



POSITIVE HACK DAYS VI

POSITIVE TECHNOLOGIES

phdays.ru

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



4,2
тыс

участников

75

докладов

8

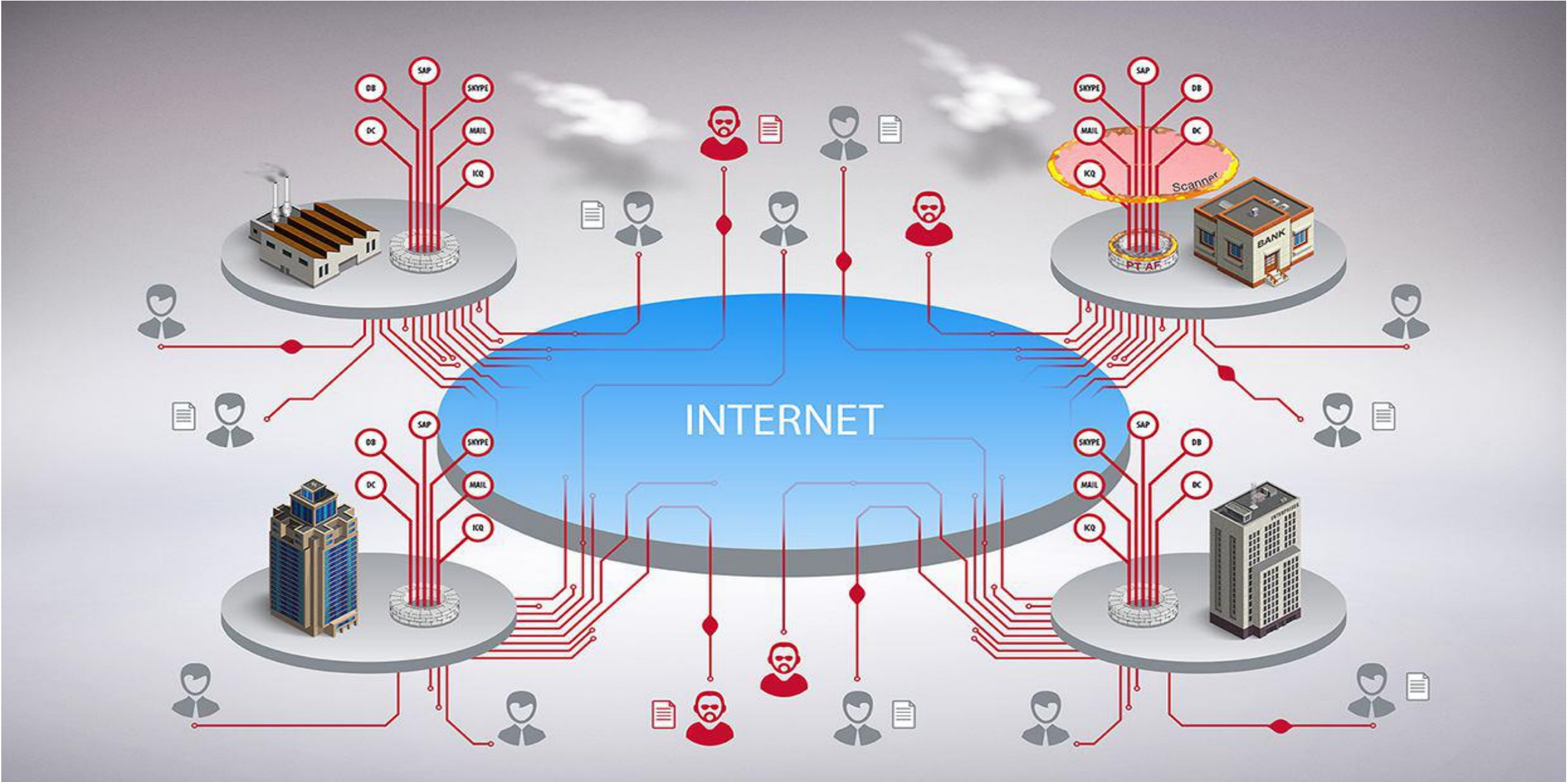
мастер-
классов

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



Максимально реалистичный макеты:

▪ Генерация

▪ Передача

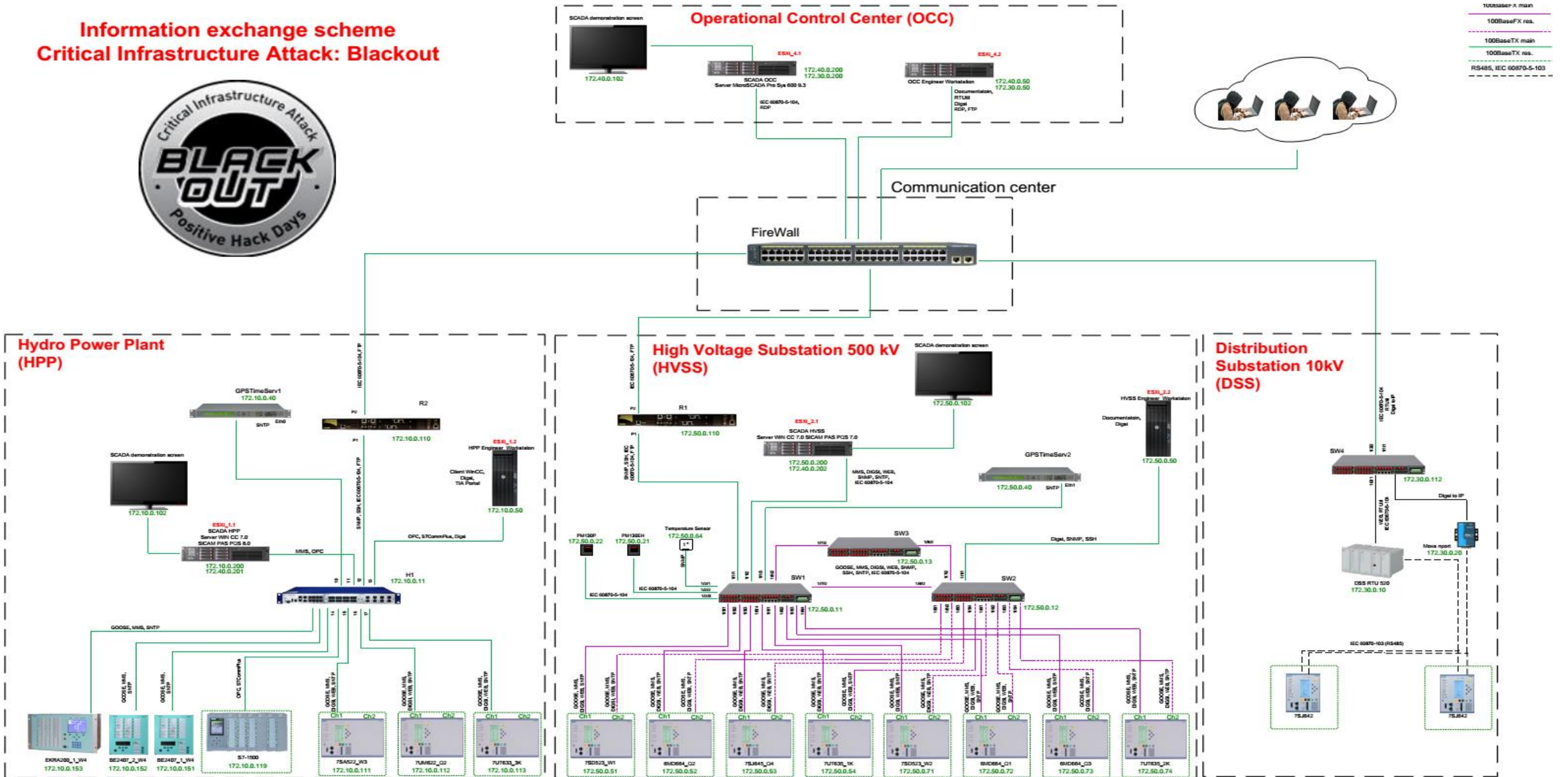
▪ Распределение

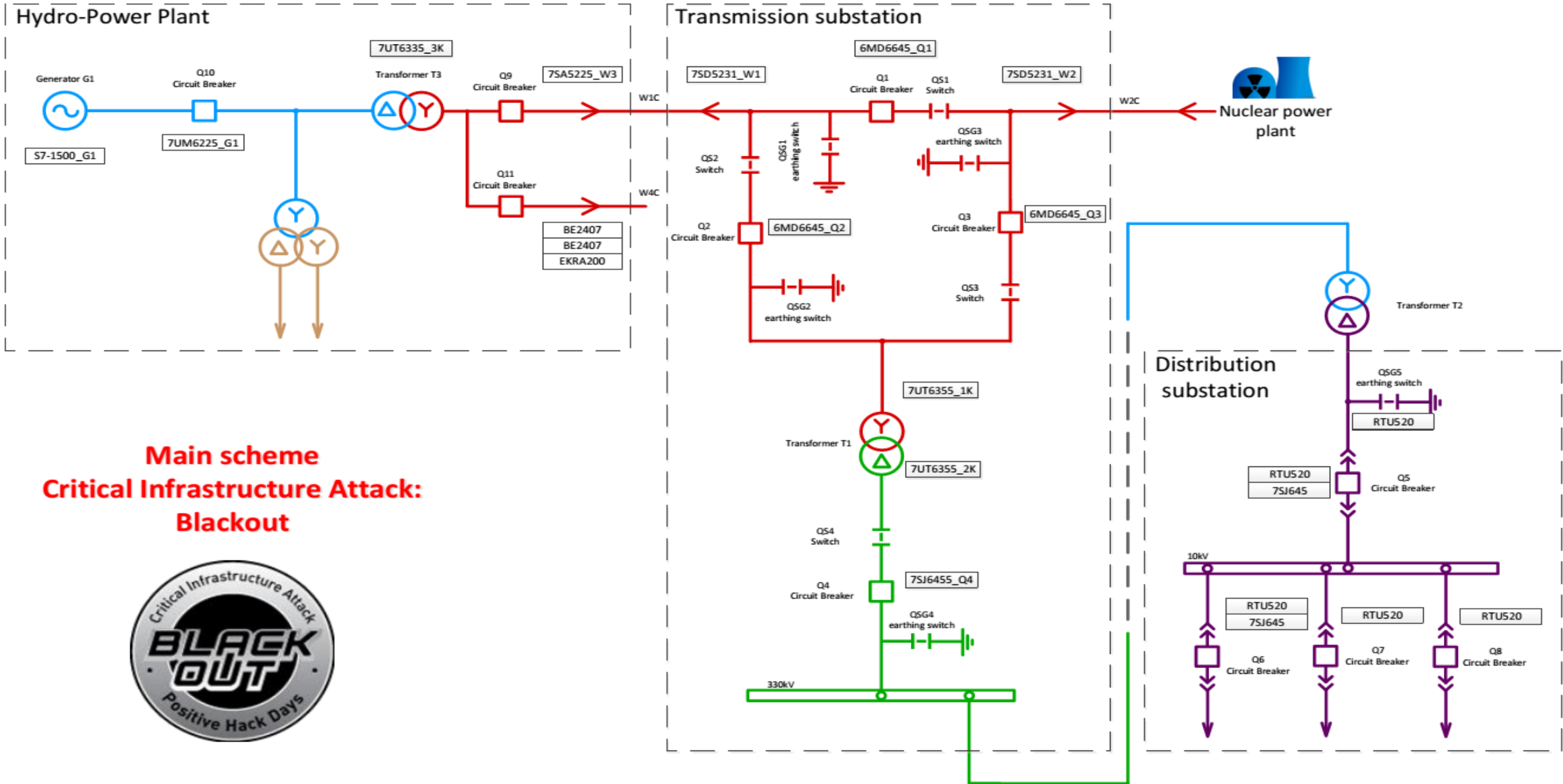
▪ Управление электроснабжением и системы автоматки «умного» дома



- 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 7ой** 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...

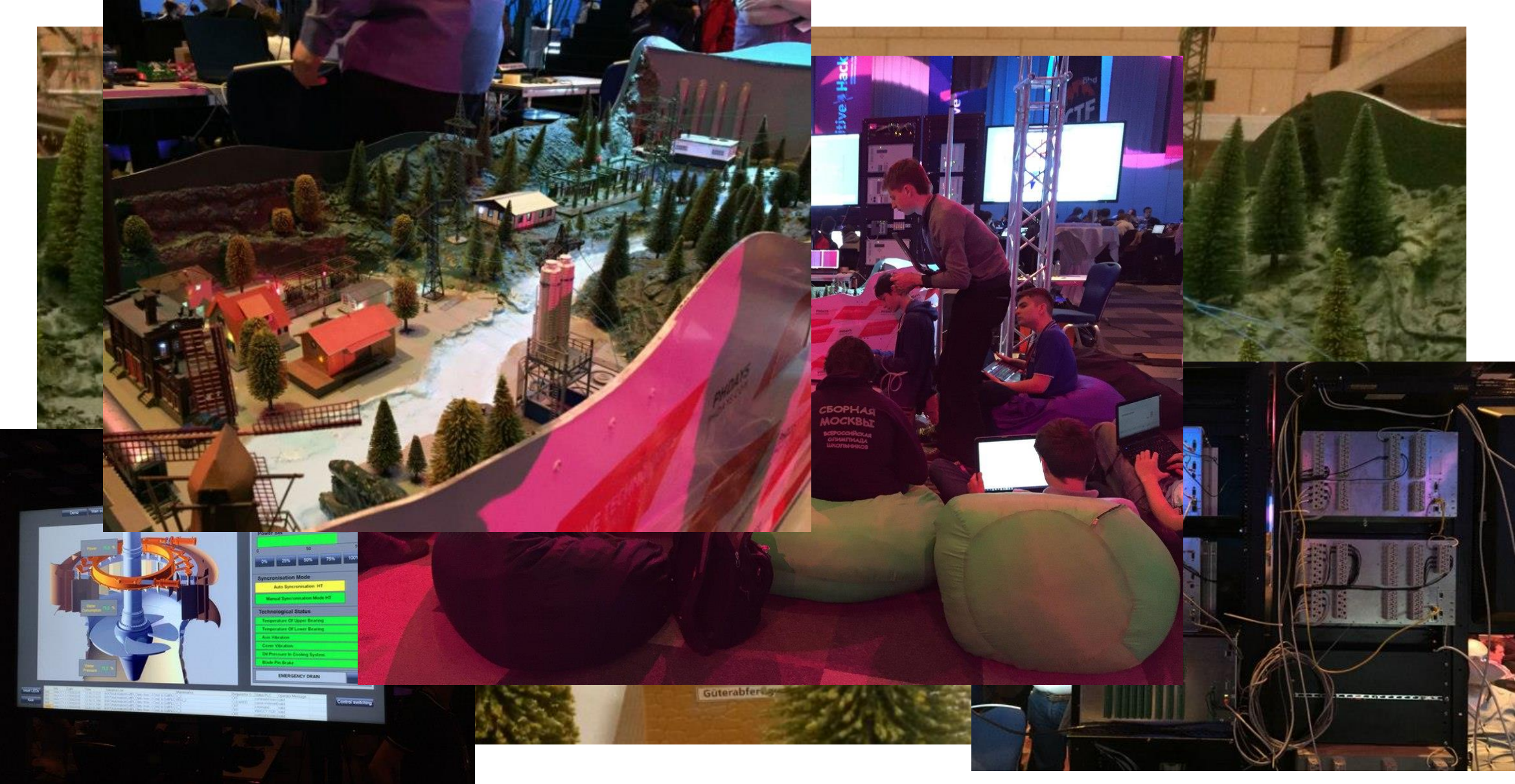
Information exchange scheme Critical Infrastructure Attack: Blackout



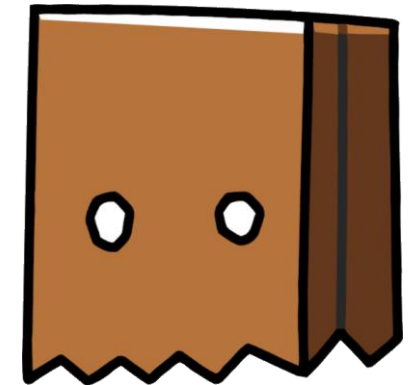
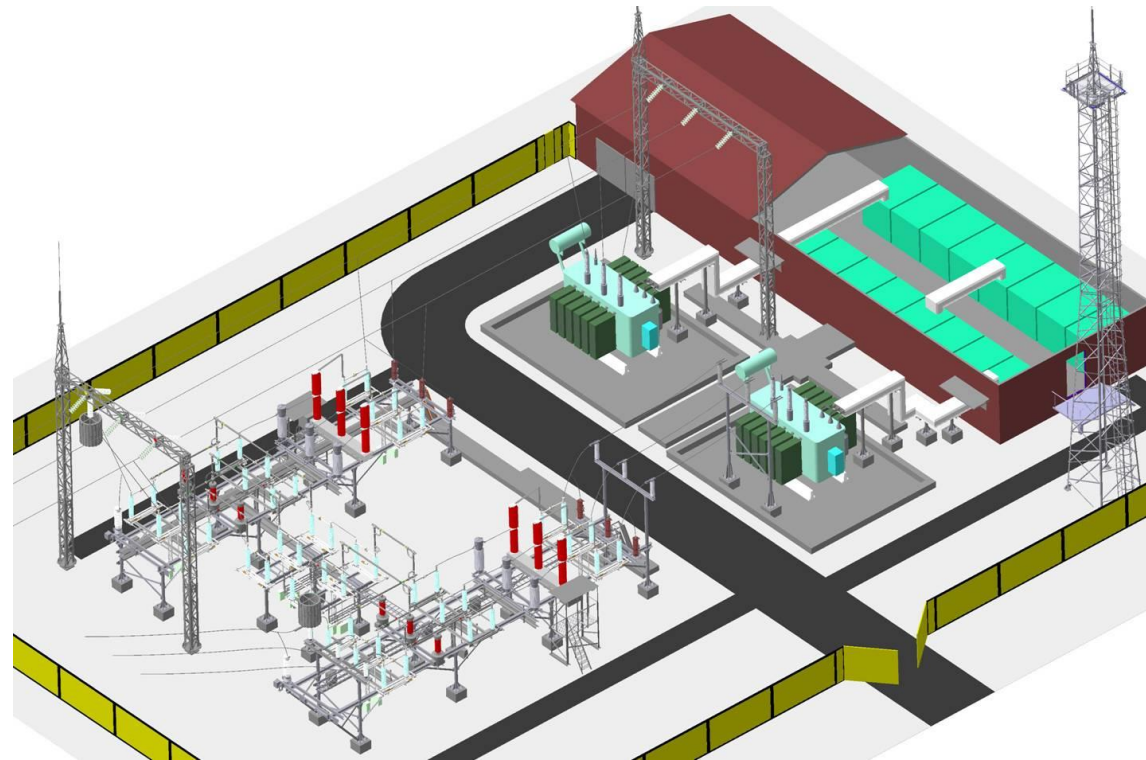
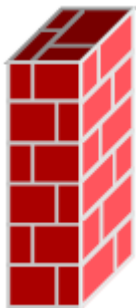


**Main scheme
Critical Infrastructure Attack:
Blackout**





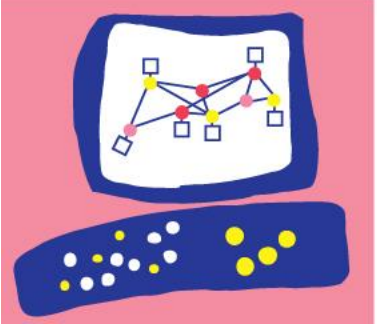
Подстанция 500кВ



**DENY ALL FROM ANY TO ANY
VIA ANY!**



Check Point®
SOFTWARE TECHNOLOGIES LTD.



Google siprotec уязвимость

Все Картинки Новости Видео Ещё Инструменты по

Результатов: примерно 887 (0,53)

[Siemens устранила уязв](http://www.securitylab.ru/news/473842)
www.securitylab.ru/news/473842
23 июл. 2015 г. - Как следует из уе
устройства **SIPROTEC 4** и **SIPRO**
Вы посещали эту страницу неско

[Терминалы Siemens SIP](http://www.securitylab.ru/news/478354)
www.securitylab.ru/news/478354
12 янв. 2016 г. - Терминалы **Siem**
коммуникационным модулем EN1

[BDU:2015-10800 - БДУ -](http://www.bdu.fstec.ru/vul/2015-10800)
www.bdu.fstec.ru/vul/2015-10800
Описание **уязвимости**, **Уязвимос**
релейной защиты **Siemens SIPRO**

Google 61850 tool

Все Картинки Видео Карты Новости Ещё

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

[CET850 IEC 61850 configuration tool V2.1 - Docum](http://www.schneider-electric.com/.../674750929-CET850-IEC-61...)
www.schneider-electric.com/.../674750929-CET850-IEC-61... **▼** **Пер**
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](http://www.schneider-electric.com/.../998-1197420_IEC-61850-E...)
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.omcronenergy.com/.../IEC-61850-Testing-Too...)
<https://www.omcronenergy.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](http://www.trianglemicroworks.com/...tools/61850-test.../test-suite)
www.trianglemicroworks.com/...tools/61850-test.../test-suite **▼** **Пер**



ОПИСАНИЕ ЗАГРУЗКА ОБНОВЛЕНИЕ ВИДЕО

IEDScout version 4.10

OMICRON документация

The screenshot displays the IEDScout Trial Version interface. The main window shows a tree view of the IEDs, with HMSAnybus selected. The Data Model for GWIOSample is expanded, showing the XCBR1 circuit breaker. A 'Control' dialog box is open, showing the control parameters for the 'Pos' object. The dialog includes fields for Originator category, Originator identification, Control sequence number, Check condition, and Test status. The 'Value' field is set to 'false'. The 'Operate' button is highlighted, and a status message 'Operate succeeded.' is visible at the bottom of the dialog. The Status History window at the bottom shows a log of events, including 'Connected to IED 'HMSAnybus'' and 'Control operation: Operate value 'false' set for control object 'HMSAnybusGWIOSample/XCBR1.Pos' in IED 'HMSAnybus''.

Name	Description	Value
LN XCBR1	Circuit breaker	
DO Beh	Behaviour	on
DO Loc	Local control behaviour	false
DO OpCnt	Operation counter	0
DO Pos	Switch status or position	off
DA [ST]	Status value of the data	off
DA [ST]	Quality of the attribute(s) rep...	good
DA [ST]	Timestamp of the last change...	01.01.1970 01...
DA [CO]	Service parameter that deter...	false
DA [CO]	Origin contains information r...	
DA [CO]	The control sequence numbe...	0
DA [CO]	Timestamp of the last change...	02.01.2016 16...
DA [CO]		false
DA [CO]		00
DA [CF]	Specifies the control model o...	direct-with-n...
DO BlkOpn	Block opening	false
DO BlkCls	Block closing	false

Description	Code	Time
Connected to IED 'HMSAnybus'.	DAT00006	16:38:02
Control operation: Operate value 'false' set for control object 'HMSAnybusGWIOSample/XCBR1.Pos' in IED 'HMSAnybus'.	DAT00074	16:38:22

OMICRON реальность

The screenshot displays the IEDScout Trial Version software interface. The main window shows a tree view of IEDs (Intelligent Electronic Devices) under the 'Data Model' section, with 'LD 6UTCTRL' expanded. A 'Control' dialog box is open, showing details for the selected IED 'SIP_'. The dialog includes fields for 'Control object', 'Control model', 'Status value', 'Originator category', 'Originator identification', 'Control sequence number', 'Check condition', 'Test status', and 'Value'. The 'Value' field is set to 'true'. The 'Status' section shows 'Select succeeded.' with a green checkmark. The background shows a faint image of power lines.

IEDs

- SIP_
- IP address: 10.0.170.80
- DataSets
- Data Model
 - LD 6UTCTRL
 - LN LLNO
 - LN BO8GGIO1
 - LN CALH1
 - LN LPHD1
 - LN Q0CILO1
 - LN Q0CSWI1
 - LN Q0XCBR1
 - LN Q1CILO1
 - LN Q1CSWI1
 - LN Q1XCBR1
 - LN Q2CILO1
 - LN Q2CSWI1
 - LN Q2XCBR1
 - LN Q3CILO1
 - LN Q3CSWI1
 - LN Q3XCBR1
 - LN STQ1GGIO1
 - LN STQ2GGIO1
 - LN STQ3GGIO1
 - LD 6UTDR
 - LD 6UTMEAS
 - LD 6UTPROT

Control

IED: SIP_
Control object: SIP_6UTCTRL/Q1CSWI1.Pos
Control model: Select Before Operate (SBO) control with enhanced security.
Status value: off

Control parameters

Originator category: station-control
Originator identification: 13 D5 C0 07
Control sequence number: 0
Check condition: Synchrocheck Interlock-Check
Test status: Test

Value: true

Select Operate Cancel

Status

Select succeeded.

Close

Errors

Polling: 1 s 100%

OMICRON Goose emulate

S7SJ_ • GOOSE • 13CTRL • LLN0.Control_DataSet

LLN0.Control_DataSet

Details

Control Block attributes

Enabled	false
Control block reference	S7SJ_13CTRL/LLN0\$GO\$Control_DataSet
Destination MAC address	01:0C:CD:01:00:01
Application ID	5
GOOSE ID	S7SJ_13/CTRL/LLN0/Control_DataSet
DataSet reference	S7SJ_13CTRL/LLN0\$DataSet
VLAN ID	0
VLAN priority	4
Needs commissioning	false
Configuration revision	1

Information sent in last GOOSE

Source MAC address	00:0C:29:F3:F0:DD
Simulation/Test	false
Entry time	07.05.2016 19:31:49.208
Status number	1
Sequence number	7804
Time allowed to live	16
Remaining time to live	8
Number of DataSet entries	2

Data

Name	Value
DA PT_PGAPC1.SPCSO.stVal	[ST] true
DA PT_PGAPC1.SPCSO.q	[ST] good

Activity Monitor

Configure GOOSE Settings

GCB attributes

GOOSE CB Ref.: S7SJ_13CTRL/LLN0\$GO\$Control_DataSet

GOOSE ID: S7SJ_13/CTRL/LLN0/Control_DataSet

Simulation/Test:

Dest MAC: 01:0C:CD:01:00:01

AppID: 5

Advanced GCB attributes

VLAN ID: 0

VLAN Priority: 4

ConfRev: 1

NdsCom:

Retransmission strategy

Initial (ms): 8

Multiplier: 1

Final (ms): 3000

GCB DataSet

S7SJ_13CTRL/LLN0\$DataSet

Name	Value
DA PT_PGAPC1.SPCSO.stVal [ST]	true
DA PT_PGAPC1.SPCSO.q [ST]	00000000000000
Validity	good
Quality Details	
Source	process
Test	false
OperatorBlocked	false

Start Stop Update Close

SIPROTEC 4 Firmware-Update CVE-2015-5374

<https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01>

SIPROTEC 7SJ62
Multifunction Protection Relay

Description Functions Downloads

Downloads

SIPROTEC Firmware-Update 04.14.00

Local folder

- SIPROTEC-Firmware
 - 7UT613
 - 63x_04.65.02
 - 7UT613_63x
 - 04.65.02

Start update!

Insert

Edit...

Remove

Preferences...

Help

Close

Preferences

Application Registration

Serial Ports

Port: UDP

Host-IP: 10 . 10 . 10

Device-IP: 10 . 10 . 10

Configuration file: c:\siemens\firmwareupdate\Firmw...

Options

- Supress warnings
- Record logfile

Working Directory: c:\siemens\firmwareupdate\

OK Cancel

SIPROTEC Firmware-Update 04.14.00

Local folder

- SIPROTEC-Firmware
 - 7UT613
 - 63x_04.65.02
 - 7UT613_63x
 - 04.65.02

Start update!

Insert

Firmware-Update

Device

BF-Number

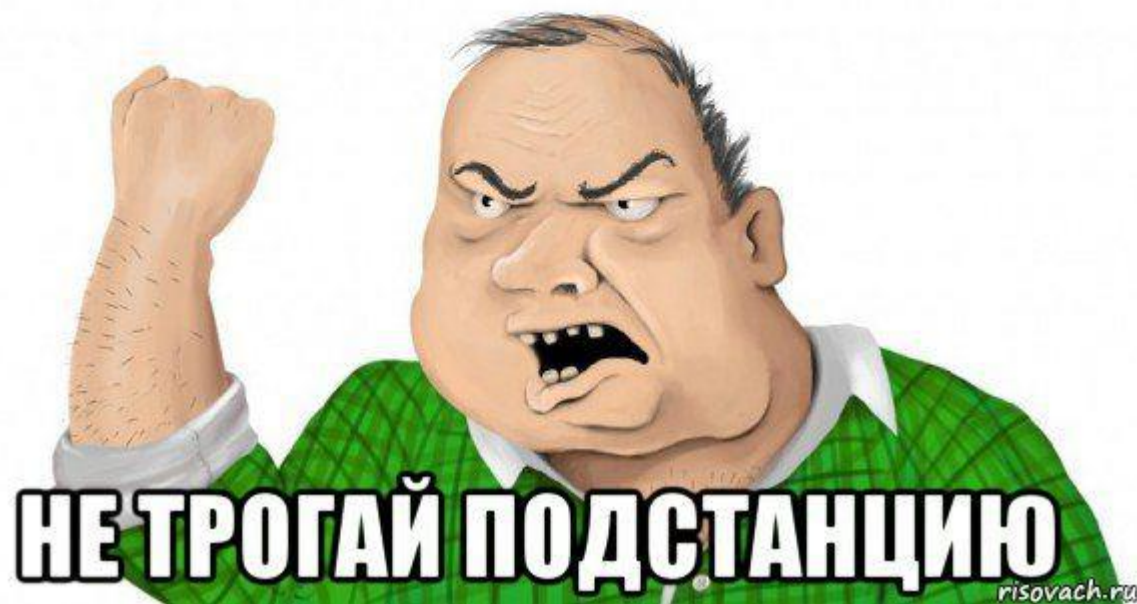
MLFB

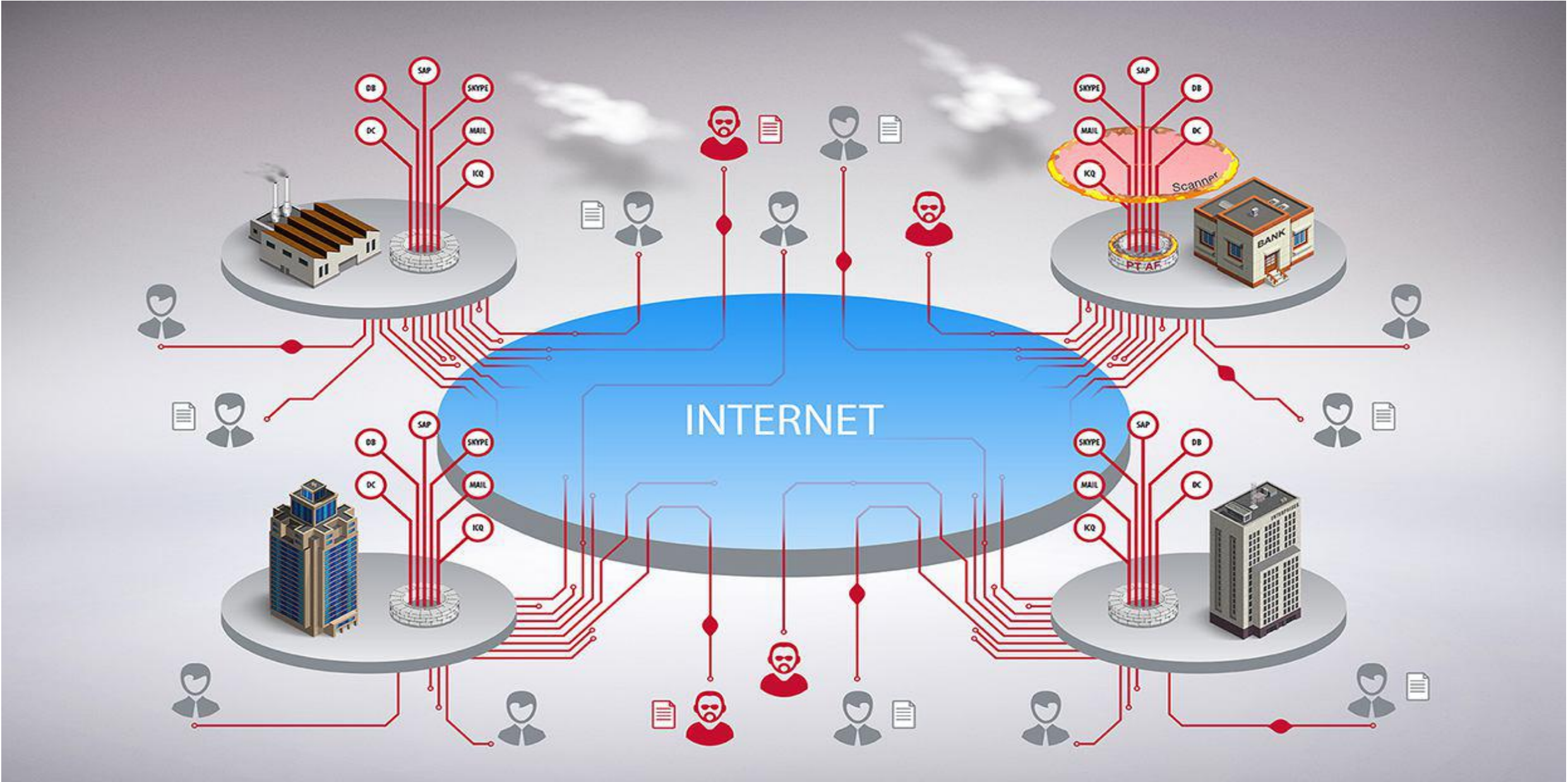
Communication: UDP 10.0.170.80 - 00:07 - 0 Byte/s

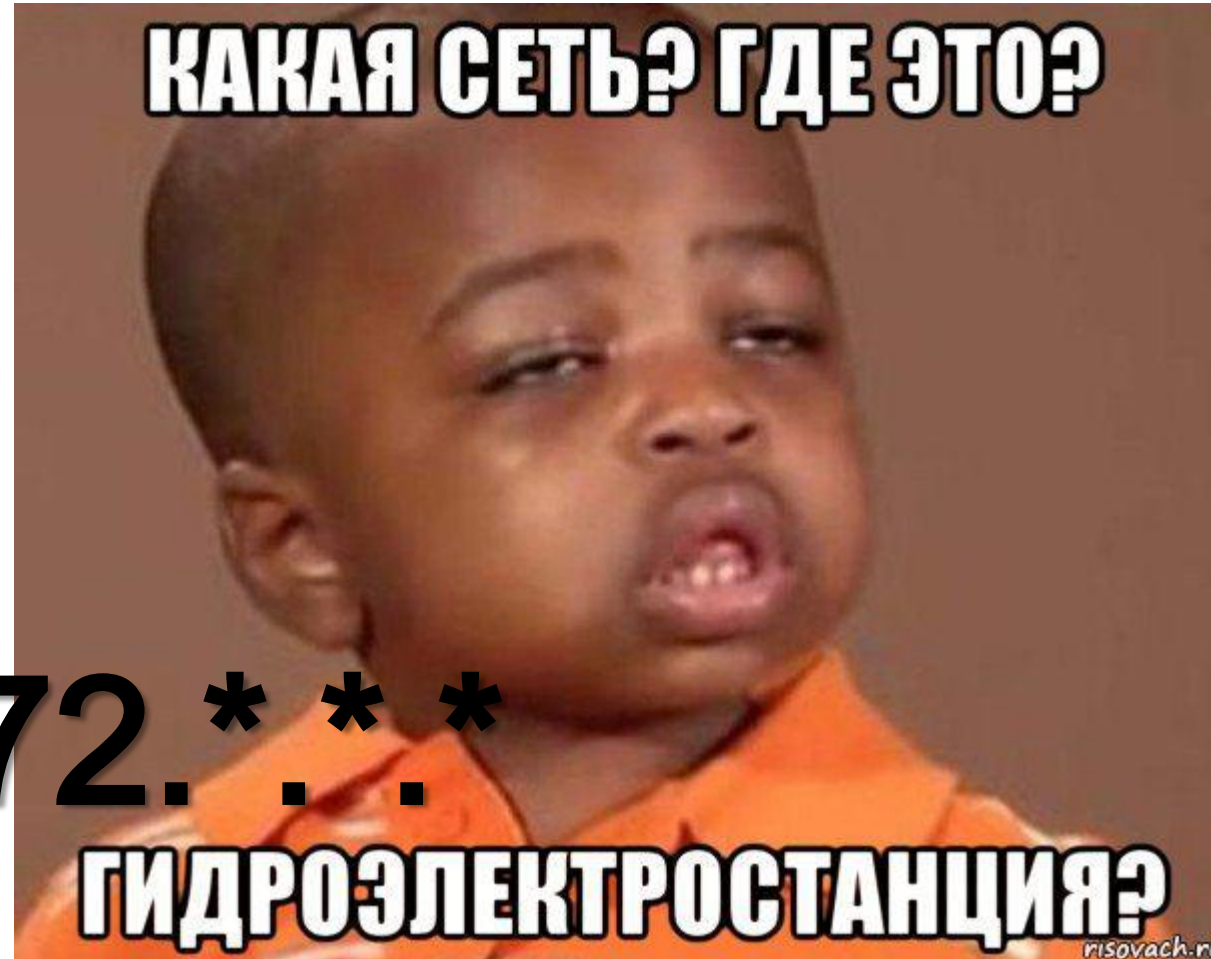
Status: Connect to device...

Percentage completed: 0 %

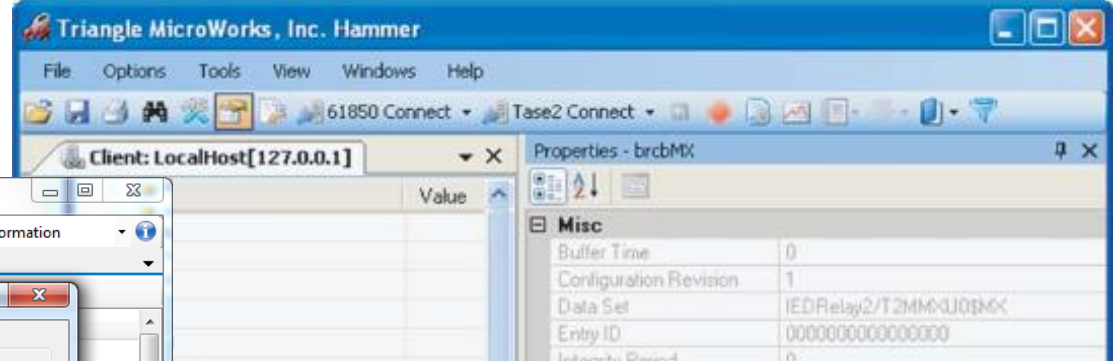
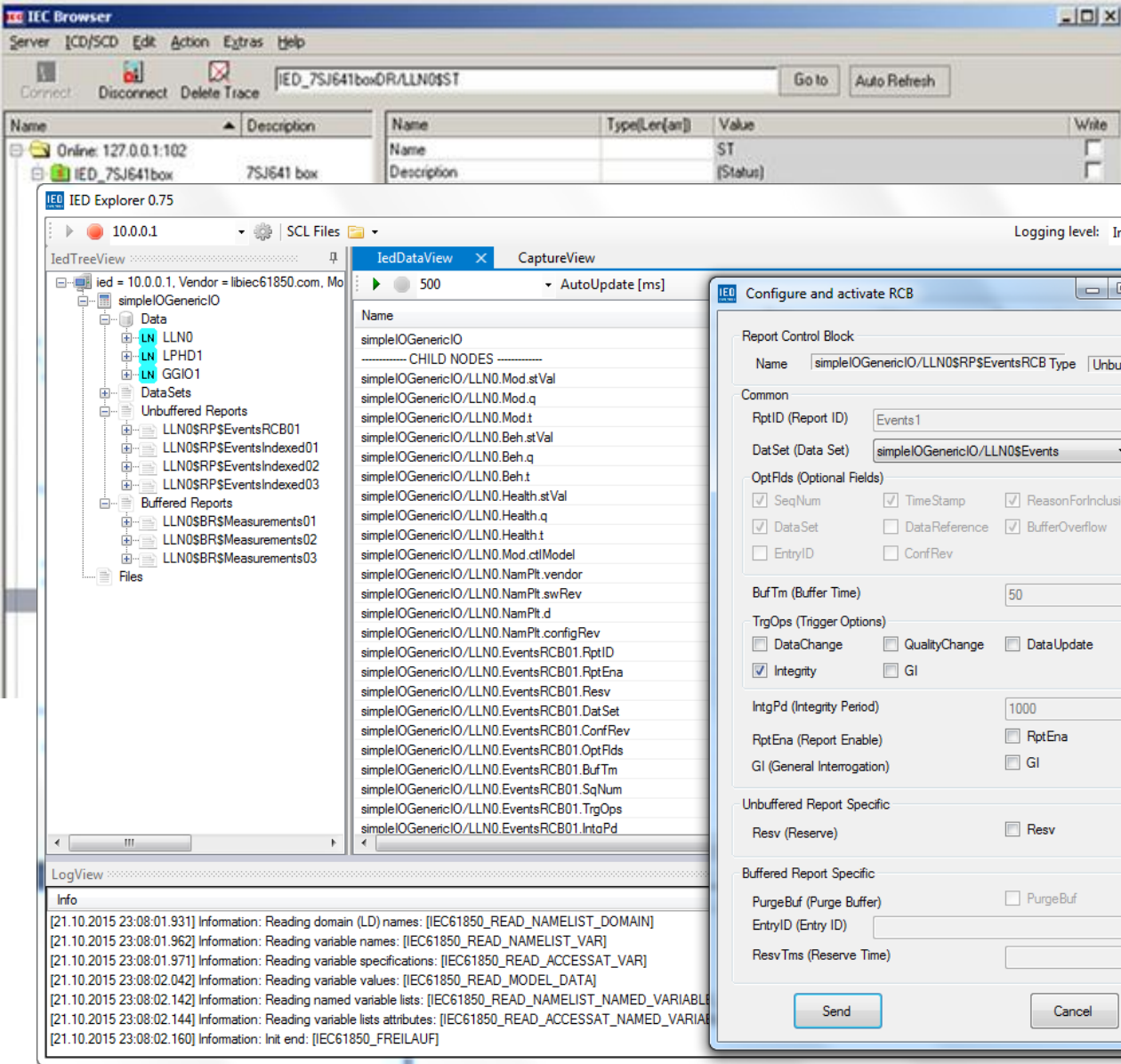
ИДИ В ШКОЛУ







\$ nmap 172.*.*.*



Personal Open source Business Explore

Search

Repositories 4

- [Code](#) 1,188
- [Issues](#) 4
- [Users](#)

Languages

- Python 1
- C 1

[Advanced search](#) [Cheat sheet](#)

stevenblair/tunnel61850
IEC 61850 GOOSE and Sampled Value tunnelling using UDP
Updated on 16 Aug 2012

mdehus/goose-IEC61850-scapy
Updated on 2 Feb 2014

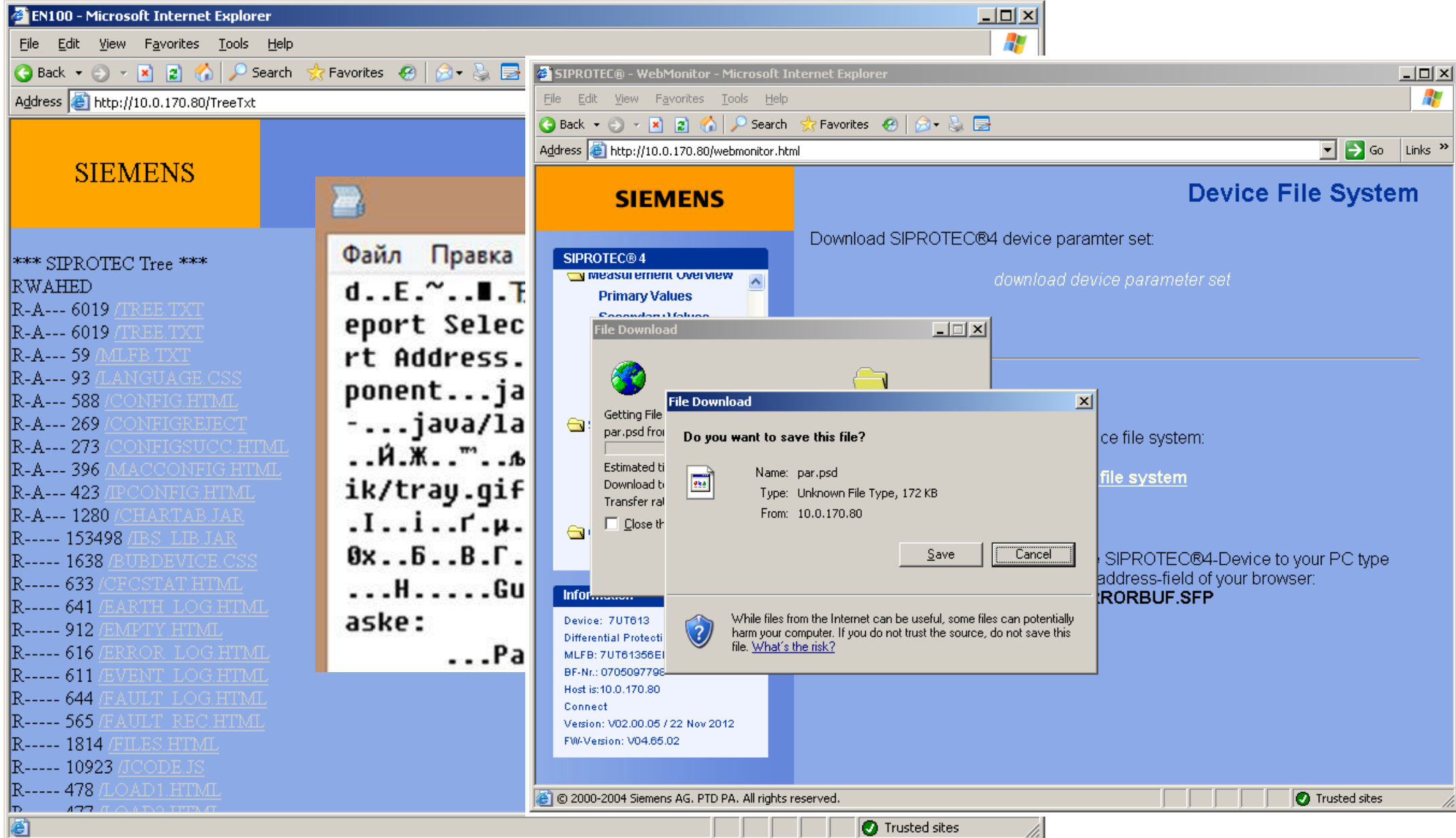
hectordelahoz/ProcessBusIec61850
This project contains an OMNeT++/INET extension to support IEC6 communication (GOOSE and SV)

SIEMENS

DIGSI 4

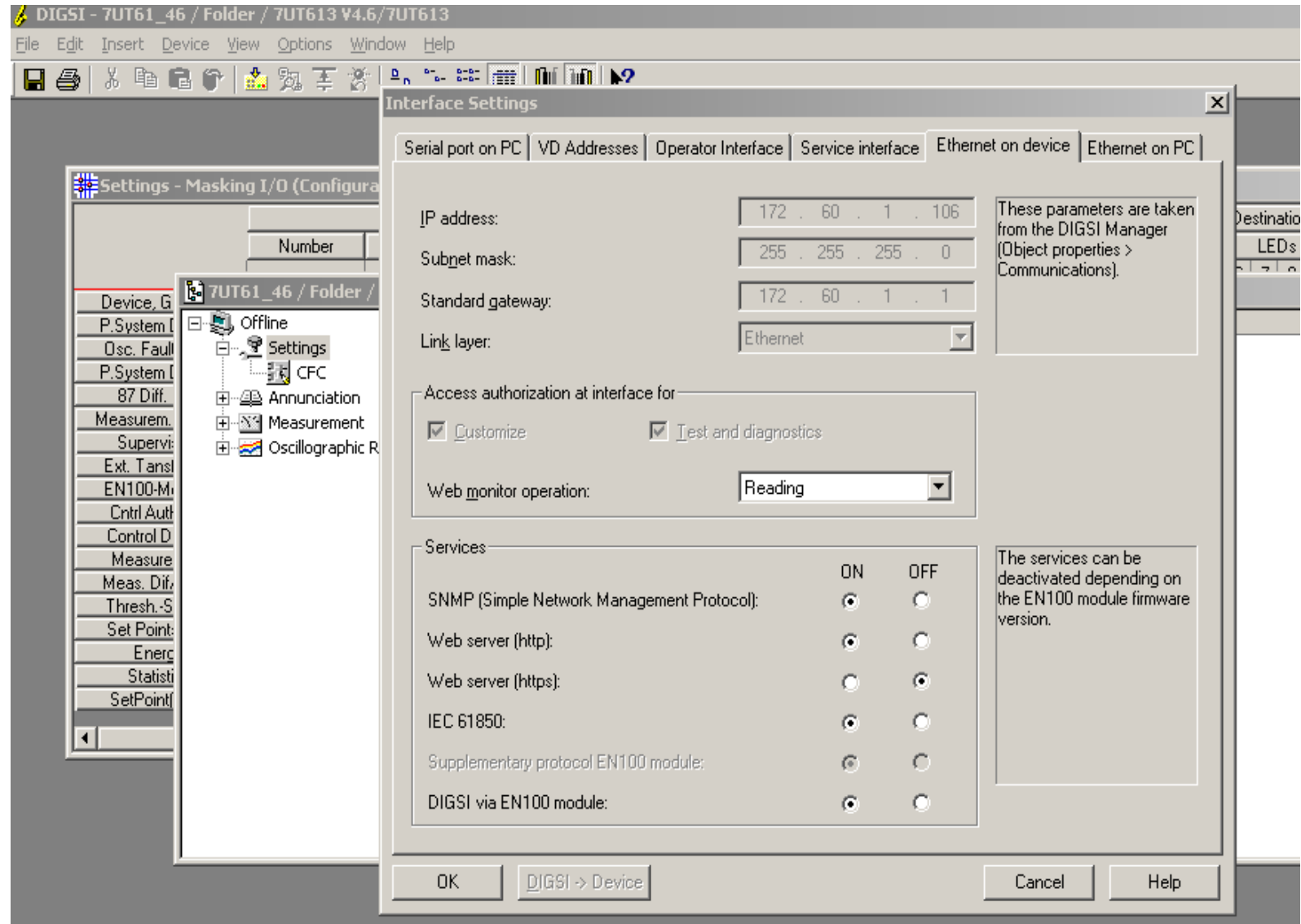
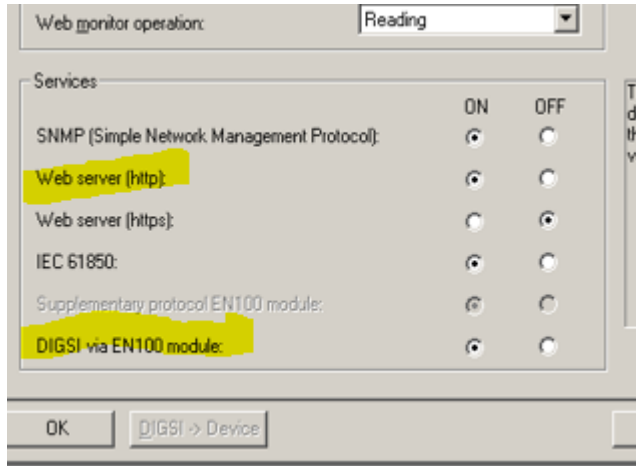
One Software for all SIPROTEC Protection Relays





Почему WEB?

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



Positive Hack Days VI – CTF style

The screenshot shows the DIGSI software interface. On the left is a tree view with the following structure:

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

The main window displays a tree view with the following structure:

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

The 'Test' folder is expanded, showing a 'Select function' list:

- Hardware Test
- Generate Indications
- Test Wave Form

The 'Test device inputs and outputs' dialog box is open, displaying a table of binary 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 00
	LEDs 1	🔴	OFF	STATUS_Q1

At the bottom of the dialog box, there is a checked checkbox for 'Automatic Update (20 sec)' and an 'Update' button. 'Close' and 'Help' buttons are also present.









Спасибо!

POSITIVE TECHNOLOGIES

ptsecurity.ru