNIC & the TN provide some mitigation**
  - Use “Control Sets”
- **The PLC provides some mitigation**
  - Use “IP Access Protection”
- **By-the-way: Protect your Windows PCs — use CMF !!!**

Do you want to act BEFORE or AFTER the incident ?



Thank you very much !


I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
www.mrburns.nl before asking dumb questions. I will use Google before
asking dumb questions. I will use Google before asking dumb questions.
I will use Google before asking dumb questions. I will use Googl efore
asking dumb questions. I will use Google before asking dumb qu
I will use Google before asking dumb questions. I will use Goog e
asking dumb questions. I will use Google before asking dumb q s.
I will use Google before asking dumb questions. I will use Goog re
asking dumb questions. I will use Google before asking dumb ques

- Home page: http://cern.c e
- TWiki: https://uimon.cern.ch/twiki/bin/viewauth/CNIC/We me
- NiceFC: http://cern mf