POSITIVE HACK DAYS VI

POSITIVE TECHNOLOGIES

phdays.ru

Positive Hack Days VI: Кто мы такие

POSITIVE TECHNOLOGIES

Илья Карпов ikarpov@ptsecurity.com

- Эксперт отдела анализа защищенности
- >5 лет работы с системами АСУ ТП
- Исследователь
- Организатор международного форума PHDays

Дружинин Евгений edruzhinin@ptsecurity.com

- Эксперт отдела анализа защищенности
- > 10 лет в ИБ
- Исследователь
- Организатор международного форума PHDays

Какой-то бородатый мужик справа

Positive Hack Days VI - Итоги

POSITIVE TECHNOLOGIES

4,2 тыс участников

75 докладов

8 мастер-классов

Атаки и защита на реальных макетах:

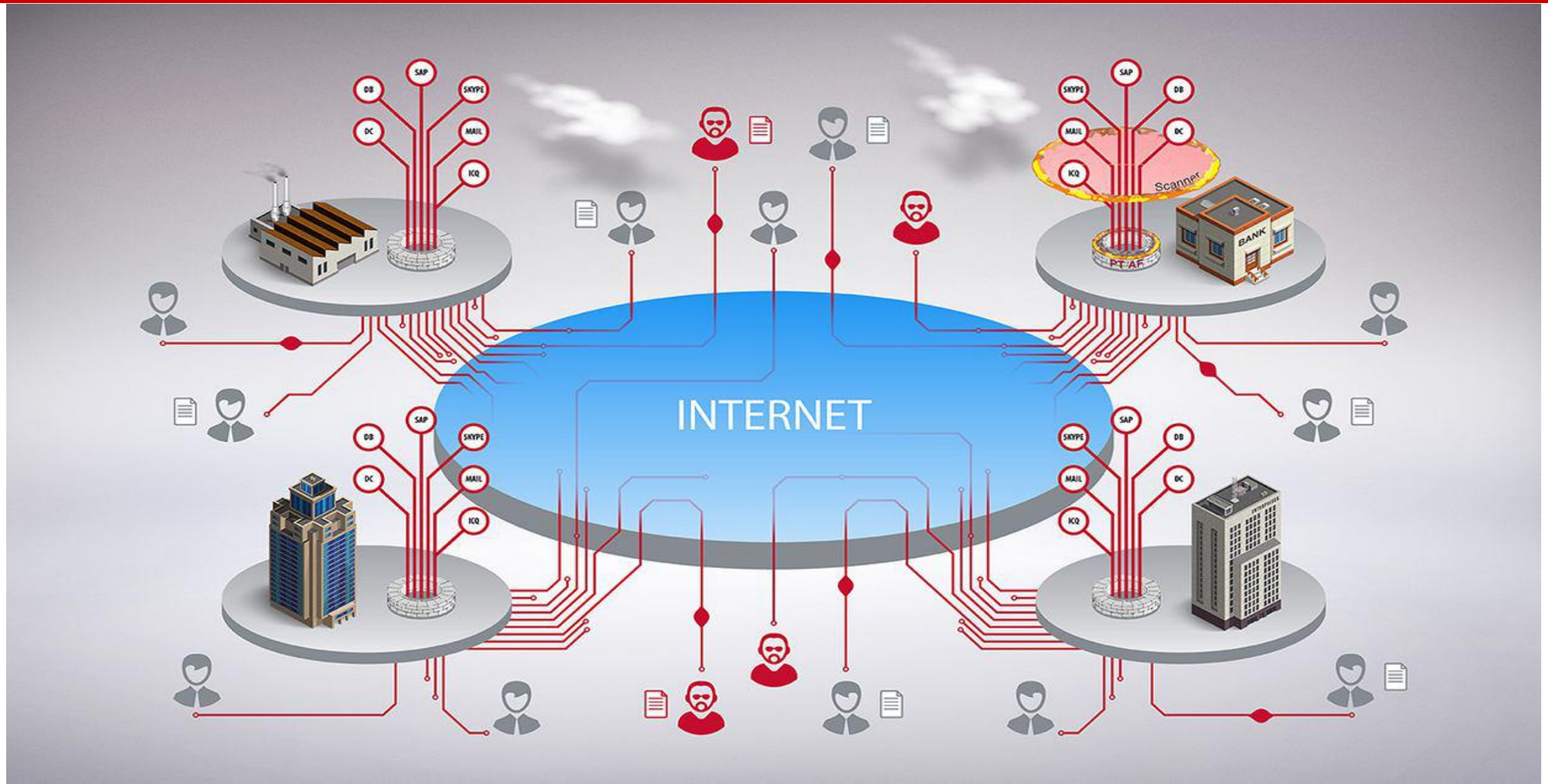
- Гидроэлектростанция
- Распределительные подстанции
- Умный дом
- Железная дорога
- Сотовая вышка
- Дроны

Новый формат конкурсов «противостояние»:

- 16 команд нападающих
- 5 команд защитников
- 3 внешних SOC
- Десятки отдельных нападающих и
- 1 школьник

Positive Hack Days VI: Архитектура сети

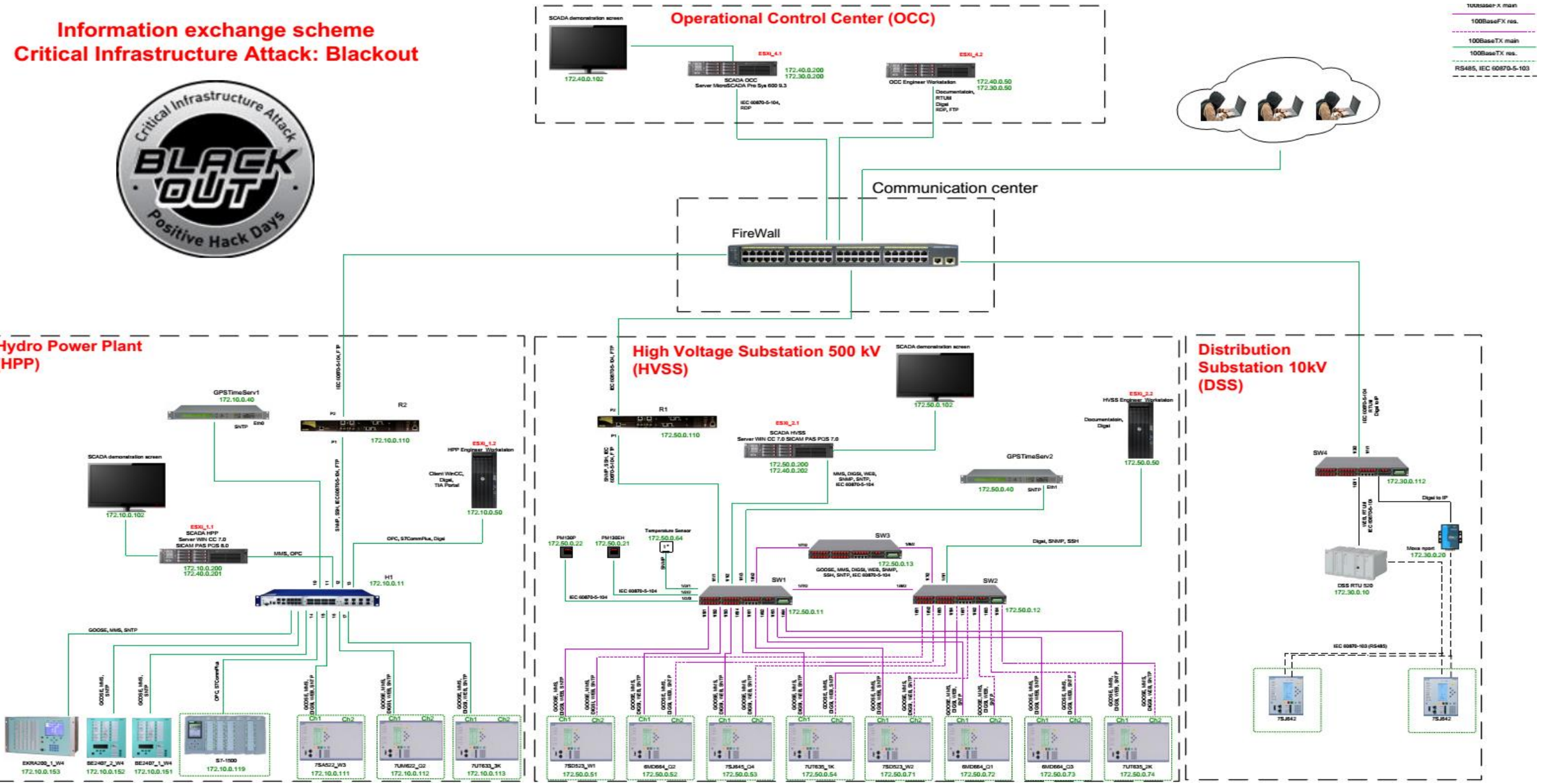
POSITIVE TECHNOLOGIES



Максимально реалистичный макеты:

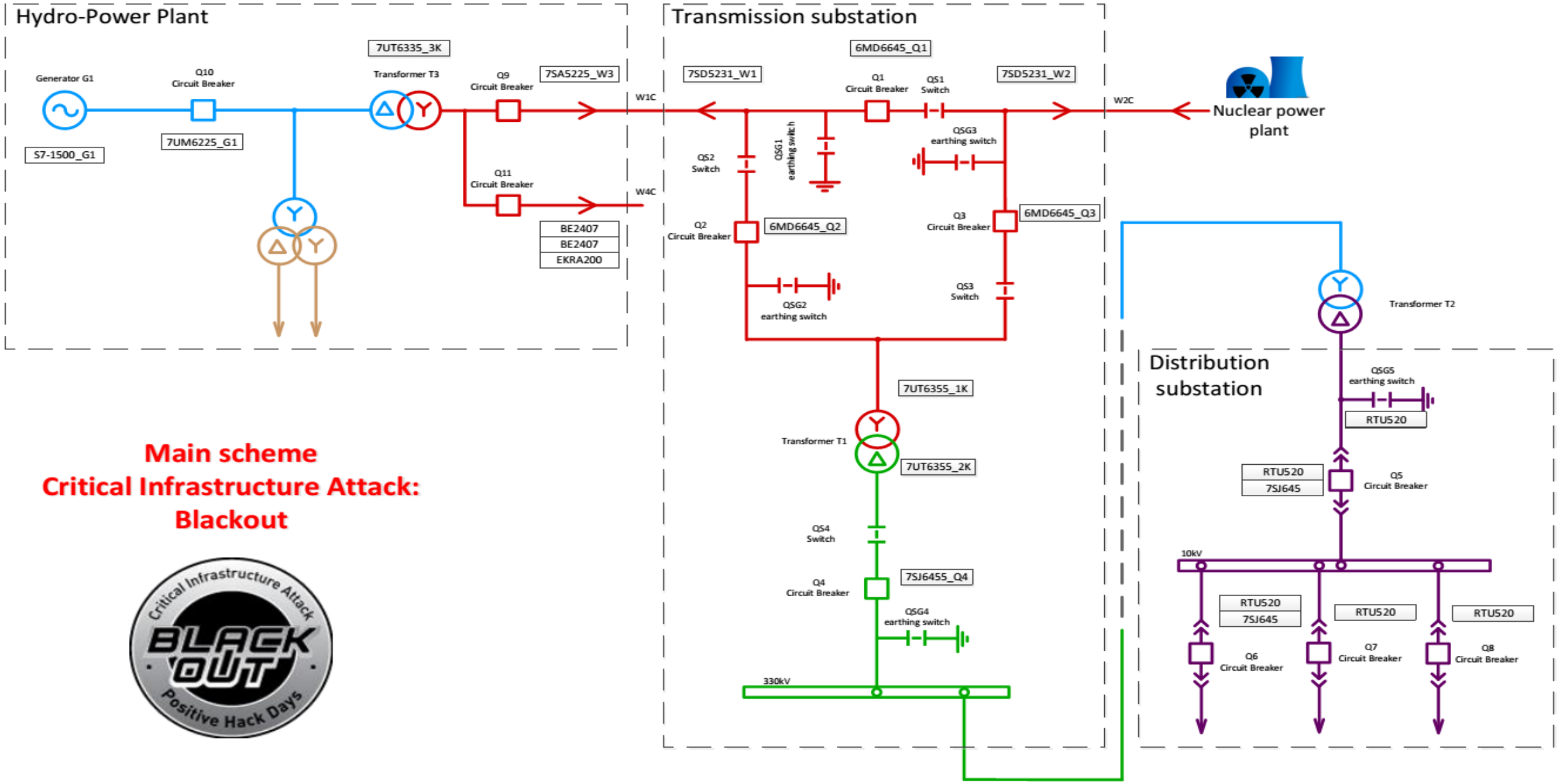
- **Генерация**
- **Передача**
- **Распределение**
- **Управление электроснабжением и системы автоматики «умного» дома**

- Терминалы РЗА **Siemens Siprotec 4**, **ЭКРА** серии **200** и **БЭ**
- Терминал удалённого управления **ABB RTU520**
- ПЛК **Siemens Simatic S7-1500** серии
- SCADA системы **Siemens WinCC 7**ой серии
- SICAMPAS серверы **7-8** версии и **ABB MicroScada SYS600**
- Инженерное ПО **Siemens DIGSI4** и **ABB RTUtil 500**
- ПЛК **Loxone MiniServer** и **Schneider Modicon M168** BacnetIP
- ПЛК **Advantech ADAM-3600** и **APAX-5580**, модуль **ADAM 6000**
- Сетевое оборудование, сервер времени…


Information exchange scheme
Critical Infrastructure Attack: Blackout
Critical Infrastructure Attack
BLACK OUT
Positive Hack Days
Operational Control Center (OCC)
SCADA demonstration screen
172.40.0.102
SCADA OCC
Server MicroSCADA Pro Sys 600 9.3
172.40.0.200
172.30.0.200
OCC Engineer Workstation
172.40.0.50
172.30.0.50
Communication center
FireWall
Hydro Power Plant (HPP)
GPSTimeServ1
172.10.0.40
R2
172.10.0.110
SCADA demonstration screen
172.10.0.102
SCADA HPP
Server WIN CC 7.0 SICAM PAS PCS 8.0
172.10.0.200
172.40.0.201
HPP Engineer Workstation
172.10.0.50
H1
172.10.0.11
MMS, OPC
OPC, S7CommPlus, Digsi
GOOSE, MMS, SNTP
S7-1500
172.10.0.119
75A522_W3
172.10.0.111
7UM622_Q2
172.10.0.112
7UT633_3K
172.10.0.113
EXR4200_1_W4
172.10.0.153
BE2407_2_W4
172.10.0.152
BE2407_1_W4
172.10.0.151
High Voltage Substation 500 kV (HVSS)
SCADA demonstration screen
172.50.0.102
R1
172.50.0.110
SCADA HVSS
Server WIN CC 7.0 SICAM PAS PCS 7.0
172.50.0.200
172.40.0.202
HVSS Engineer Workstation
172.50.0.50
GPSTimeServ2
172.50.0.40
PM130P
172.50.0.22
PM130EH
172.50.0.21
Temperature Sensor
172.50.0.64
SW3
172.50.0.13
SW1
172.50.0.11
SW2
172.50.0.12
Digsi, SNMP, SSH
7SD523_W1
172.50.0.51
6MD664_Q2
172.50.0.52
7SJ645_Q4
172.50.0.53
7UT635_1K
172.50.0.54
7SD523_W2
172.50.0.71
6MD664_Q1
172.50.0.72
6MD664_Q3
172.50.0.73
7UT635_2K
172.50.0.74
Distribution Substation 10kV (DSS)
SW4
172.30.0.112
Digsi to IP
DSS RTU 520
172.90.0.10
Mosa agent
172.30.0.20
IEC 60870-103 (RS485)
7SJ642
7SJ642
100BaseFX main
100BaseFX res.
100BaseTX main
100BaseTX res.
RS485, IEC 60870-5-103

Positive Hack Days VI: Энергетика - Структура

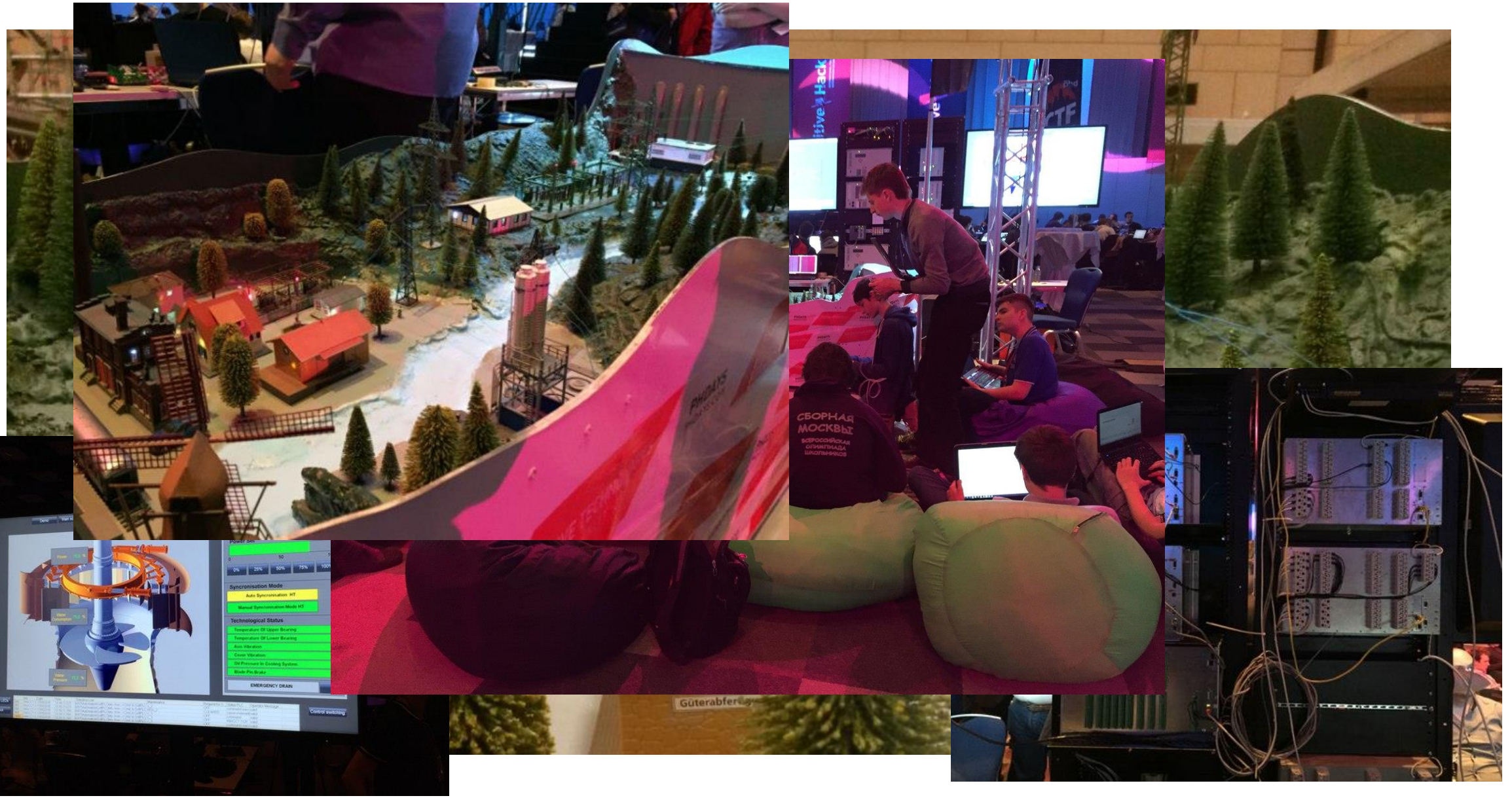
POSITIVE TECHNOLOGIES



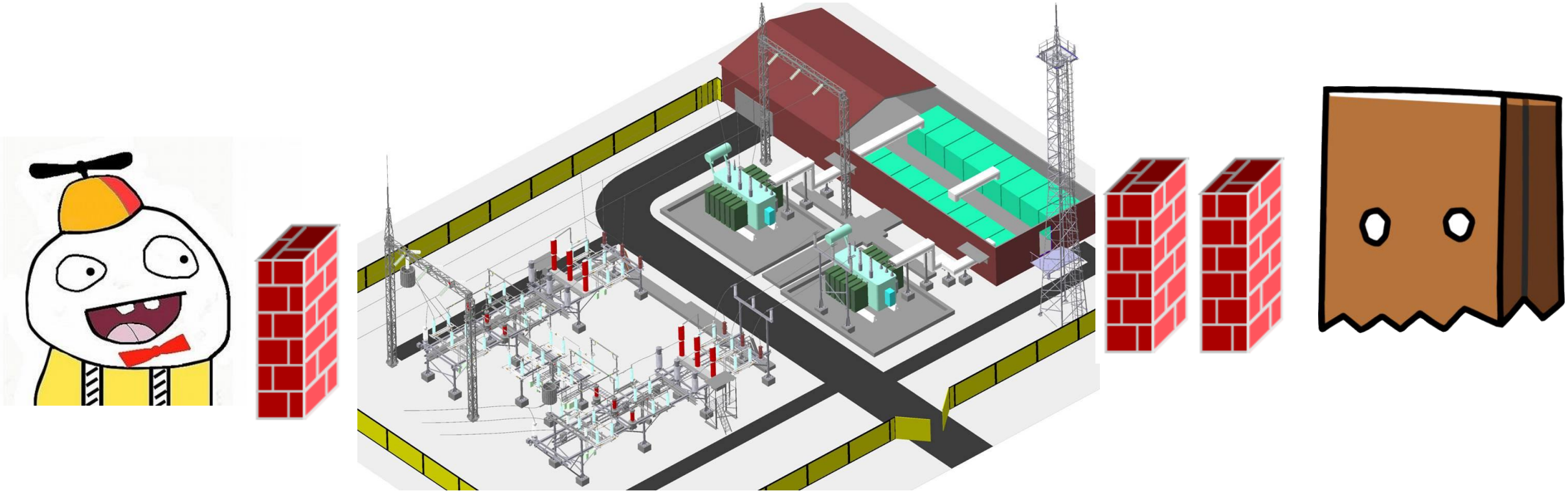
Main scheme
Critical Infrastructure Attack:
Blackout

Positive Hack Days VI: Энергетика - Структура

POSITIVE TECHNOLOGIES



Подстанция 500кВ



Check Point®
SOFTWARE TECHNOLOGIES LTD.

Positive Hack Days VI – School style

POSITIVE TECHNOLOGIES

Google siprotec уязвимость

Все Картинки Новости Видео Ещё Инструменты пои

Результатов: примерно 887 (0,53

Siemens устранила уязв
www.securitylab.ru/news/473842
23 июл. 2015 г. - Как следует из ув
устройства **SIPROTEC** 4 и **SIPRO**
Вы посещали эту страницу неско

Терминалы Siemens SIP
www.securitylab.ru/news/478354
12 янв. 2016 г. - Терминалы **Siem**
коммуникационным модулем EN1

BDU:2015-10800 - БДУ -
www.bdu.fstec.ru/vul/2015-1080
Описание **уязвимости**, **Уязвимо**
релейной защиты **Siemens SIPR**

Google 61850 tool

Все Картинки Видео Карты Новости Ещё

Результатов: примерно 112 000 (0,35 сек.)

CET850 IEC 61850 configuration tool V2.1 - Docum
www.schneider-electric.com/.../674750929-CET850-IEC-**61**... Пе
CET850 is the IEC **61850** Edition 1 & 2 configurator associated with the Sepam server.The CET850 software enables protection ...

[PDF] **IEC 61850 Engineering Process and Multi-Vend**
www.schneider-electric.com/.../998-1197420_IEC-**61850**-E... Пер
engineering approach as defined in the IEC **61850** standard versus tradi configuration **tools** by discussing the benefits and cost savings.

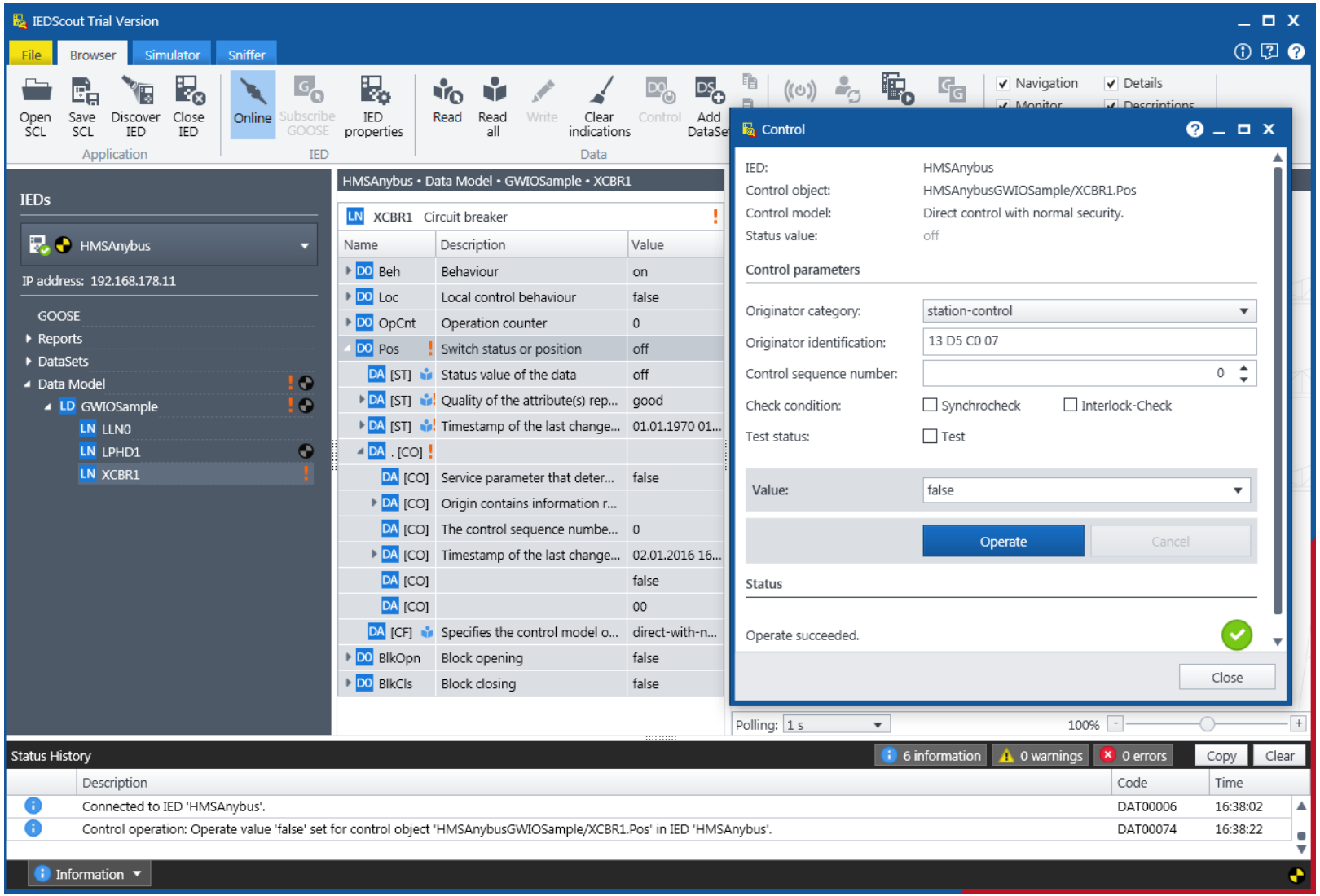
[PDF] **IEC 61850 Testing Tools - Omicron**
https://www.omicronenergy.com/.../IEC-**61850**-Testing-**Too**... Пер
OMICRON provides the most advanced IEC **61850** testing **tools** for ... F IEC **61850** GOOSE and Sampled Values, corresponding.

61850 Test Suite - Triangle MicroWorks
www.trianglemicroworks.com/...**tools**/**61850**-test.../test-suite Пер

IEDScout version 4.10

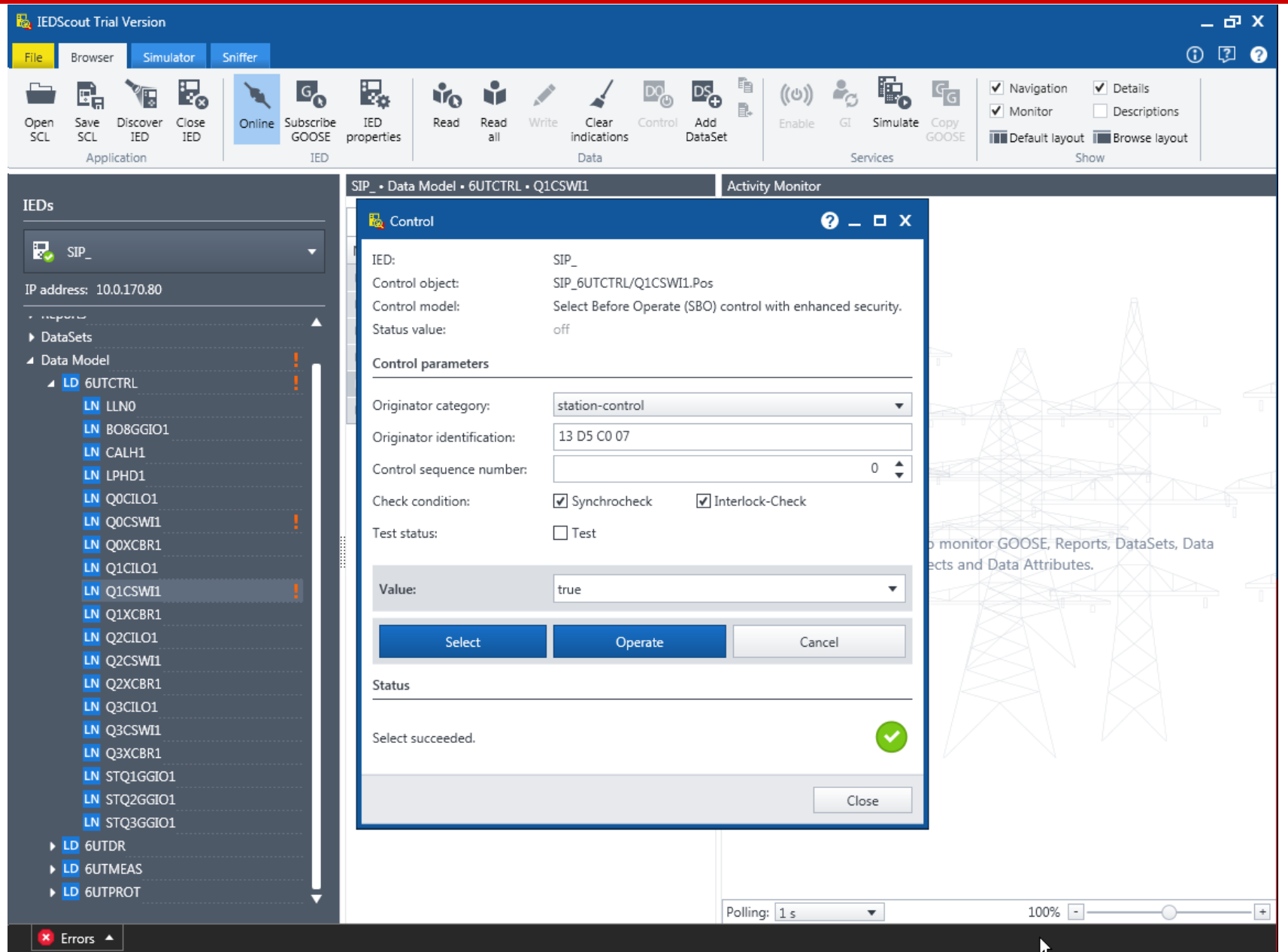
OMICRON

документация

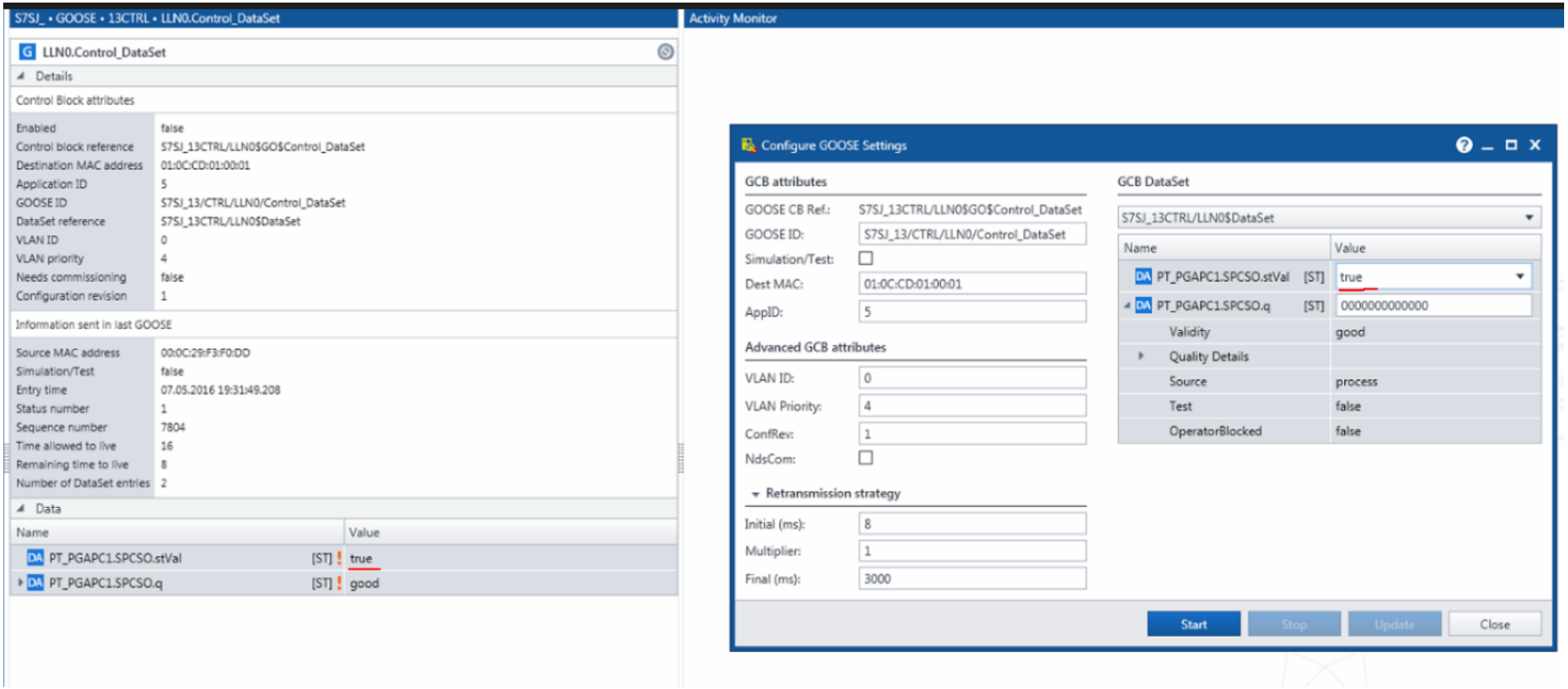


OMICRON

реальность



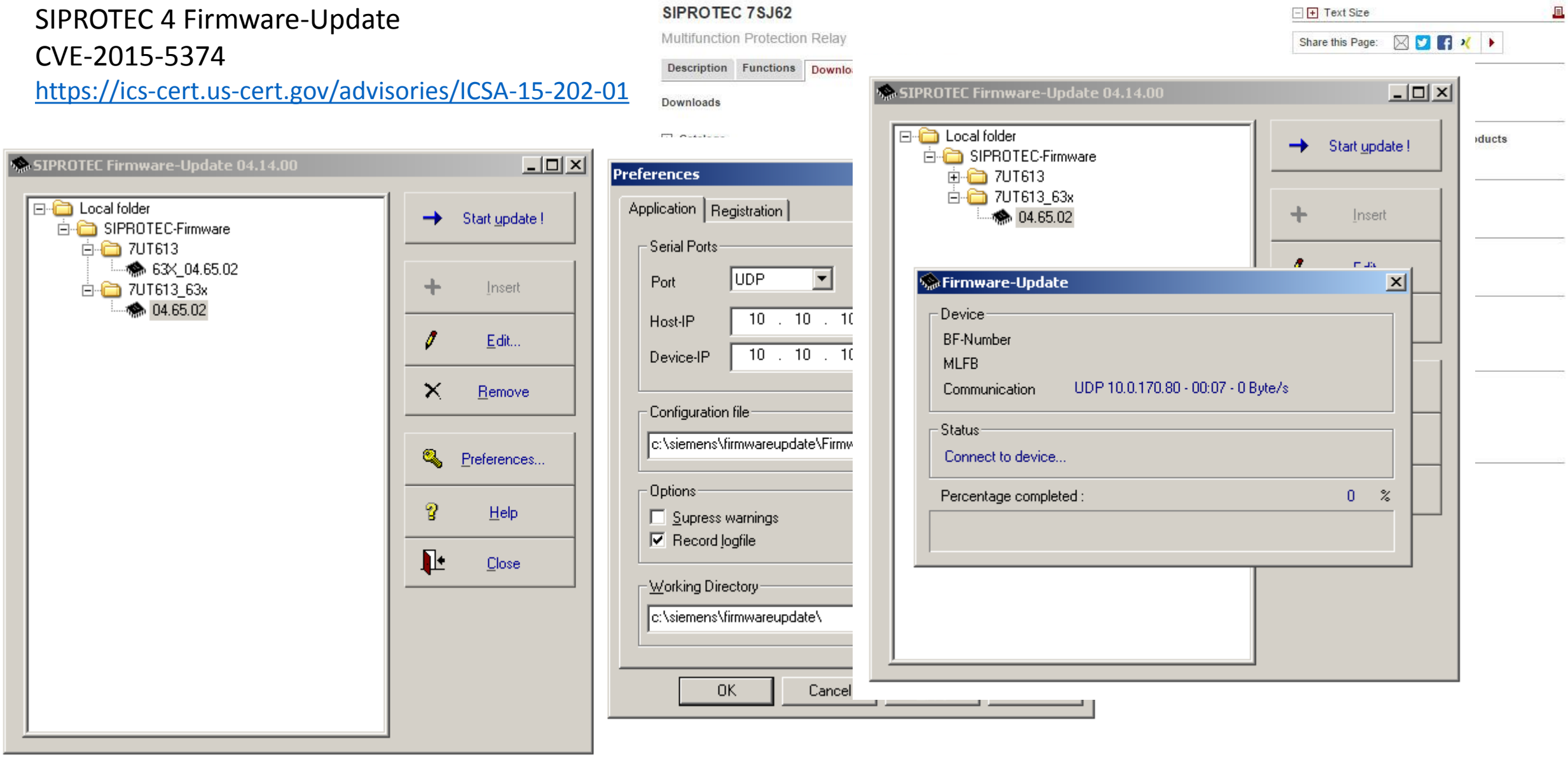
OMICRON Goose emulate

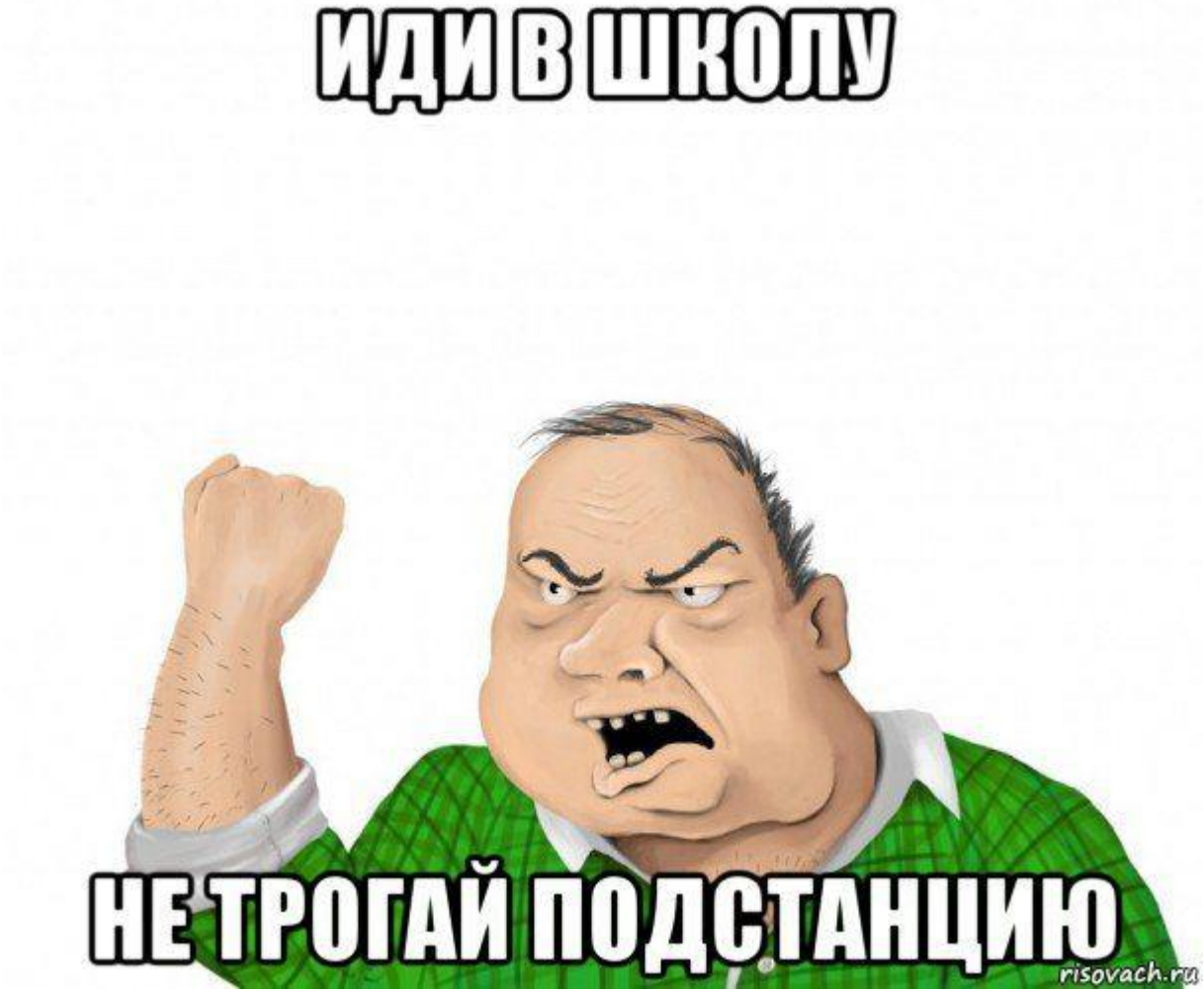


Positive Hack Days VI – School style

POSITIVE TECHNOLOGIES

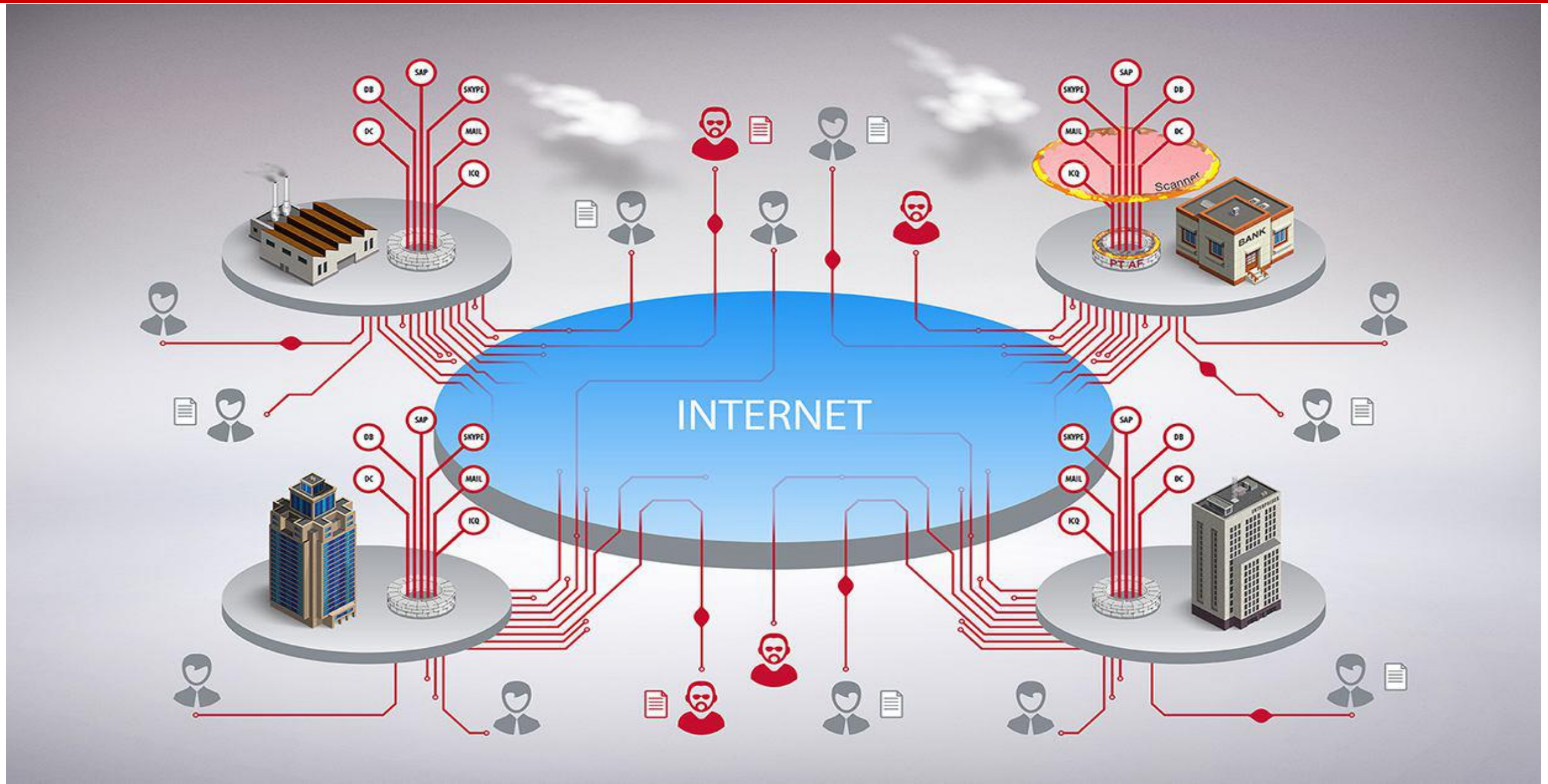
SIPROTEC 4 Firmware-Update
CVE-2015-5374
https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01



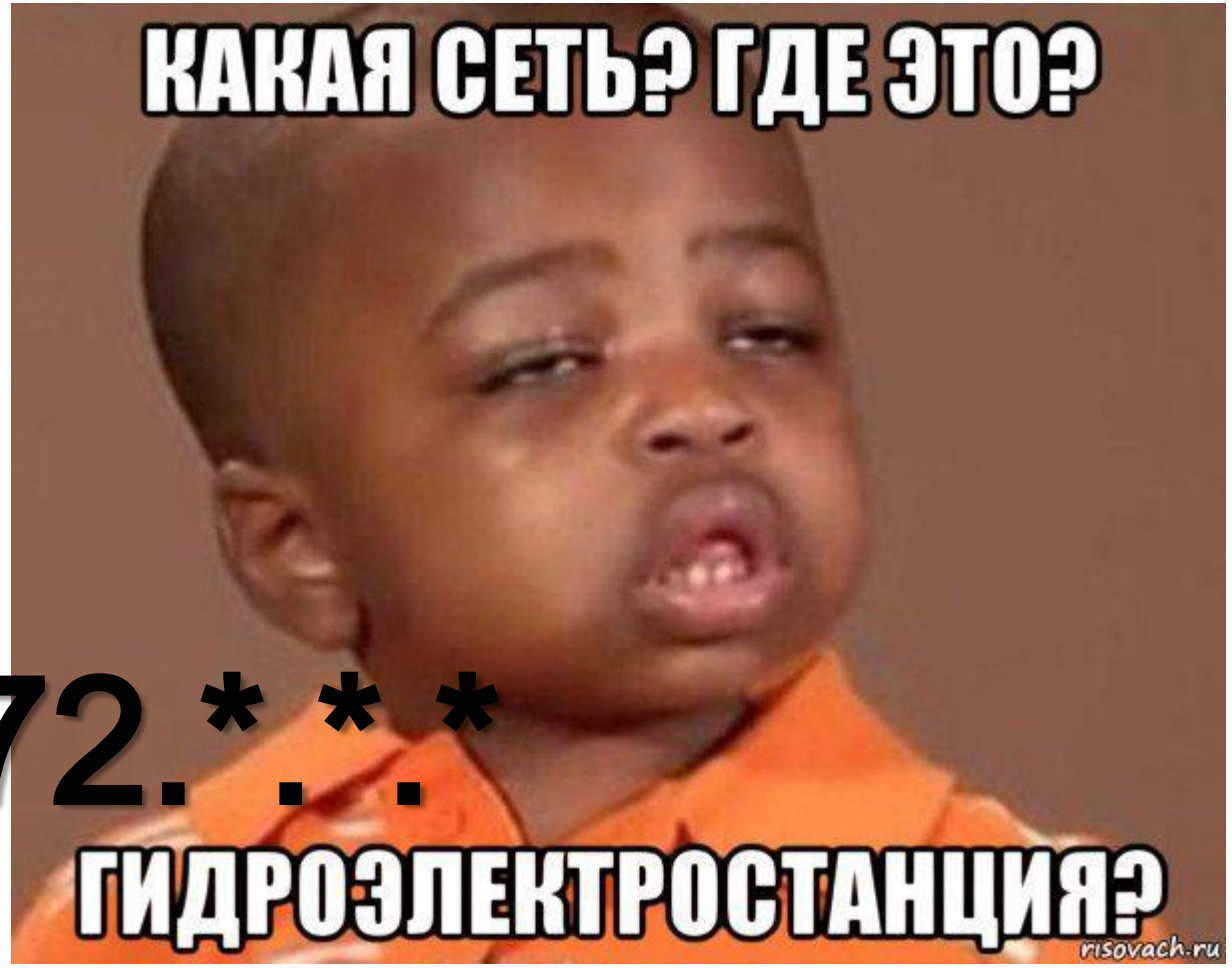

ИДИ В ШКОЛУ
НЕ ТРОГАЙ ПОДСТАНЦИЮ
risovach.ru

Positive Hack Days VI: Архитектура сети

POSITIVE TECHNOLOGIES

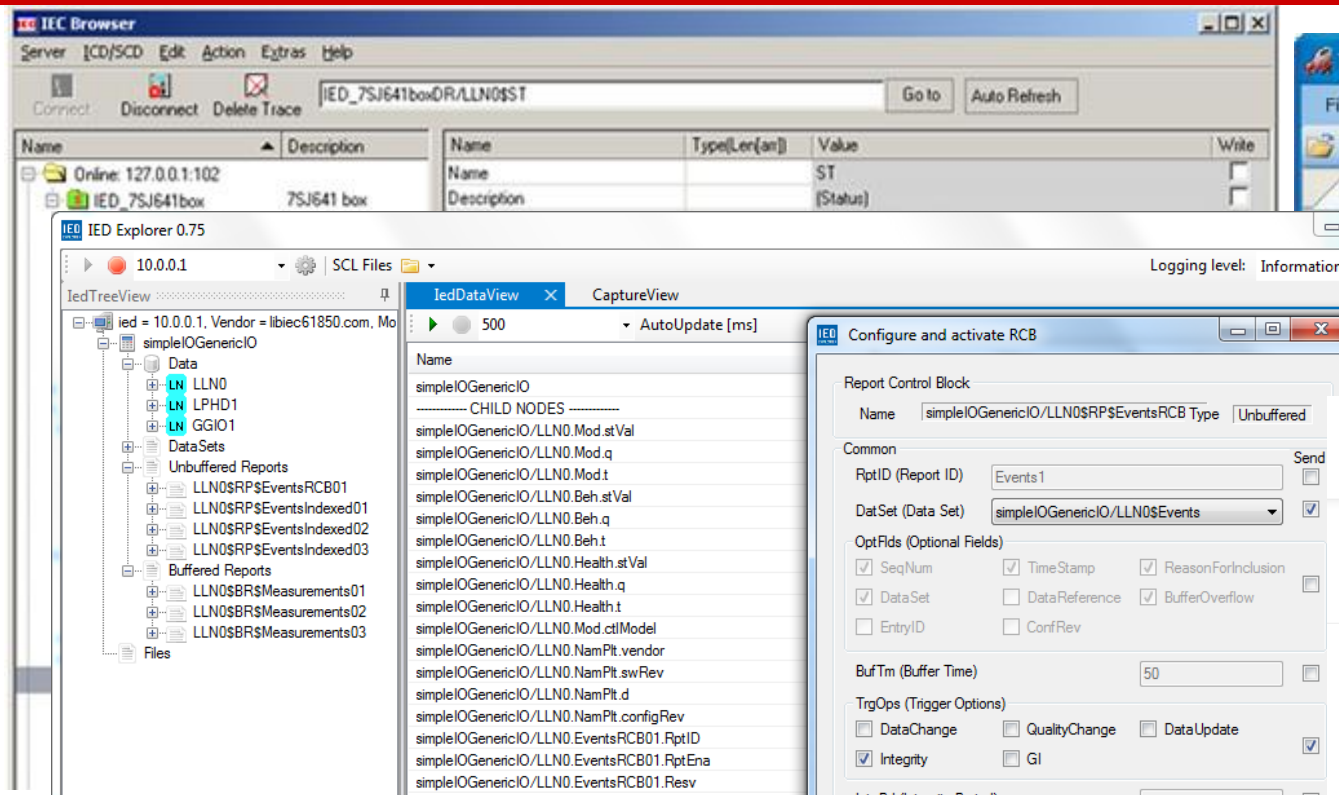


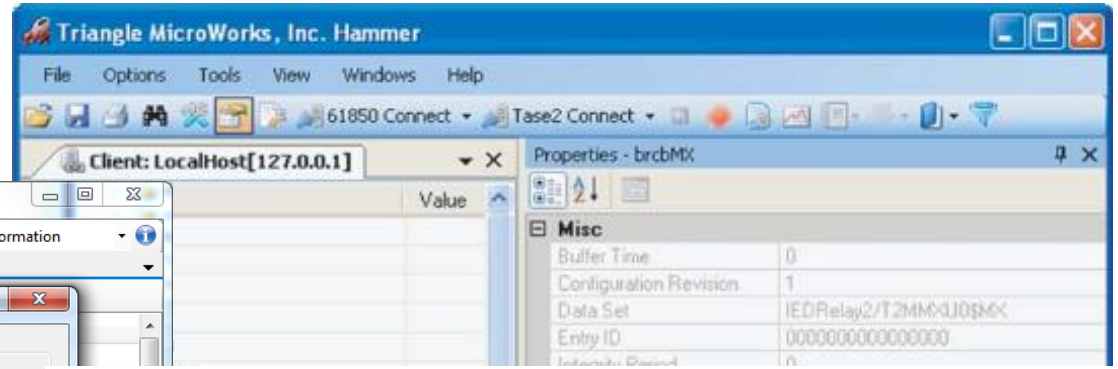
$ nmap 172.*.*.*



Positive Hack Days VI – CTF style

POSITIVE TECHNOLOGIES





Personal Open source Business Explore

Search 61850 goose

Repositories 4
Code 1,188
Issues 4
Users

Languages
Python 1
C 1

Advanced search Cheat sheet

stevenblair/tunnel **61850**
IEC **61850** **GOOSE** and Sampled Value tunnelling using UDP
Updated on 16 Aug 2012

mdehus/**goose**-IEC **61850**-scapy
Updated on 2 Feb 2014

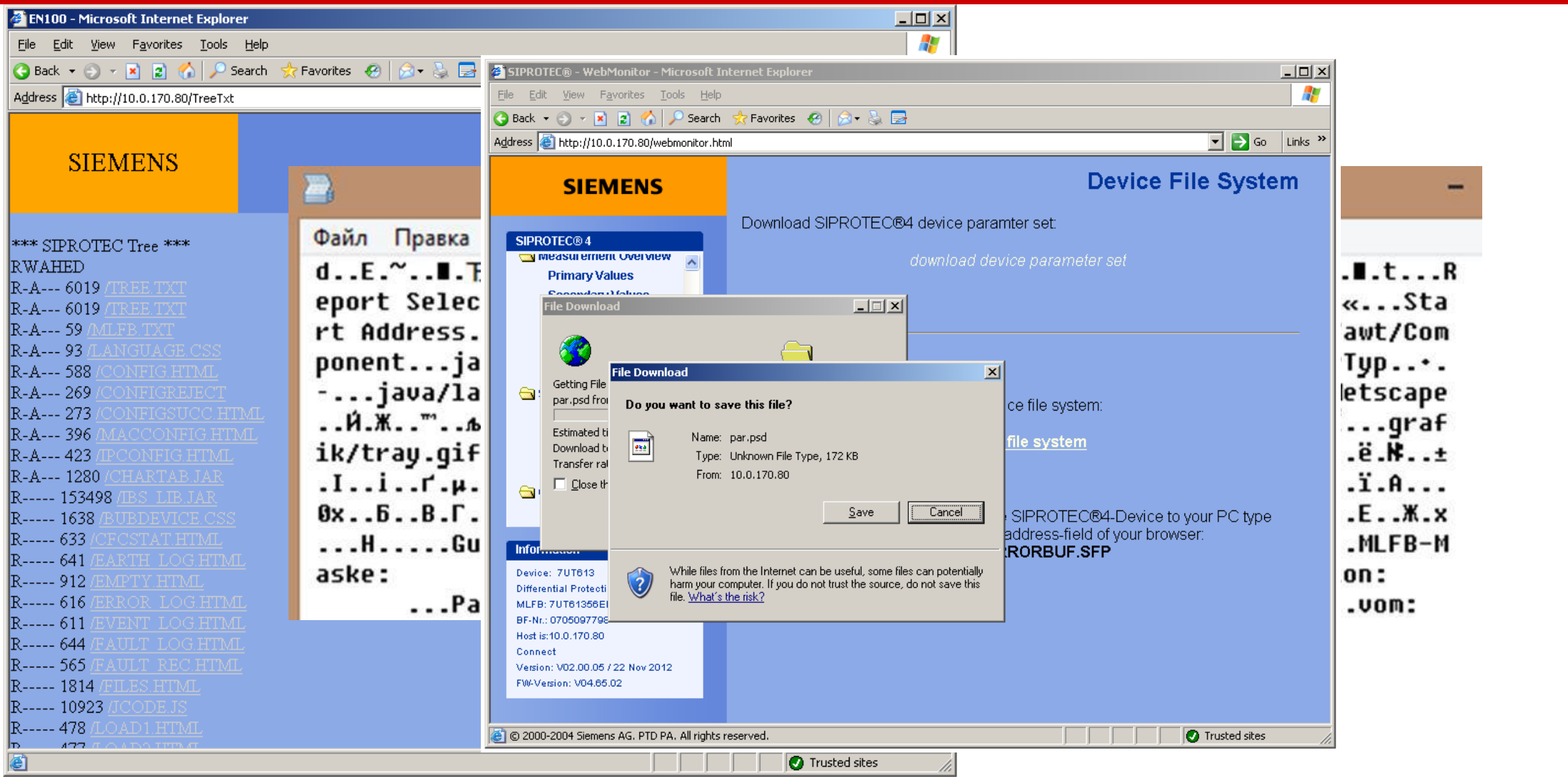
hectordelahoz/ProcessBuslec **61850**
This project contains an OMNeT++/INET extension to support IEC6 communication (**GOOSE** and SV)

SIEMENS

DIGSI 4
One Software for all SIPROTEC Protection Relays

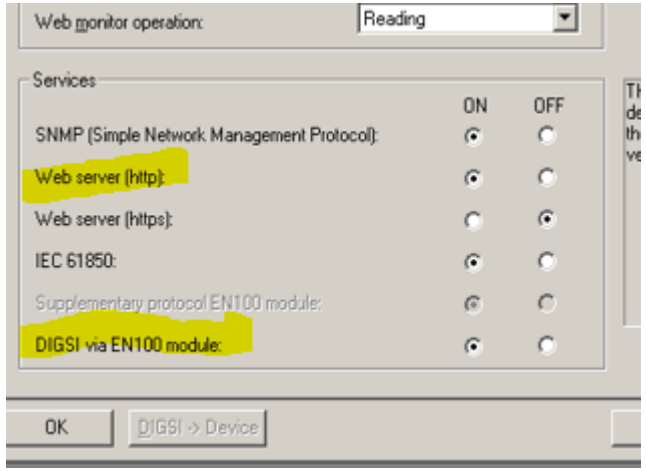
Positive Hack Days VI – CTF style

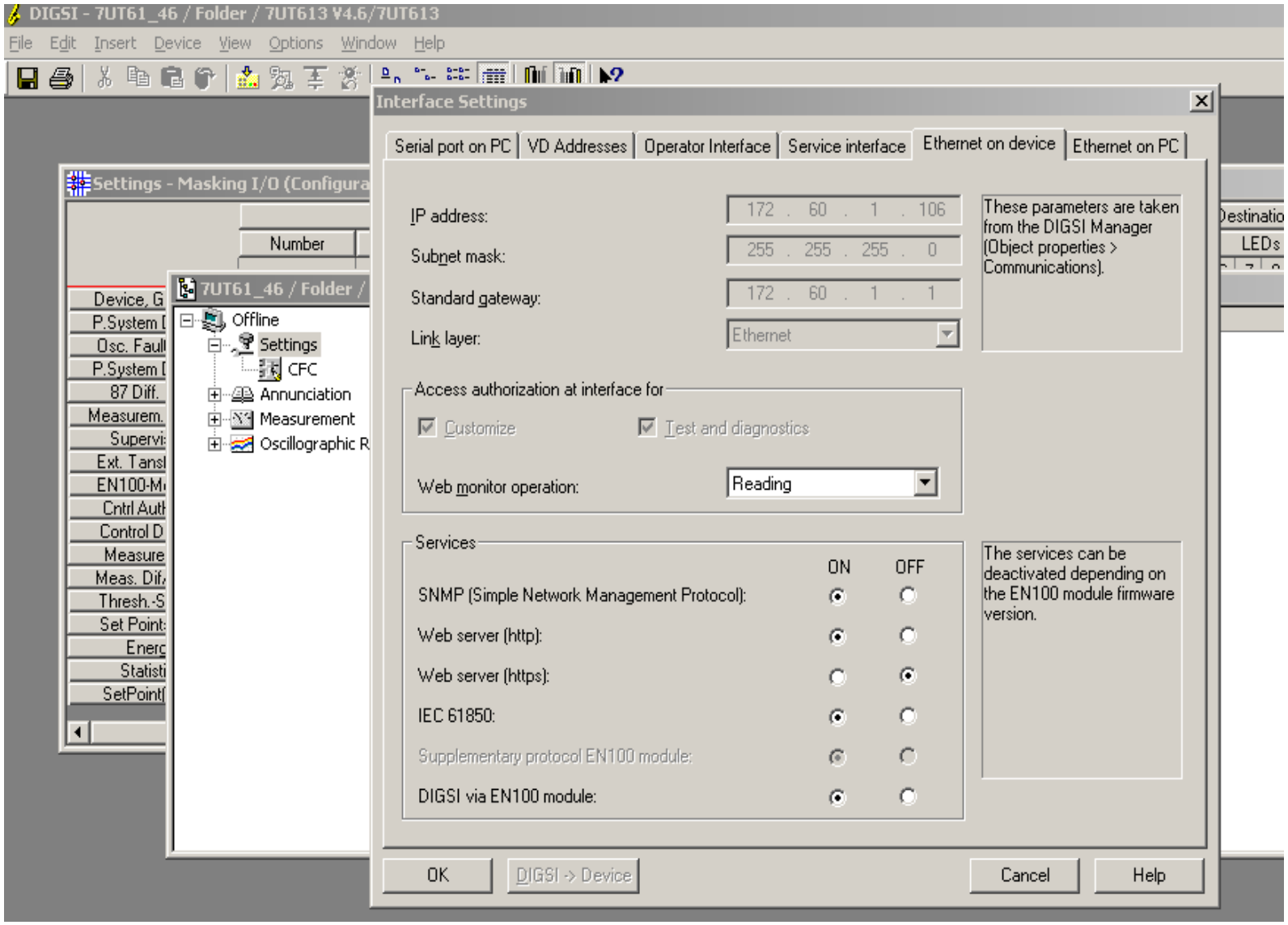
POSITIVE TECHNOLOGIES



Почему WEB?

До конца 2015 года в старых прошивках нельзя было изменить параметры!!!





Positive Hack Days VI – CTF style

POSITIVE TECHNOLOGIES

DIGSI - 7UT61_46_2 / Folder / 7UT613 V4.6/7UT613 V04.65.02

File Edit Insert Device View Options Window Help

7UT61_46_2 /

- Online
  - Settings
    - CFC
  - Control
  - Annuncia
    - Event
    - Trip L
    - Gene
    - Spont
    - Statis
  - Measurer
    - Prima
    - Secor
    - Perce
    - Other
  - Oscillogra
    - Oscill
  - Test

DIGSI - 7UT61_46_2 / Folder / 7UT613 V4.6/7UT613 V04.65.02

File Edit Insert Device View Options Window Help

7UT61_46_2 / Folder / 7UT613 V4.6/7UT613 V04.65.02

- Online
  - Settings
  - Control
  - Annunciation
  - Measurement
  - Oscillographic Records
  - Test

Select function

- Hardware Test
- Generate Indications
- Test Wave Form

Test device inputs and outputs

Binary input, binary output and LED

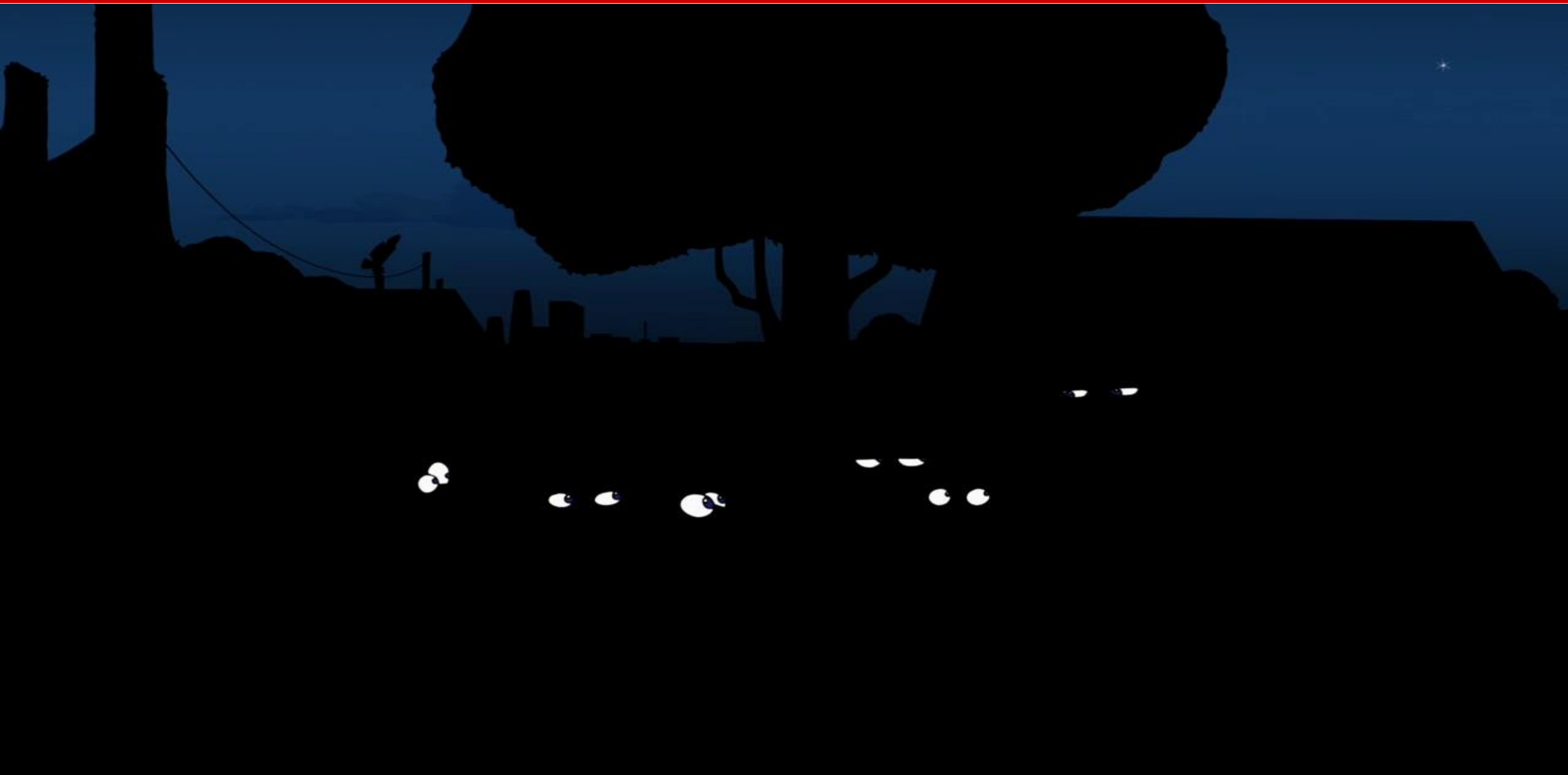
	No.	Actual	Nominal	Conf.
BI	BI 3		High	
	BI 4		High	
	BI 5		High	
BO	BO 1		ON	Q1
	BO 2		ON	Q1
	BO 3		OFF	>Buchh. -2;Q2
	BO 4		ON	Error Sum Alarm;Alarm Sum Event;Q
	BO 5		OFF	Q0;Q3
	BO 6		ON	Q0;Q3
	BO 7		OFF	Q0
	BO 8		OFF	Pos;SP OO
	LEDs 1		OFF	STATUS_Q1

Automatic Update (20 sec) Update

Close Help

Positive Hack Days VI - Blackout

POSITIVE TECHNOLOGIES



Positive Hack Days VI – Protector style

POSITIVE TECHNOLOGIES


Спасибо!
POSITIVE TECHNOLOGIES
ptsecurity.ru