

“Практическая демонстрация типовых атак и 0-day уязвимостей в SCADA и PLC-контроллерах”

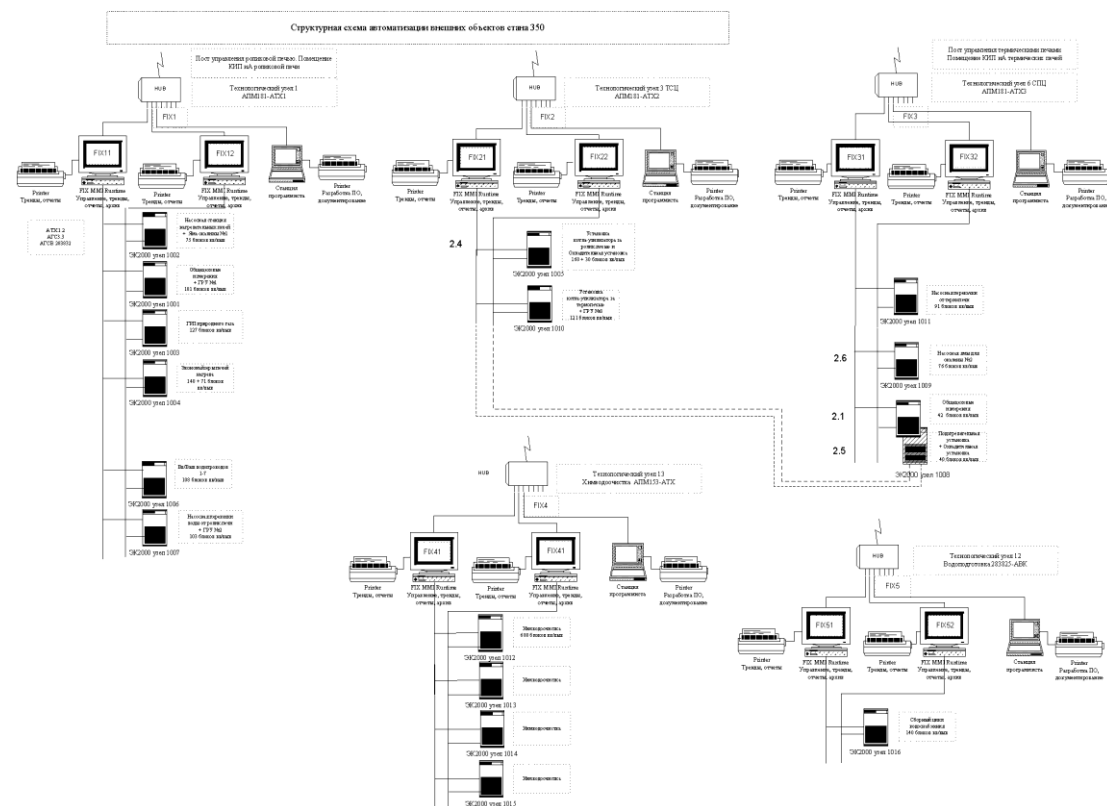
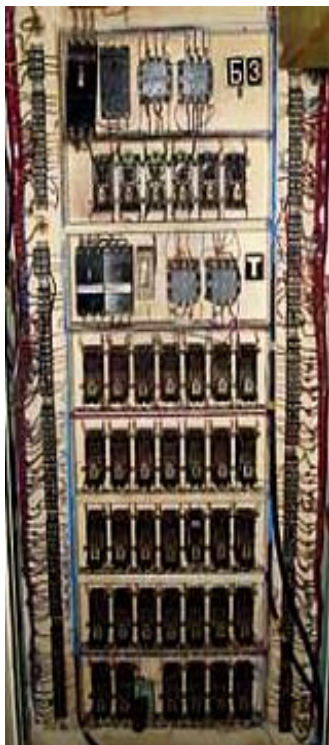
Павел Волобуев

Александр Миноженко

Александр Поляков

Современная промышленная система

От релейных систем к современной АСУ



Современная промышленная система

Миф: промышленные системы не подвержены угрозам

Технологии, используемые в АСУ ТП сегодня:

Windows

Linux

Ethernet

HTTP

XML

DCOM

.NET

SQL

SOAP

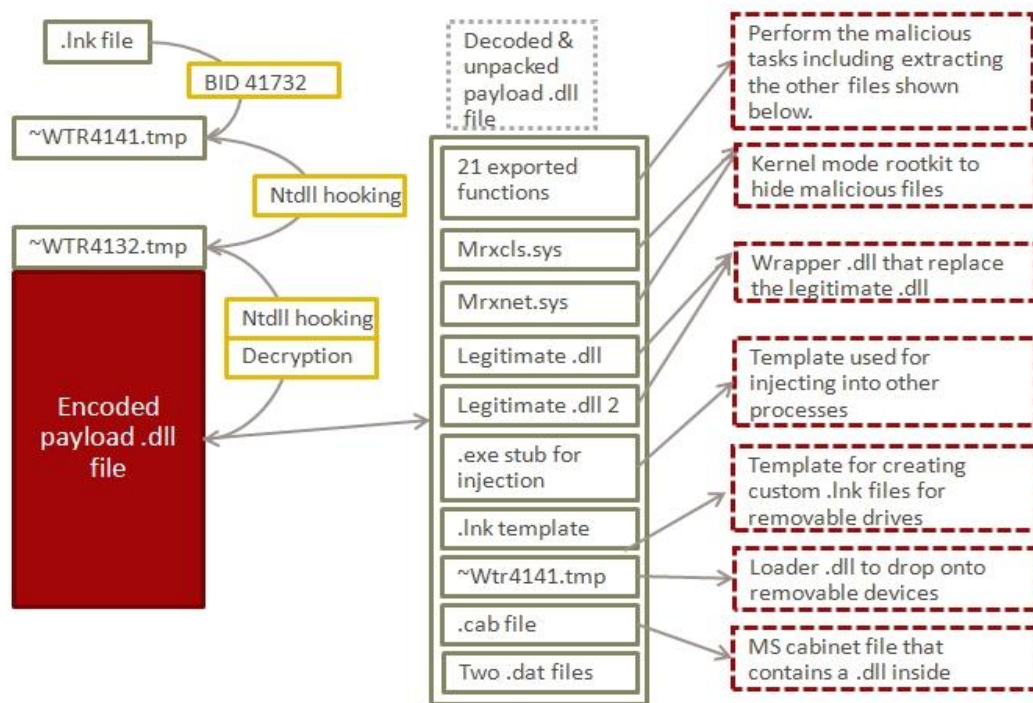
Современная промышленная система

Миф: промышленные системы не подвержены угрозам

1. Промышленные системы вместе со всеми положительными аспектами использования этих технологий получили «в подарок» и все их проблемы
2. Уязвимости этих технологий широко известны.
3. Эксплуатация уязвимостей в промышленной среде хоть и имеет свою специфику, но возможна и почти не отличается от эксплуатации в корпоративной сети.

Современная промышленная система

Stuxnet:



4 уязвимости Windows

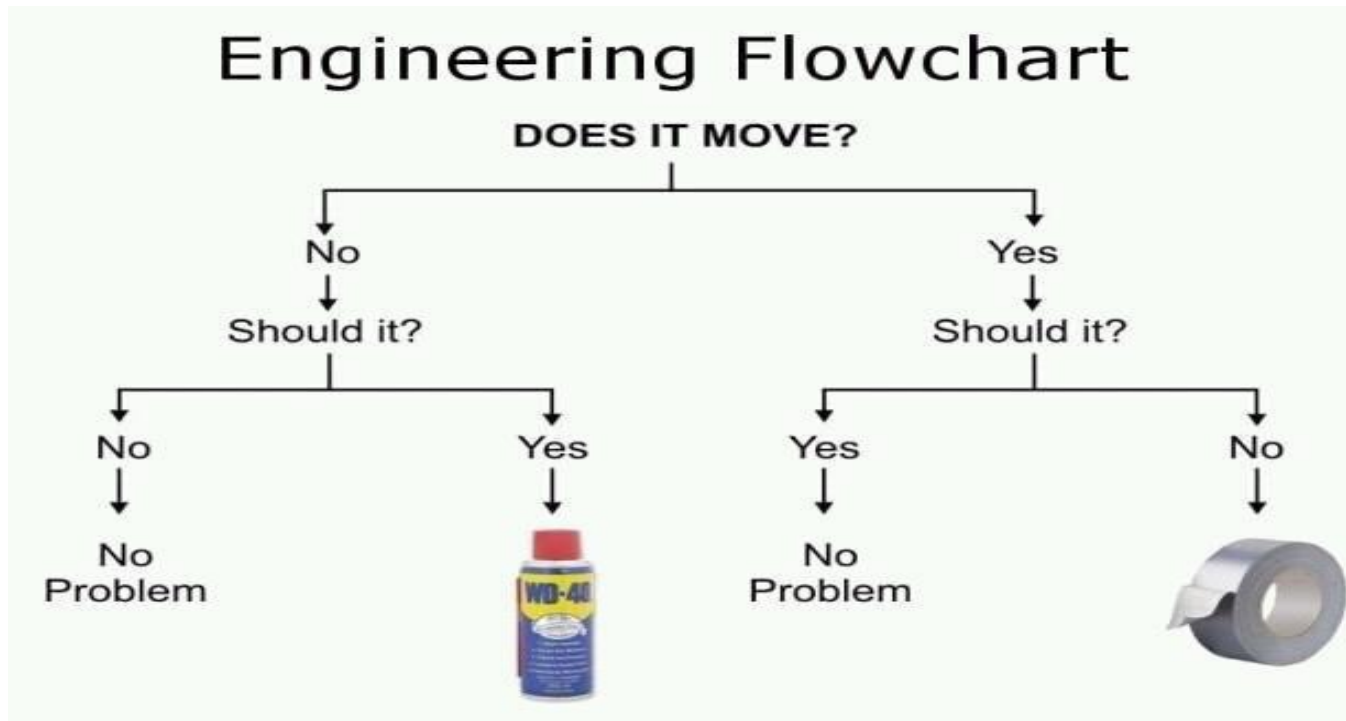
Украденная цифровая подпись драйвера

Уязвимость в ПО от Siemens

Стандартные учетные записи

Причины

Производители и инженеры КИПиА уделяют основное внимание функционалу и производительности, а также обеспечению работоспособности, часто в ущерб безопасности системы



Проблемные сегменты

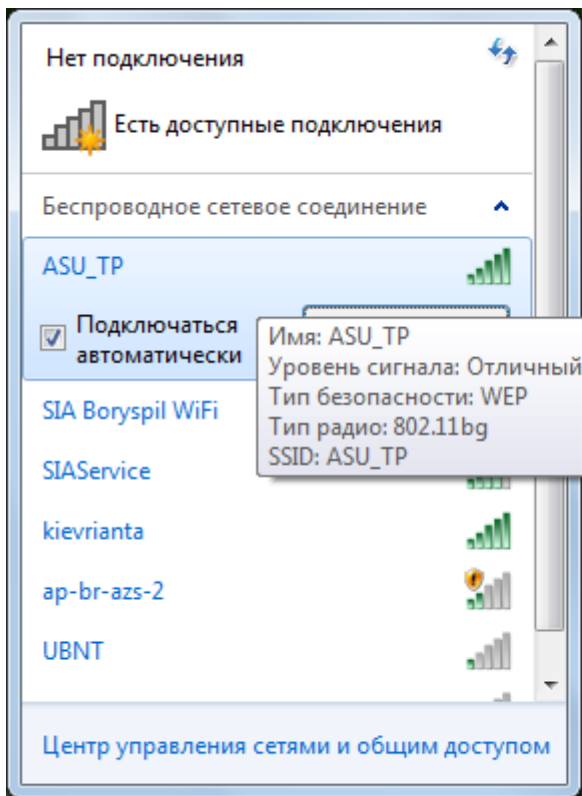
Беспроводные коммуникации

Дистанционные методы управления

Удаленная диспетчеризация

Веб-технологии

Проблемные сегменты



SSID сети раскрывает ее предназначение

WEP-шифрование является нестойким, и взламывается за минуты.

Угрозы

Вирусы

Троянские программы

Черви

DoS-атаки

ARP-спуфинг

Некорректное обновление ПО

Несанкционированный доступ к данным

Человеческий фактор

Воздействие на технологический процесс: теперь уже реальность

Даже в примитивной схеме есть место для проблем с безопасностью

Сервер АСУТП считывает информацию о производительности насоса и уровне в резервуаре и задает контрольные значения для контроллеров (ПЛК)

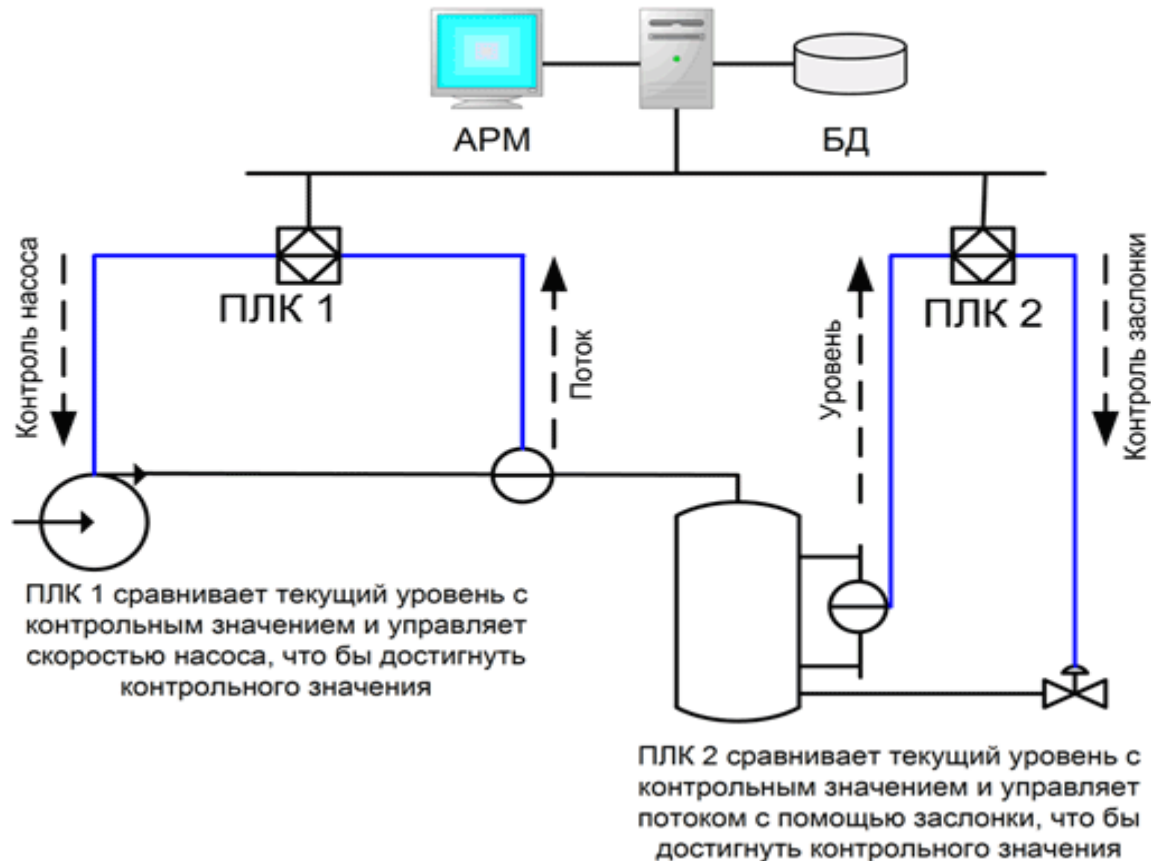


Рисунок: 1998, Cisco

Немного практики. 4 производителя

SCADA

**WellinTech**

PLC



OPC Systems .NET

Michelin Tire

JBT AeroTech

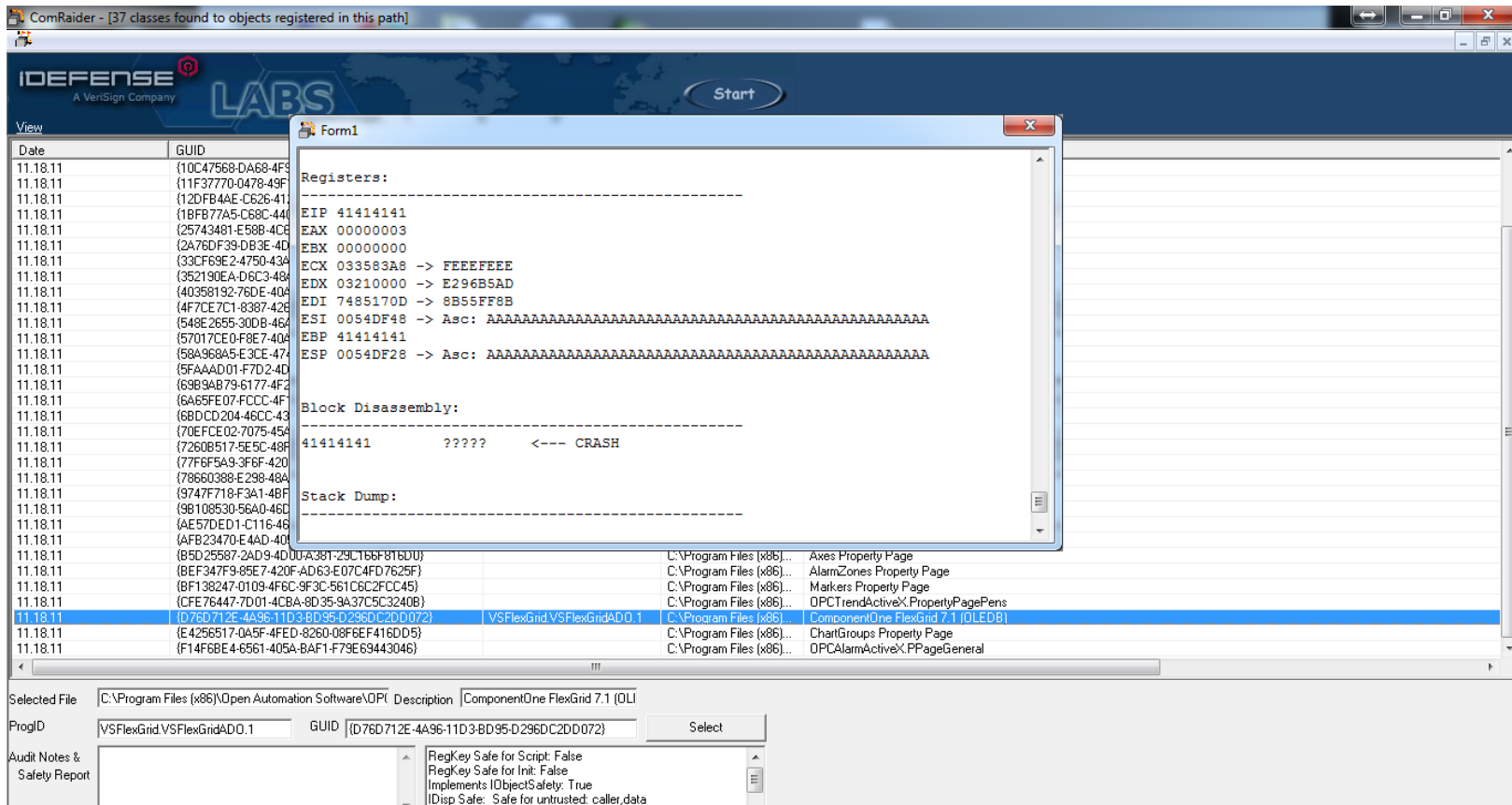


Dart Oil and Gas

Blue Pillar - Hospital

Nuclear powered U.S. Navy submarines and aircraft carriers.

1. OPC Systems .NET ActiveX BOF 0-day DSECRG-00249



ComRaider - [37 classes found to objects registered in this path]

IDEFENSE LABS A VeriSign Company

Start

View

Date	GUID	ProgID	Description
11.18.11	{10C47568-DA68-4F9...		
11.18.11	{11F37770-0478-49F...		
11.18.11	{120FB4AE-C626-41...		
11.18.11	{18FB77A5-C68C-44...		
11.18.11	{25743481-E588-4C...		
11.18.11	{2A76DF39-DB3E-4D...		
11.18.11	{33CF68E2-4750-43...		
11.18.11	{352190EA-D6C3-4...		
11.18.11	{40358192-76DE-40...		
11.18.11	{4F7CE7C1-8387-42...		
11.18.11	{548E2655-30D8-46...		
11.18.11	{57017CE0-F8E7-40...		
11.18.11	{58A968A5-E3CE-47...		
11.18.11	{5FAAAD01-F7D2-4D...		
11.18.11	{69B9AB79-6177-4F...		
11.18.11	{6A65FE07-FCCC-4F...		
11.18.11	{6BDCD204-46CC-43...		
11.18.11	{70EFC02-7075-45...		
11.18.11	{7260B517-5E5C-48...		
11.18.11	{77F6F5A9-3F6F-42...		
11.18.11	{78660388-E298-48...		
11.18.11	{9747F718-F3A1-48...		
11.18.11	{9B108530-56A0-46...		
11.18.11	{AE57DED1-C116-46...		
11.18.11	{AFB23470-E4AD-40...		
11.18.11	{B5D25587-2AD9-4D...	C:\Program Files [x86]...	Axis Property Page
11.18.11	{BEF347F9-85E7-420F-AD63-E07C4FD7625F}	C:\Program Files [x86]...	AlarmZones Property Page
11.18.11	{BF138247-0109-4F6C-9F3C-561C6C2FCC45}	C:\Program Files [x86]...	Markers Property Page
11.18.11	{CFE76447-7D01-4CBA-8D35-9A37C5C32408}	C:\Program Files [x86]...	OPCTrendActiveX.PropertyPagePens
11.18.11	{D76D712E-4A96-11D3-BD95-D296DC2DD072}	C:\Program Files [x86]...	ComponentOne FlexGrid 7.1 [OLEDB]
11.18.11	{E4256517-0A5F-4FED-8260-08F6EF416DD5}	C:\Program Files [x86]...	ChartGroups Property Page
11.18.11	{F14F6BE4-6561-405A-BAF1-F79E69443046}	C:\Program Files [x86]...	OPCALamActiveX.PPPageGeneral

Form1

Registers:

```

EIP 41414141
EAX 00000003
EBX 00000000
ECX 033583A8 -> FFFFFFFF
EDX 03210000 -> E296B5AD
EDI 7485170D -> 8B55FF8B
ESI 0054DF48 -> Asc: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
EBP 41414141
ESP 0054DF28 -> Asc: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

```

Block Disassembly:

```

41414141      ?????    <---- CRASH

```

Stack Dump:

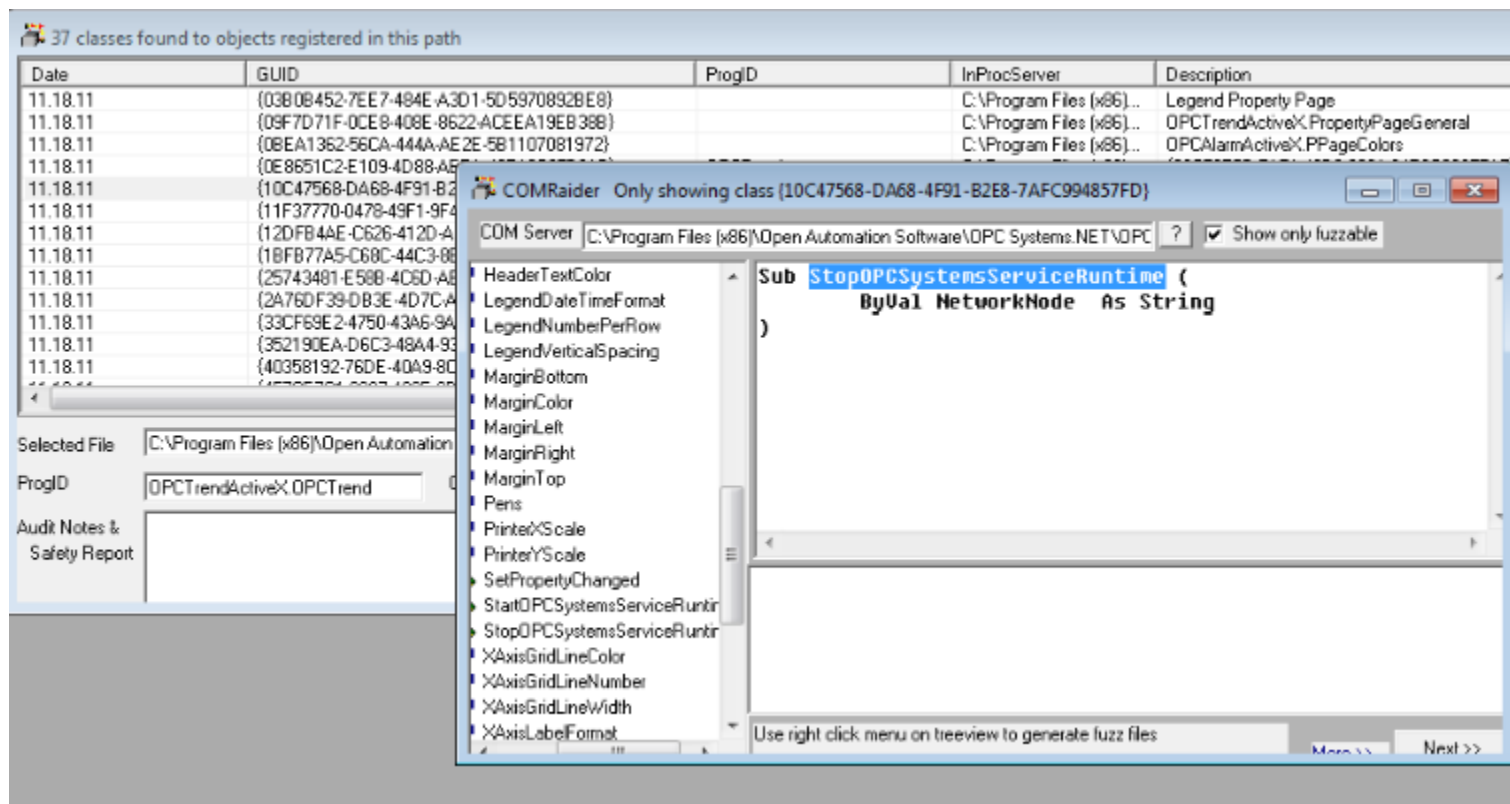
Selected File: C:\Program Files [x86]\Open Automation Software\OPC\ Description: ComponentOne FlexGrid 7.1 [OLEDB]

ProgID: VSFlexGrid.VSFlexGridADO.1 GUID: {D76D712E-4A96-11D3-BD95-D296DC2DD072} Select

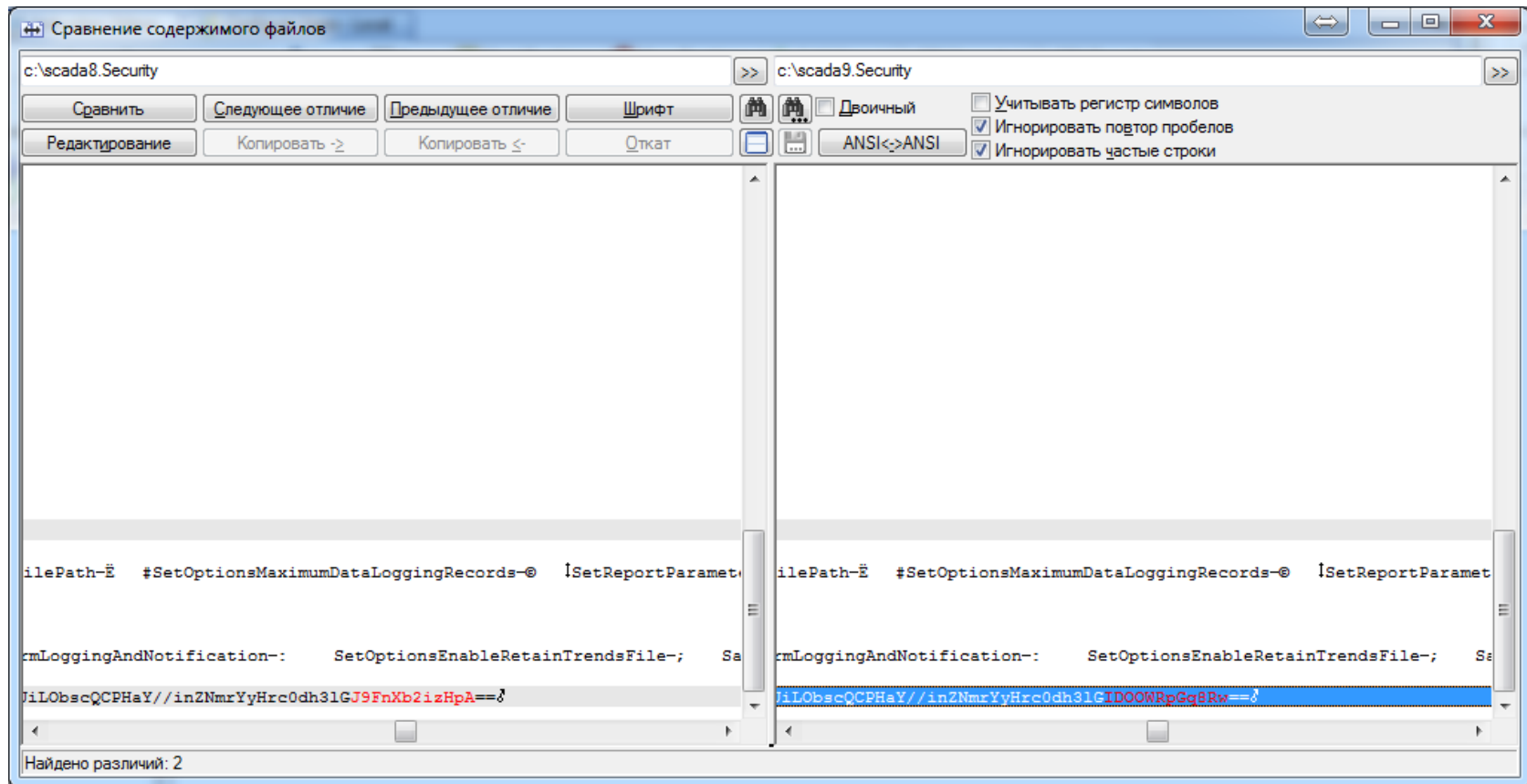
Audit Notes & Safety Report

RegKey Safe for Script: False
RegKey Safe for Init: False
Implements IOObjectSafety: True
Disp Safe: Safe for untrusted: caller,data

2. OPC Systems .NET ActiveX Unauthorized DOS DSECRG-00249



3. OPC Systems .NET insecure password storage DSECRG-00248



large projects in China such as South-to-North Water Transfer Project , West-East Natural Gas Transmission Project ,The Three Gorges Dam



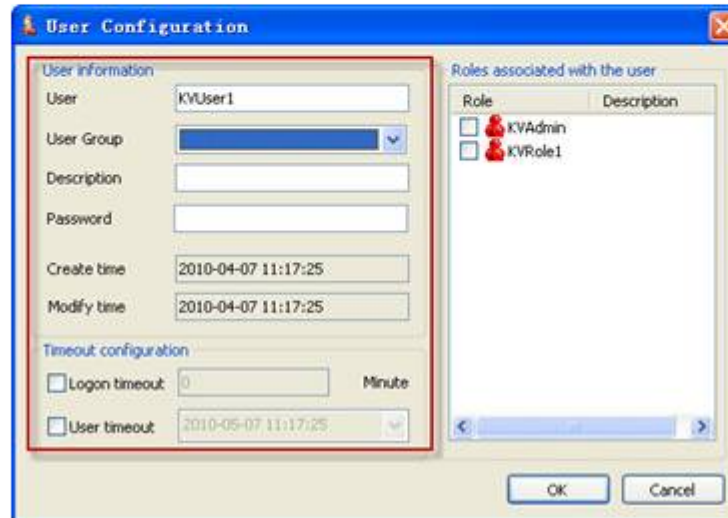
WellinTech is engaged in the automation software, independent R&D, marketing and service. By 2009, WellinTech has more than 260 employees, and is the largest professional automation software company in Asia.

4. KingSCADA 3.0 - Default passwords

The system provides a system administrator user- KVAdministrator which can not be deleted or edited (except for the password). The password defaults to be “administrator”. The rights of the user are as follows:

1. No logon timeout
2. No user timeout
3. Automatically associated with KVAdmin applied in the whole station.

The second step: Click “User” with the right mouse button in Security Management System dialog box, and then select “New User” in the context menu popped up, a dialog box will be popped up as the picture below shows:



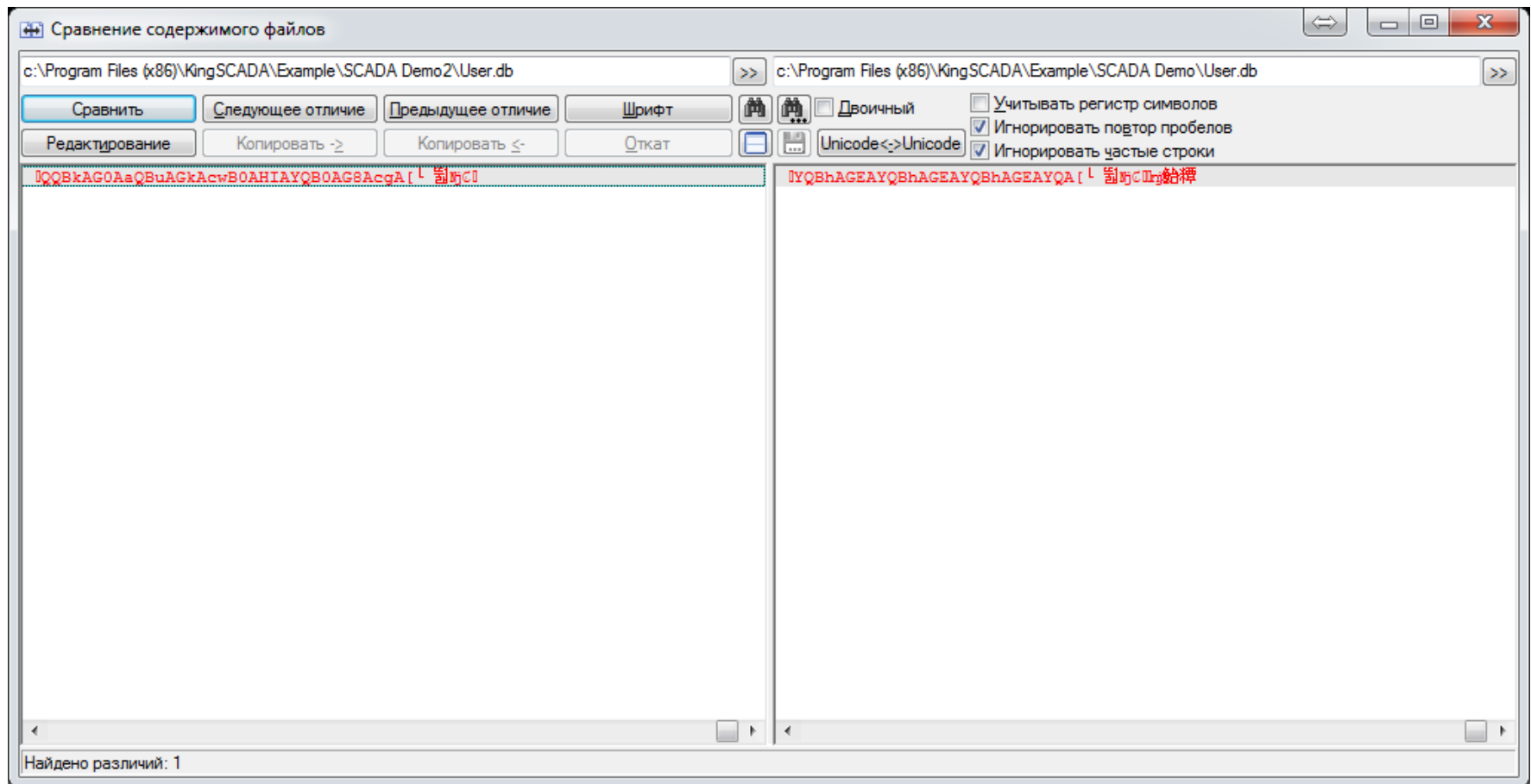
The image shows a 'User Configuration' dialog box with the following fields and sections:

- User information:**
 - User: KVUser1
 - User Group: [dropdown menu]
 - Description: [text field]
 - Password: [text field]
 - Create time: 2010-04-07 11:17:25
 - Modify time: 2010-04-07 11:17:25
- Timeout configuration:**
 - ☐ Logon timeout: 0 Minute
 - ☐ User timeout: 2010-05-07 11:17:25
- Roles associated with the user:**

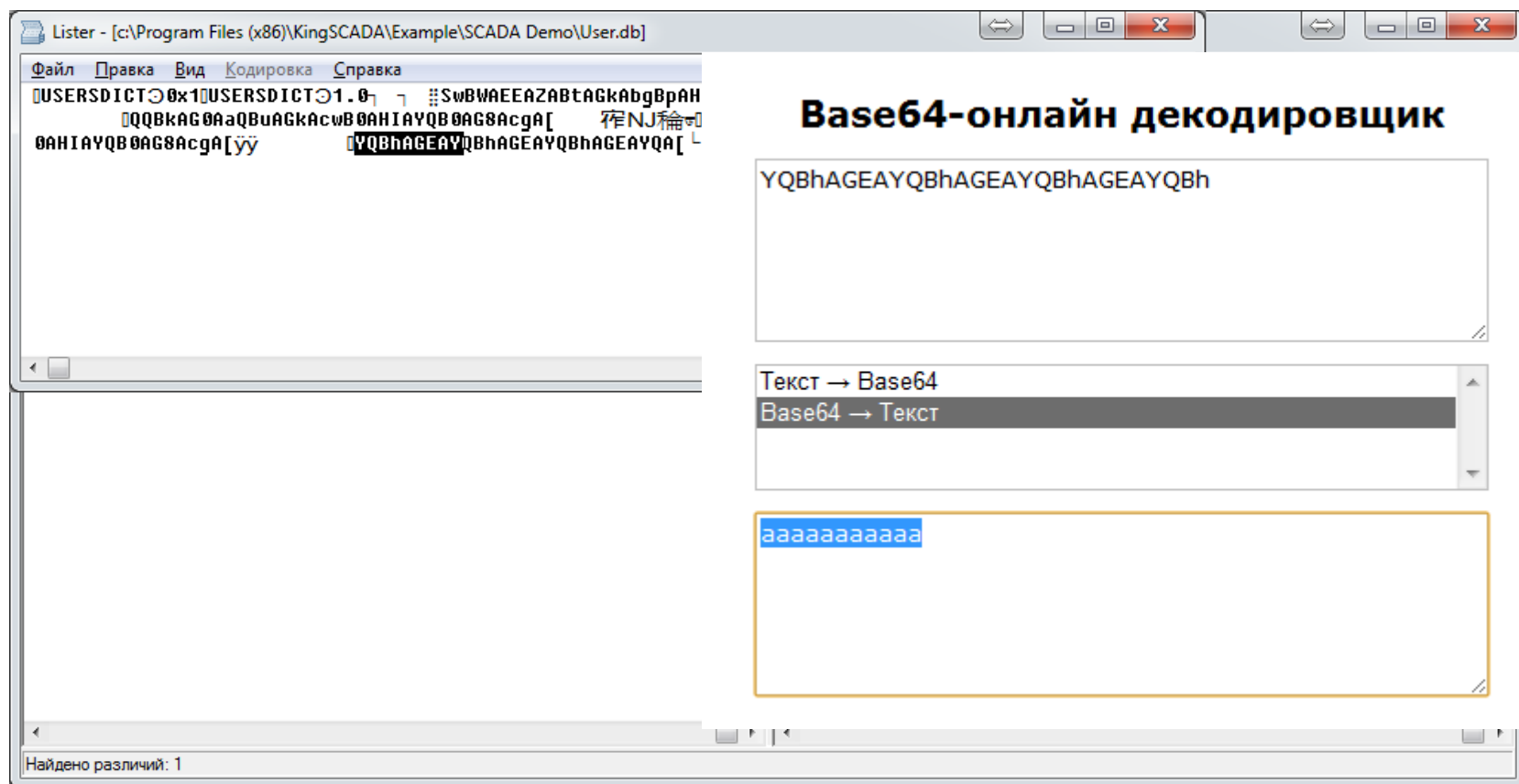
Role	Description
<input type="checkbox"/> KVAdmin	
<input type="checkbox"/> KVRole1	

Buttons: OK, Cancel

5. KingSCADA 3.0 - Insecure password encryption [DSECRG-00247]



5. KingSCADA 3.0 - Insecure password encryption [DSECRG-00247]



SCADA весело но PLC ещё интереснее и неизведаннее



6. WAGO 750 PLC – Default passwords [DSECRG-00243]

When using a proxy server, the proxy server must be bypassed for local addresses. Information on how to bypass the proxy server for local addresses can be found in the help section of your browser under “Proxy server” or “LAN settings”.

A login is required to access the configuration pages via hyperlinks. The following users are created by default:

User	Password
admin	wago
user	user
guest	guest

Fig. 7: Users and passwords of the 750-841 Controller’s WEB server

Using firmware version (09) and above, the process data can be displayed in the right window of the “IO config” configuration page. Access to process data is based on the “GenIoConf.xml” file in the “etc” folder of the node’s file system. Data generation is disabled by default and can be activated on the “Features” configuration page.



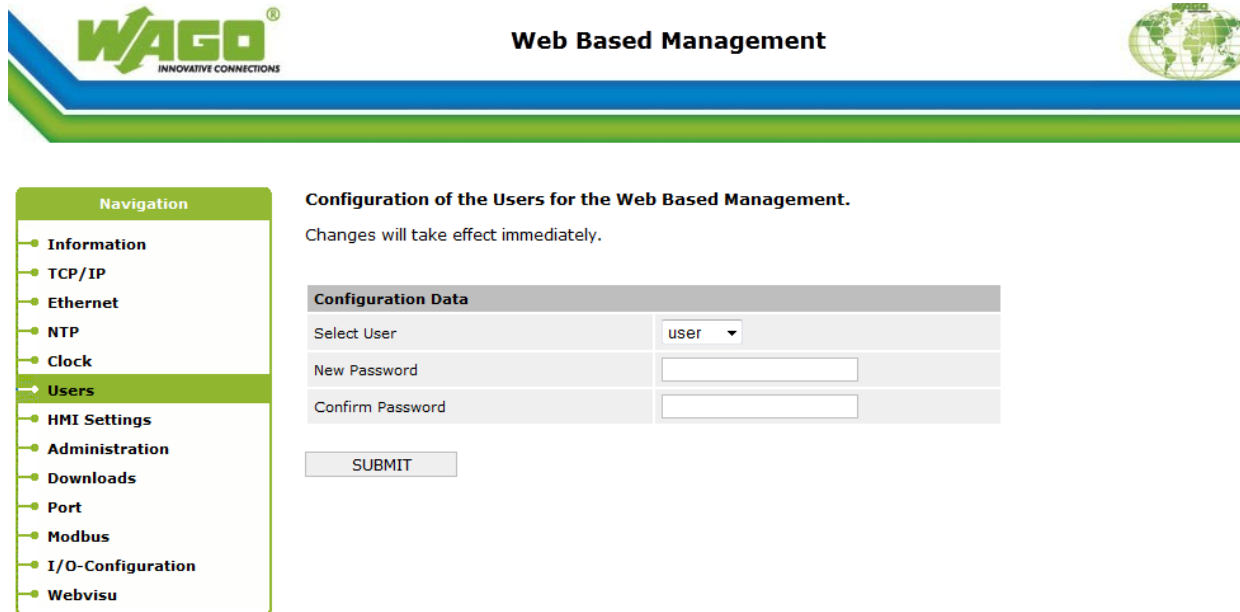
7. WAGO 750 PLC – information disclose [DSECRG-00245]

```
//PLC/persist.dat  
//PLC/DEFAULT.CHK  
//PLC/minml.jar  
//PLC/webvisu.jar  
//PLC/webvisu.htm  
//PLC/visu_ini.xml  
//PLC/alm_ini.xml  
//PLC/graben_ddevis.txt  
//PLC/tabelle_variablen_xml.zip  
//PLC/tabelle_array_xml.zip
```

8. WAGO 750 PLC – Unauthorized firmware access [DSECRG-00244]

GET Http://ipaddress:/PLC/DEFAULT.PRG

9. WAGO 750 PLC – CSRF password change [DSECRG-00246]



The image shows the WAGO Web Based Management interface. At the top, there is a header with the WAGO logo (green and blue stylized 'WAGO' with 'INNOVATIVE CONNECTIONS' below it) and the text 'Web Based Management' next to a globe icon. Below the header is a navigation menu on the left with the following items: Information, TCP/IP, Ethernet, NTP, Clock, Users (highlighted with a green bar and a right-pointing arrow), HMI Settings, Administration, Downloads, Port, Modbus, I/O-Configuration, and Webvisu. The main content area is titled 'Configuration of the Users for the Web Based Management.' and includes a note 'Changes will take effect immediately.' Below this is a 'Configuration Data' section with three rows: 'Select User' with a dropdown menu showing 'user', 'New Password' with a text input field, and 'Confirm Password' with a text input field. At the bottom of this section is a 'SUBMIT' button.

POST /SETWEBPASS?

ULIST=admin&PASS1=aaaa&PASS2=aaaa&SUBMIT=SUBMIT

передовой чешский производитель промышленных систем



Machinery



Ironworks, metallurgy



Mines, hoist engines



Chemistry, petrochemistry,
pharmacy



Building materials industry



Electrical engineering



Energetics



Central heating



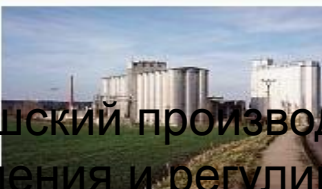
Building installations



Water treatment



передовой чешский производитель промышленных систем управления и регулирования



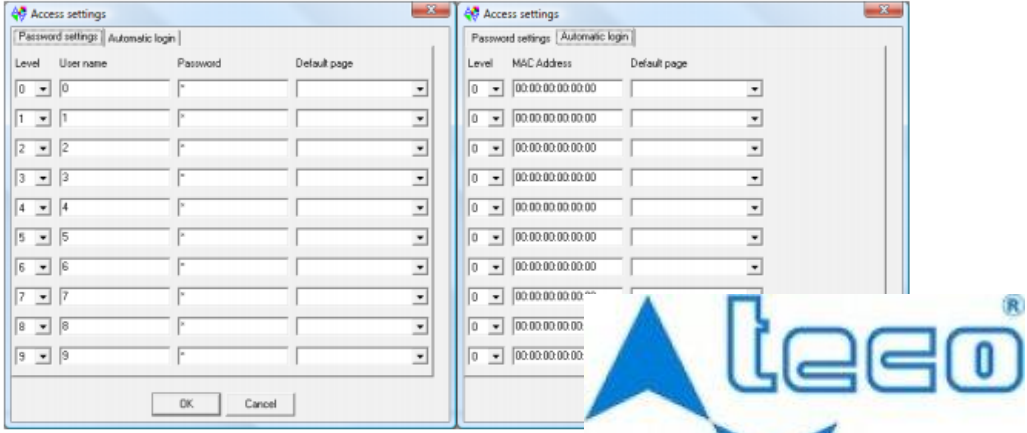
10. TECOMAT PLC – default passwords [DSECRG-00250]

www.tecomat.com/wpimages/other/DOCS/eng/TXV00328_02_Mosaic_WebMaker_en.pdf

Не удастся отобразить некоторые фрагменты этого PDF-документа. Открыть его в приложении Adobe Reader? password

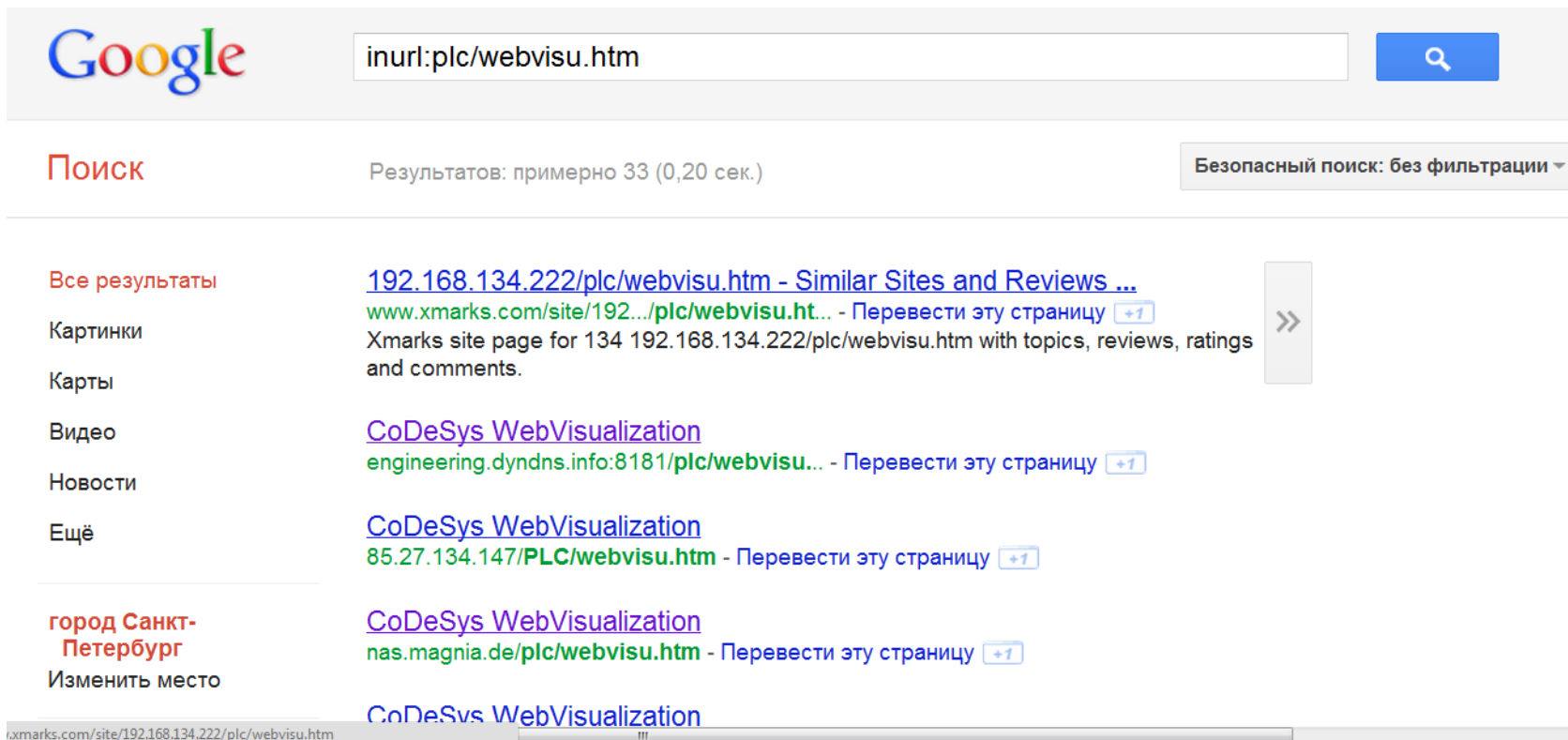
WebMaker tool

2.4 Password settings



On the card Password settings there are ten pairs of user name - password. While logging in the web server via the web browser, the user name and password must be set for each pair. Default settings is user name same as the password for level 0 (the user name is 0 and password 0, too.).

Поиск в Google WAGO PLC



The screenshot shows a Google search interface. The search bar contains the text 'inurl:plc/webvisu.htm'. Below the search bar, the word 'Поиск' (Search) is displayed in red. To the right of 'Поиск', it says 'Результатов: примерно 33 (0,20 сек.)'. Further right, there is a button labeled 'Безопасный поиск: без фильтрации' (Safe search: without filtering). On the left side, there is a vertical list of filters: 'Все результаты' (All results), 'Картинки' (Images), 'Карты' (Maps), 'Видео' (Videos), 'Новости' (News), 'Ещё' (More), 'город Санкт-Петербург' (city Saint-Petersburg), and 'Изменить место' (Change location). The main search results area shows three entries. Each entry consists of a title, a URL, and a snippet. The first entry is '192.168.134.222/plc/webvisu.htm - Similar Sites and Reviews ...' with a snippet from xmarks.com. The second entry is 'CoDeSys WebVisualization' with a URL 'engineering.dyndns.info:8181/plc/webvisu...' and a snippet. The third entry is 'CoDeSys WebVisualization' with a URL '85.27.134.147/PLC/webvisu.htm' and a snippet. Each entry has a '+1' button next to it. At the bottom of the search results, there is a horizontal bar with the URL 'xmarks.com/site/192.168.134.222/plc/webvisu.htm' and a '!!!' icon.

Google

inurl:plc/webvisu.htm

Поиск

Результатов: примерно 33 (0,20 сек.)

Безопасный поиск: без фильтрации ▾

Все результаты

Картинки

Карты

Видео

Новости

Ещё

город Санкт-Петербург

Изменить место

192.168.134.222/plc/webvisu.htm - Similar Sites and Reviews ...
www.xmarks.com/site/192.../plc/webvisu.ht... - Перевести эту страницу +1
Xmarks site page for 134 192.168.134.222/plc/webvisu.htm with topics, reviews, ratings and comments.

CoDeSys WebVisualization
engineering.dyndns.info:8181/plc/webvisu... - Перевести эту страницу +1

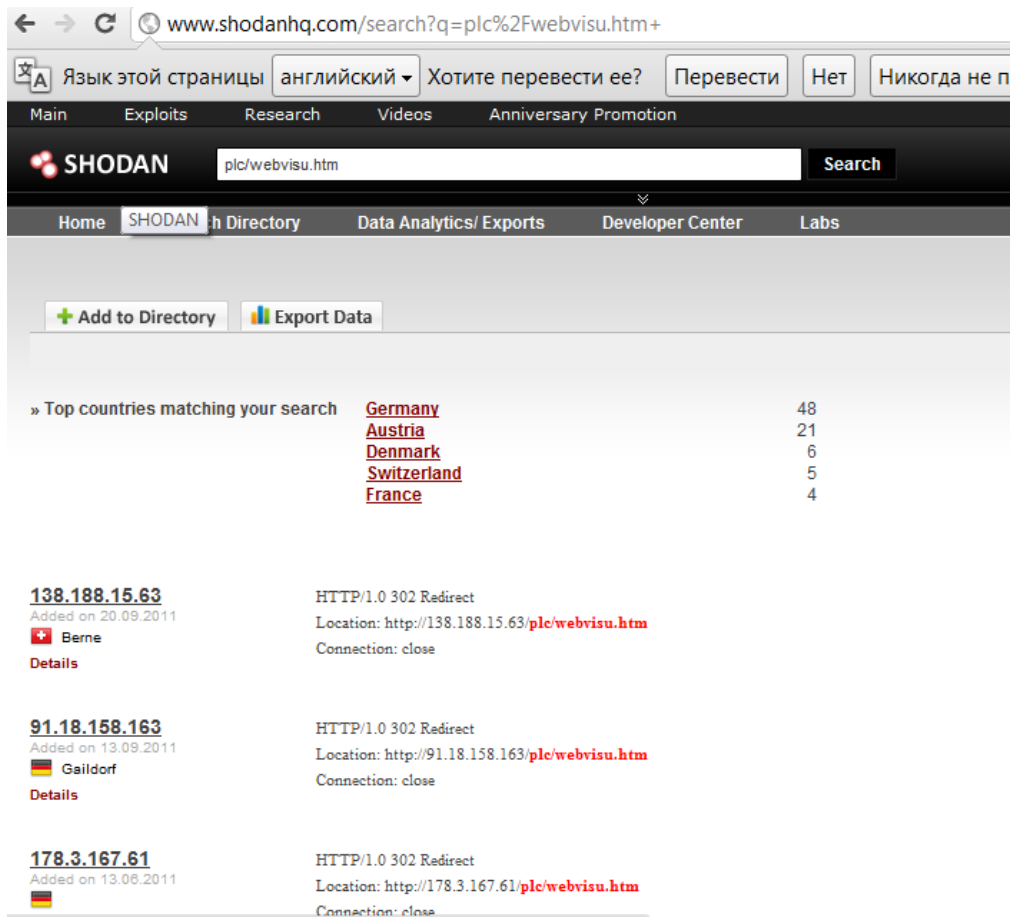
CoDeSys WebVisualization
85.27.134.147/PLC/webvisu.htm - Перевести эту страницу +1

CoDeSys WebVisualization
nas.magnia.de/plc/webvisu.htm - Перевести эту страницу +1

CoDeSys WebVisualization

xmarks.com/site/192.168.134.222/plc/webvisu.htm

Поиск в Shodan WAGO PLC



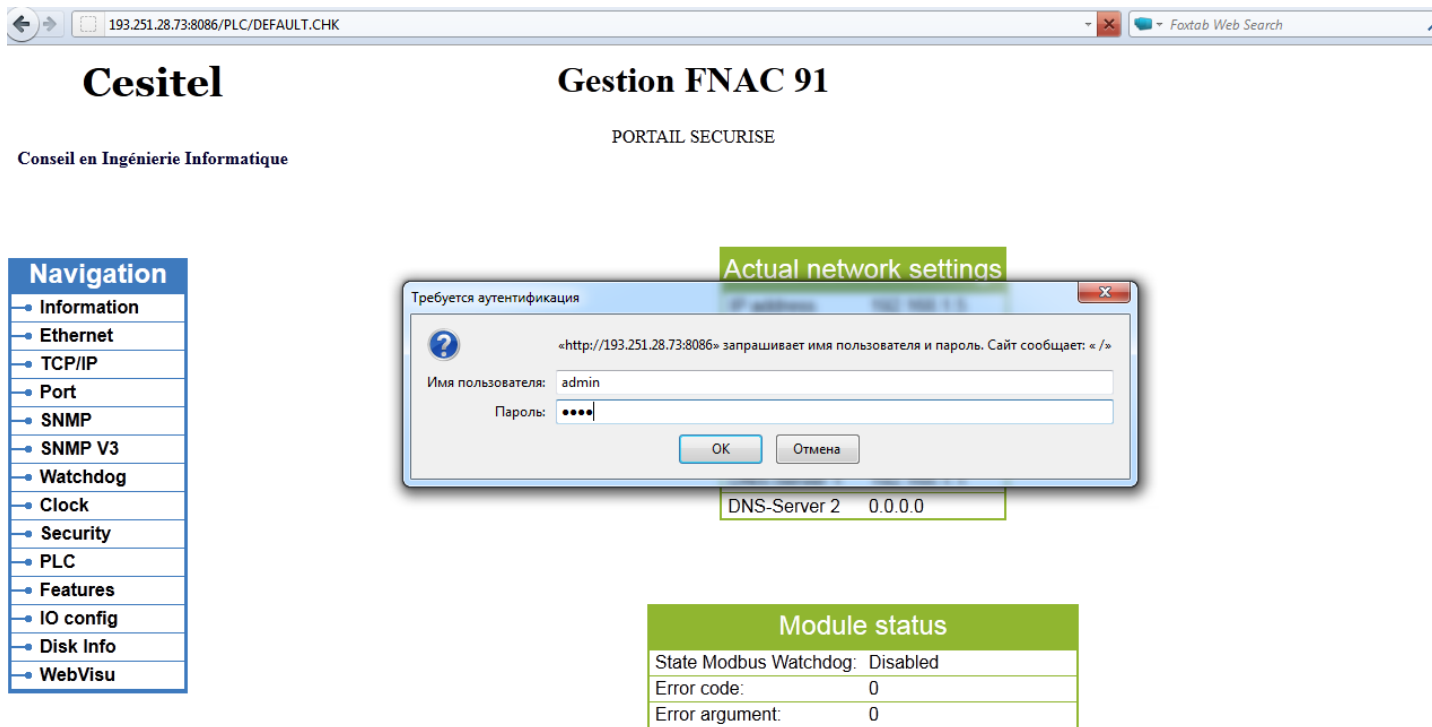
The screenshot shows a web browser window with the URL `www.shodanhq.com/search?q=plc%2Fwebvisu.htm+`. The page displays search results for the query `plc/webvisu.htm`. The results are organized into a table with columns for IP address, location, and connection details.

IP Address	Location	Connection
138.188.15.63	Germany	HTTP/1.0 302 Redirect
91.18.158.163	Austria	HTTP/1.0 302 Redirect
178.3.167.61	Denmark	HTTP/1.0 302 Redirect

Additional details for each result include the date added, the location name, and a link to the details page.

- 138.188.15.63**: Added on 20.09.2011, Location: `http://138.188.15.63/plc/webvisu.htm`, Connection: close
- 91.18.158.163**: Added on 13.09.2011, Location: `http://91.18.158.163/plc/webvisu.htm`, Connection: close
- 178.3.167.61**: Added on 13.08.2011, Location: `http://178.3.167.61/plc/webvisu.htm`, Connection: close

А теперь в реальном мире



The screenshot shows a web browser window with the address bar displaying '193.251.28.73:8086/PLC/DEFAULT.CHK'. The page title is 'Cesitel Gestion FNAC 91' and the subtitle is 'PORTAIL SECURISE'. The main content area is divided into two sections: 'Navigation' on the left and 'Actual network settings' on the right.

Navigation

- Information
- Ethernet
- TCP/IP
- Port
- SNMP
- SNMP V3
- Watchdog
- Clock
- Security
- PLC
- Features
- IO config
- Disk Info
- WebVisu

Actual network settings

Требуется аутентификация

«http://193.251.28.73:8086» запрашивает имя пользователя и пароль. Сайт сообщает: « /»

Имя пользователя: admin

Пароль:

OK Отмена

DNS-Server 2 0.0.0.0

Module status

State Modbus Watchdog:	Disabled
Error code:	0
Error argument:	0

А теперь в реальном мире



Cesitel

Gestion FNAC 91

Conseil en Ingénierie Informatique

PORTAIL SECURISE

This page is intended to disable the basic authentication. Additionally you can set new passwords for the existing user. The new values are stored in an EEPROM and changes will take effect after the next software or hardware reset.

Navigation

- Information
- Ethernet
- TCP/IP
- Port
- SNMP
- SNMP V3
- Watchdog
- Clock
- Security
- PLC
- Features
- IO config
- Disk Info
- WebVisu

Webserver Security

Webserver authentication enabled ☒

UNDO

SUBMIT

Webserver and FTP User configuration

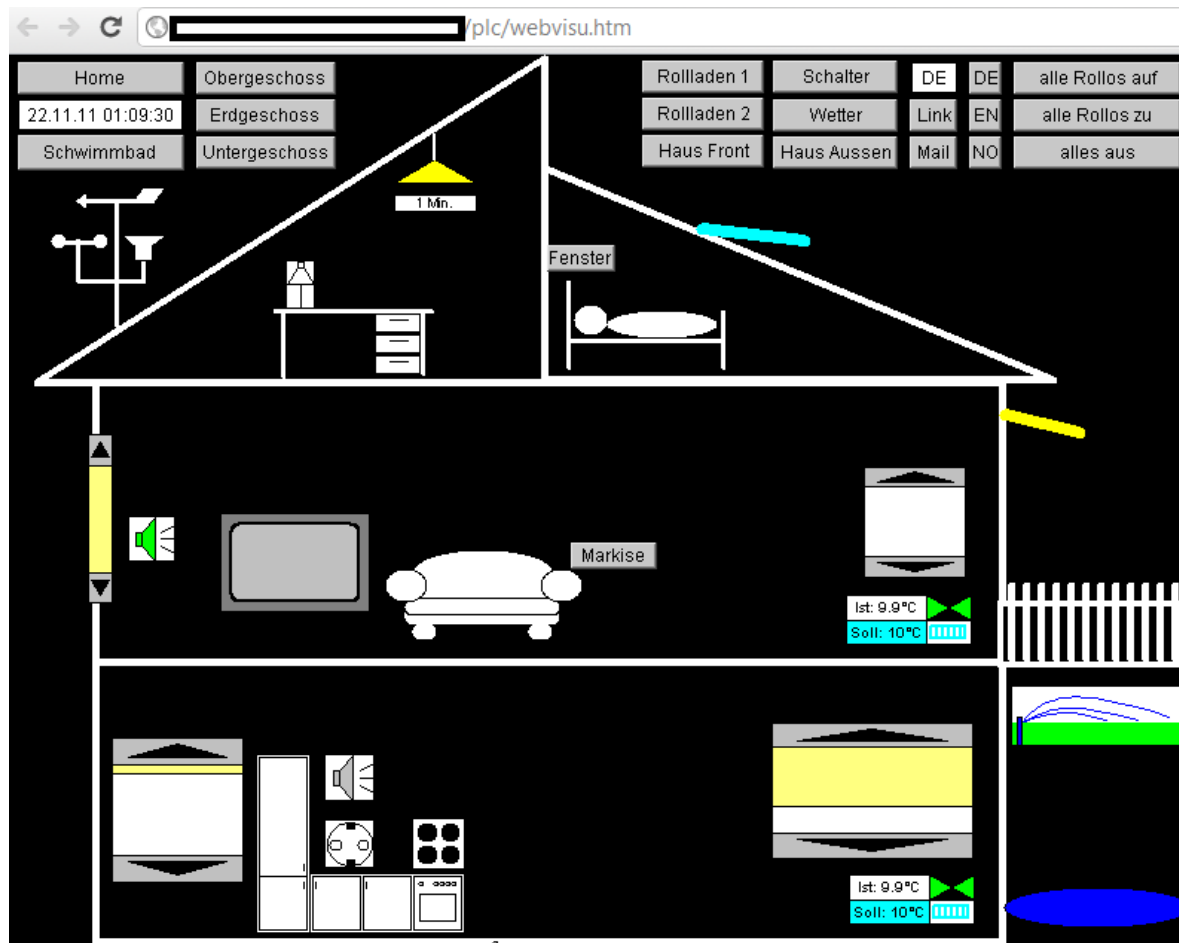
User: Password:

Confirm Password:

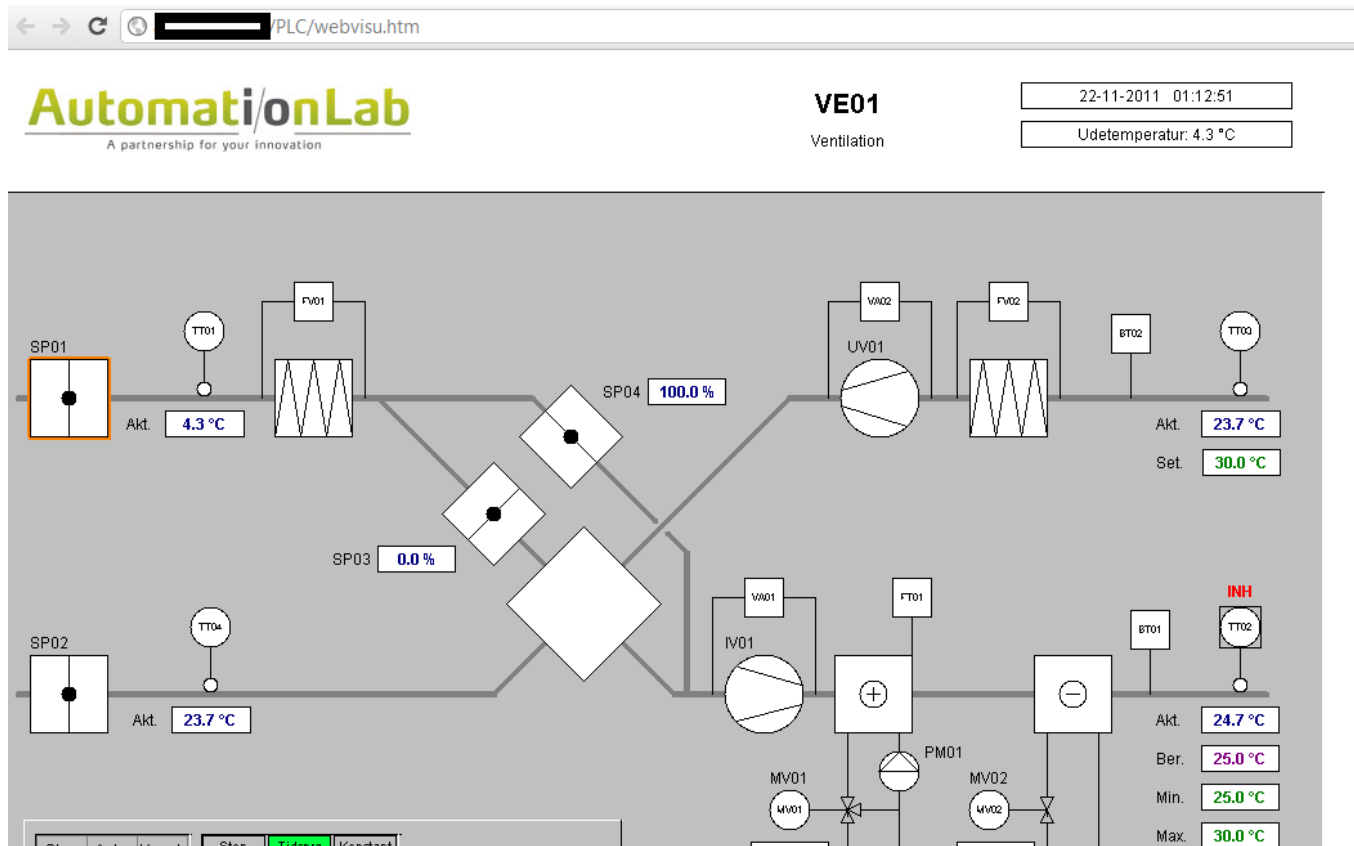
UNDO

SUBMIT

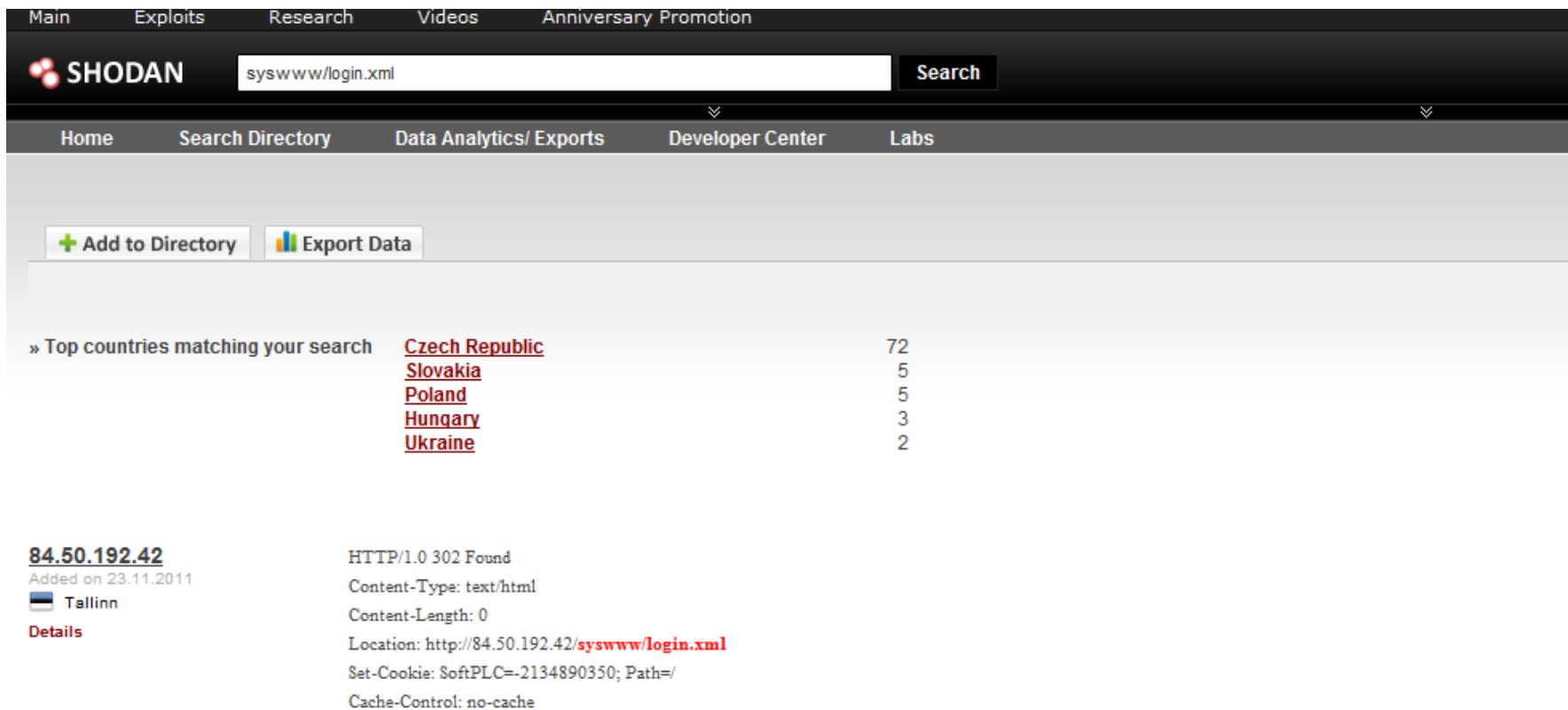
А теперь в реальном мире (WAGO PLC)



А теперь в реальном мире (WAGO PLC)




Поиск в Shodan Tecomat Foxtrot PLC



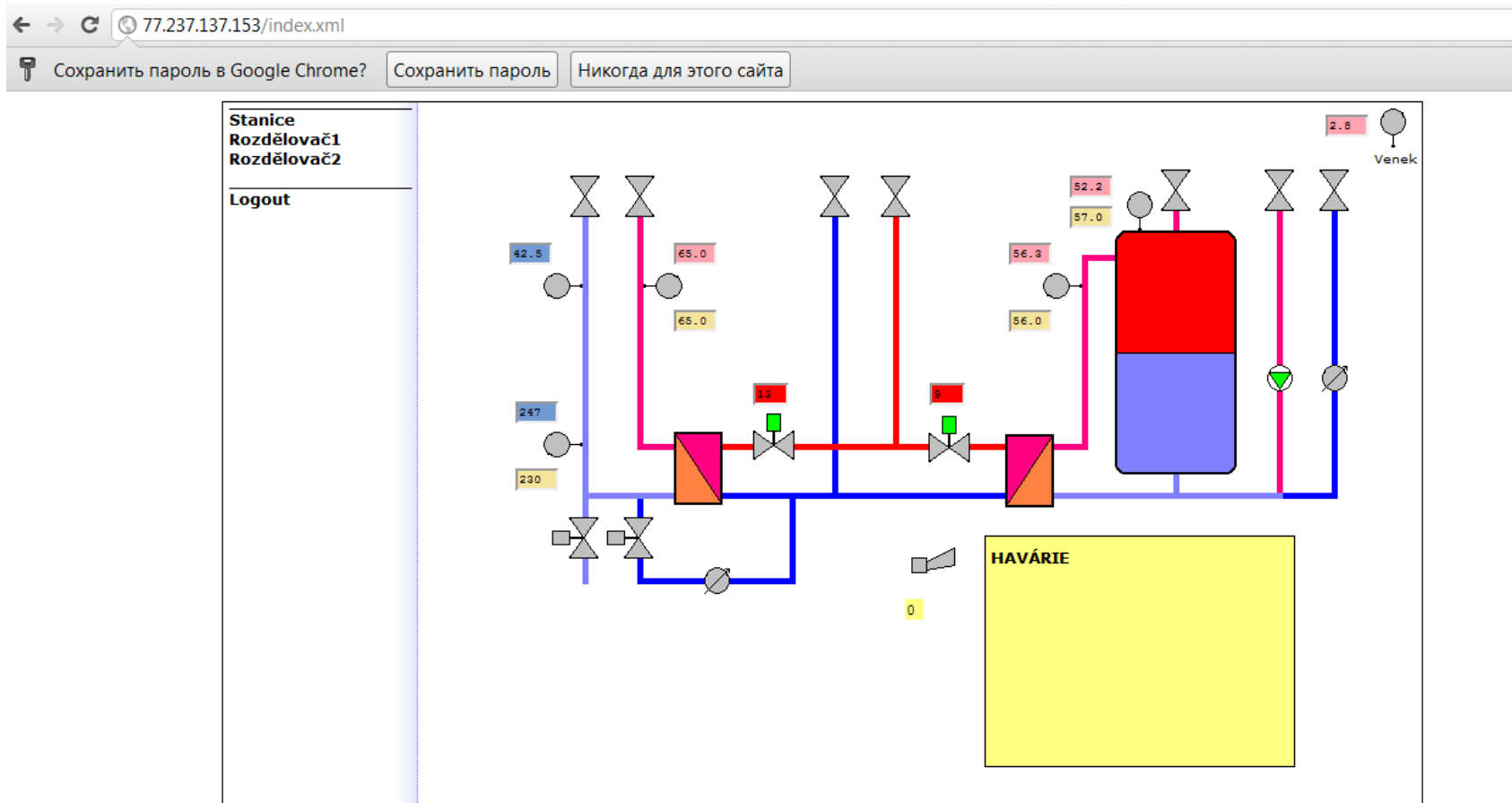
The screenshot displays the Shodan search engine interface. At the top, there is a navigation bar with links: Main, Exploits, Research, Videos, and Anniversary Promotion. Below this is the Shodan logo and a search bar containing the query 'syswww/login.xml'. A 'Search' button is located to the right of the search bar. Below the search bar is a secondary navigation bar with links: Home, Search Directory, Data Analytics/ Exports, Developer Center, and Labs. Below this is a section with two buttons: '+ Add to Directory' and 'Export Data'. The main content area shows search results for 'Top countries matching your search'. The results are as follows:

Country	Count
Czech Republic	72
Slovakia	5
Poland	5
Hungary	3
Ukraine	2

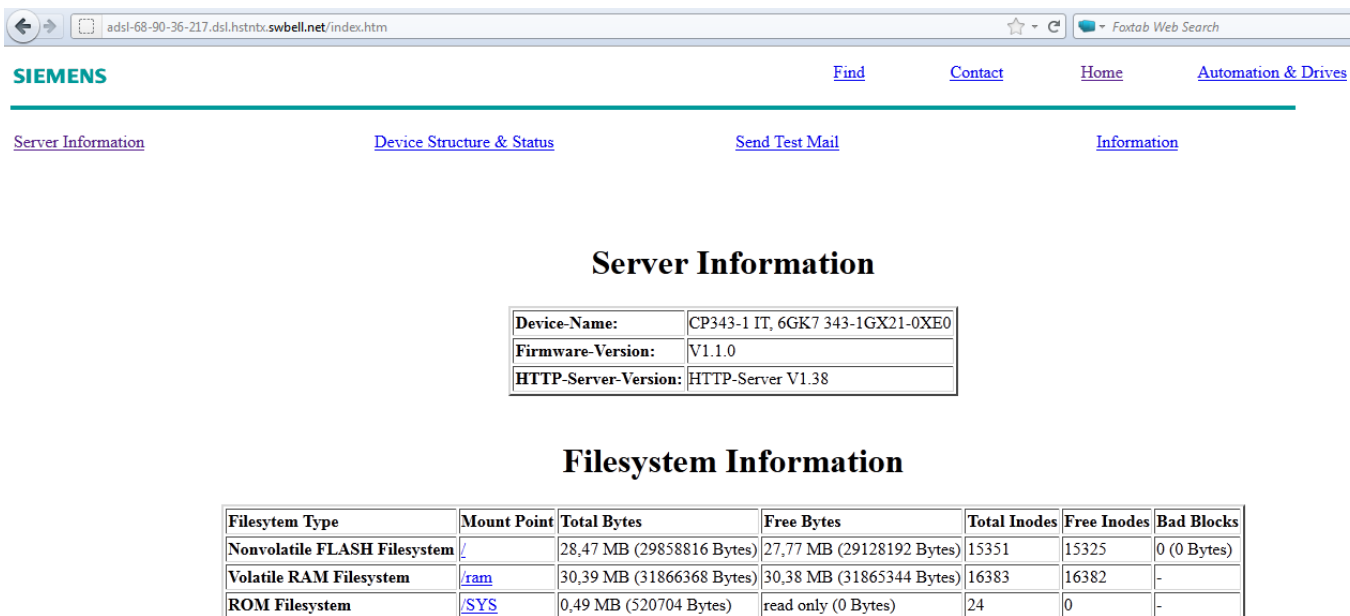
Below the country results, there is a detailed view of a specific search result for IP address 84.50.192.42. The details include:

- 84.50.192.42**
- Added on 23.11.2011
-  Tallinn
- [Details](#)
- HTTP/1.0 302 Found
- Content-Type: text/html
- Content-Length: 0
- Location: <http://84.50.192.42/syswww/login.xml>
- Set-Cookie: SoftPLC=-2134890350; Path=
- Cache-Control: no-cache

А теперь в реальном мире (Tecomat Foxtrot PLC)



А теперь в реально мире (SIMATIC PLC)



The screenshot shows a web browser window displaying the Siemens SIMATIC Manager interface. The address bar shows the URL: `adsl-68-90-36-217.dsl.hstnrx.swbell.net/index.htm`. The page features a navigation bar with links: [Find](#), [Contact](#), [Home](#), and [Automation & Drives](#). Below this, there are links for [Server Information](#), [Device Structure & Status](#), [Send Test Mail](#), and [Information](#).

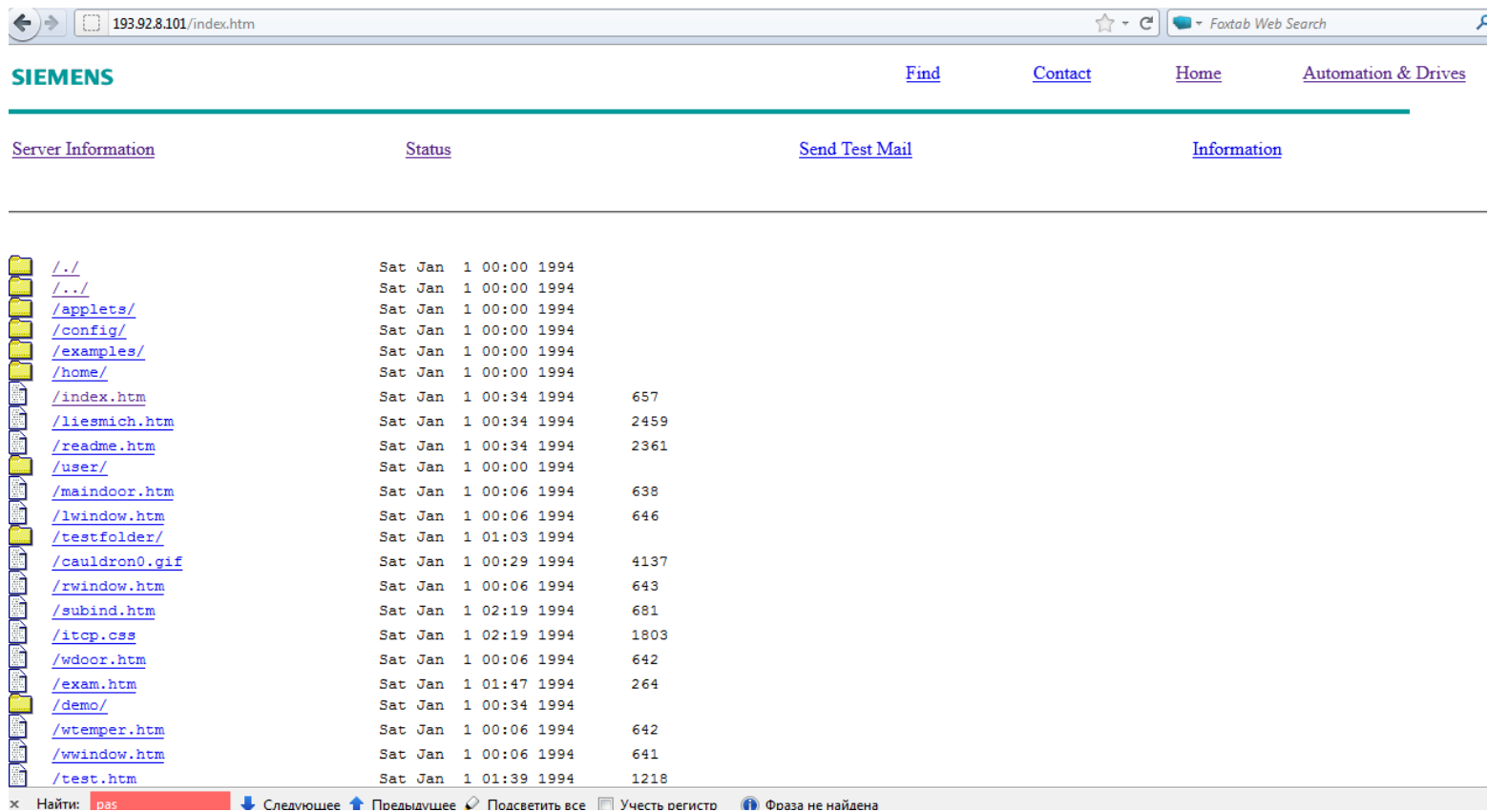
Server Information

Device-Name:	CP343-1 IT, 6GK7 343-1GX21-0XE0
Firmware-Version:	V1.1.0
HTTP-Server-Version:	HTTP-Server V1.38

Filesystem Information

Filesystem Type	Mount Point	Total Bytes	Free Bytes	Total Inodes	Free Inodes	Bad Blocks
Nonvolatile FLASH Filesystem	/	28,47 MB (29858816 Bytes)	27,77 MB (29128192 Bytes)	15351	15325	0 (0 Bytes)
Volatile RAM Filesystem	ram	30,39 MB (31866368 Bytes)	30,38 MB (31865344 Bytes)	16383	16382	-
ROM Filesystem	SYS	0,49 MB (520704 Bytes)	read only (0 Bytes)	24	0	-

А теперь в реально мире (SIMATIC PLC)



193.92.8.101/index.htm

SIEMENS

Find Contact Home Automation & Drives

Server Information Status Send Test Mail Information

./	Sat Jan 1 00:00 1994	
../	Sat Jan 1 00:00 1994	
/applets/	Sat Jan 1 00:00 1994	
/config/	Sat Jan 1 00:00 1994	
/examples/	Sat Jan 1 00:00 1994	
/home/	Sat Jan 1 00:00 1994	
/index.htm	Sat Jan 1 00:34 1994	657
/liesmich.htm	Sat Jan 1 00:34 1994	2459
/readme.htm	Sat Jan 1 00:34 1994	2361
/user/	Sat Jan 1 00:00 1994	
/maindoor.htm	Sat Jan 1 00:06 1994	638
/lwindow.htm	Sat Jan 1 00:06 1994	646
/testfolder/	Sat Jan 1 01:03 1994	
/cauldron0.gif	Sat Jan 1 00:29 1994	4137
/rwindow.htm	Sat Jan 1 00:06 1994	643
/subind.htm	Sat Jan 1 02:19 1994	681
/itcp.css	Sat Jan 1 02:19 1994	1803
/wdoor.htm	Sat Jan 1 00:06 1994	642
/exam.htm	Sat Jan 1 01:47 1994	264
/demo/	Sat Jan 1 00:34 1994	
/wtemper.htm	Sat Jan 1 00:06 1994	642
/wwindow.htm	Sat Jan 1 00:06 1994	641
/test.htm	Sat Jan 1 01:39 1994	1218

Найти: pas Следующее Предыдущее Подсветить все Учить регистр Фраза не найдена

А теперь в реальном мире (WAGO PLC)

Navigation
→ Information
• TCP/IP
• Ethernet
• NTP
• Clock
• Users
• HMI Settings
• Administration
• Downloads
• Port
• Modbus
• I/O-Configuration
• Webvisu

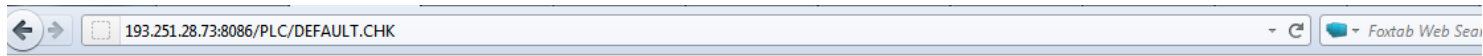
Status Information

Coupler Details	
Order Number	0758-0874-0000-0111
Processor Type	Intel(R) Celeron(R) M processor 600MHz
Fieldbus Type	Profibus-Master
Firmware Revision	01.01.26(05)
License Information	Codesys-Runtime-License
HTML Pages Revision	01.01.26(05)
KBus FW Revision	01.03.11(00)

Network Details Eth0 (X8)	
State	enabled
Mac Address	00:30:DE:FF:B6:4E
IP Address	10.3.252.250
Subnet Mask	255.255.0.0

Network Details Eth1 (X9)	
State	enabled
Mac Address	00:30:DE:FF:B6:4F
IP Address	192.168.196.120
Subnet Mask	255.255.255.0

А теперь в реальном мире



Cesitel
 Conseil en Ingénierie Informatique

Gestion FNAC 91
 PORTAIL SECURISE

Navigation

- Information
- Ethernet
- TCP/IP
- Port**
- SNMP
- SNMP V3
- Watchdog
- Clock
- Security
- PLC
- Features
- IO config
- Disk Info
- WebVisu

Port Settings		
Protocol	Port	Enabled
FTP	21	<input checked="" type="checkbox"/>
SNTP	123	<input type="checkbox"/>
HTTP	80	<input checked="" type="checkbox"/>
SNMP	161, 162	<input checked="" type="checkbox"/>
Ethernet IP	44818 (TCP), 2222 (UDP)	<input type="checkbox"/>
Modbus UDP	502	<input checked="" type="checkbox"/>
Modbus TCP	502	<input checked="" type="checkbox"/>
WAGO Services	6626	<input checked="" type="checkbox"/>
CoDeSys	2455	<input checked="" type="checkbox"/>
BootP	68	<input type="radio"/>
DHCP	68	<input type="radio"/>
use IP from EEPROM	--	<input checked="" type="radio"/>

UNDO

SUBMIT

Обнаружили, а что дальше?

- Атаки на SCADA
- **Атаки на PLC**
- Атаки на инфраструктуру и ОС
- **Атаки на протоколы**

Практические атаки

Реализация зависит от протокола.

Мы рассмотрим Modbus TCP

Порт 502 по умолчанию

Modbus TCP Frame Format		
Name	Length	Function
Transaction Identifier	2 bytes	For synchronization between messages of server & client
Protocol Identifier	2 bytes	Zero for MODBUS/TCP
Length Field	2 bytes	Number of remaining bytes in this frame
Unit Identifier	1 byte	Slave Address (255 if not used)
Function code	1 byte	Function codes as in other variants
Data bytes	n bytes	Data as response or commands

Команды (Function Codes)

			Function Name	Function Code
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Inputs	2
		Internal Bits or Physical Coils	Read Coils	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bit access	Physical Input Registers	Read Input Register	4
		Internal Registers or Physical Output Registers	Read Holding Registers	3
			Write Single Register	6
			Write Multiple Registers	16
			Read/Write Multiple Registers	23
	File Record Access	Mask Write Register	22	
		Read FIFO Queue	24	
		Read File Record	20	
		Write File Record	21	
Diagnostics			Read Exception Status	7
			Diagnostic	8
			Get Com Event Counter	11
			Get Com Event Log	12
			Report Slave ID	17
			Read Device Identification	43
Other			Encapsulated Interface Transport	43

Защита?

- Аутентификация
- Шифрование
- Контрольная сумма

Неа, не слышал :)

Прочие протоколы и сервисы

Port Settings		
Protocol	Port	Enabled
FTP	21	<input checked="" type="checkbox"/>
SNTP	123	<input type="checkbox"/>
HTTP	80	<input checked="" type="checkbox"/>
SNMP	161, 162	<input checked="" type="checkbox"/>
Ethernet IP	44818 (TCP), 2222 (UDP)	<input type="checkbox"/>
Modbus UDP	502	<input checked="" type="checkbox"/>
Modbus TCP	502	<input checked="" type="checkbox"/>
WAGO Services	6626	<input checked="" type="checkbox"/>
CoDeSys	2455	<input checked="" type="checkbox"/>
BootP	68	<input type="radio"/>
DHCP	68	<input type="radio"/>
use IP from EEPROM	--	<input checked="" type="radio"/>

Атаки на WAGO

- **FTP** Заливка модифицированной прошивки через FTP (дефалт пароль)
- **HTTP** Скачка прошивки (без аутентификации)
- **HTTP** выключение и смена настроек (дефалт пароль)
- **SNMP** информация (дефалт стринг)
- **MODBUS** изменение значения регистров (без аутентификации)
- **WAGO Services** Смена настроек и DOS (Без аутентификации)
- **CODESYS** Перезаливка прошивки (без аутентификации)

Практические атаки

- Раскрытие информации (Information Disclose)
- Отказ в обслуживании (Denial of Service)
- Отказ в доступе (Denial of Access)
- Отказ в управлении (Denial of control)
- Отказ в представлении (Denial of view)
- **Подмена представления (Manipulation of View)**

Практические атаки

DEMO

А теперь в реальном мире (OMG!)

```
Nmap done: 1 IP address (1 host up) scanned in 6.57 seconds
c:\Program Files\Nmap>nmap -p 21,80,123,80,161,162,44818,502,6626,2455,68 -PN w
agobuero.dyndns.org
Starting Nmap 5.51 ( http://nmap.org ) at 2011-11-23 03:06 Russian Standard Time
WARNING: Duplicate port number(s) specified. Are you alert enough to be using
Nmap? Have some coffee or Jolt(tm).
Nmap scan report for wagobuero.dyndns.org (84.141.113.183)
Host is up (0.061s latency).
rDNS record for 84.141.113.183: p548d71b7.dip.t-dialin.net
PORT      STATE      SERVICE
21/tcp    open      ftp
68/tcp    closed    dhcpd
80/tcp    open      http
123/tcp   closed    ntp
161/tcp   filtered  snmp
162/tcp   closed    snmptrap
502/tcp   open      asa-appl-proto
2455/tcp  open      unknown
6626/tcp  open      unknown
44818/tcp closed    unknown
Nmap done: 1 IP address (1 host up) scanned in 7.47 seconds
c:\Program Files\Nmap>_
```

Предварительный итог



Итого

- Да, действительно безопасность на уровне лет 90х
- Да, необходимо заниматься безопасностью АСУТП
- Да, есть интересные направления исследований (PLC)
- Да, необходимо больше исследований в этой области
(рассмотрен 1 контроллер из >50)
- Да, мы ищем помощников в наши ряды в том числе и для этих задач



Digital Security

<http://www.dsec.ru>

www.twitter.com/pvolobuev
p.volobuev@dsec.ru