

The CrISTAL Project

Critical Infrastructures Security Testing & Analysis LAB

SCADA (in)Security: Hacking Critical Infrastructures

Raoul Chiesa

Alessio L.R. Pennasilico

raoul@mediaservice.net

mayhem@alba.st

Troopers'08 – April 23rd-24th 2008, Munich (Germany)

\$ whois raoul

Founder @



UN consultant on cybercrime issues at UNICRI agency



OPST, OPSA, Key Contributor for OSSTMM (1.5, 2.0, 2.1, 3.0)

Board of Directors of:

CLUSIT, ISECOM OWASP-Italy, Telecom Security Task Force



CrISTAL, Project Manager for Hacker's Profiling Project



What is SCADA?

Going commercial...

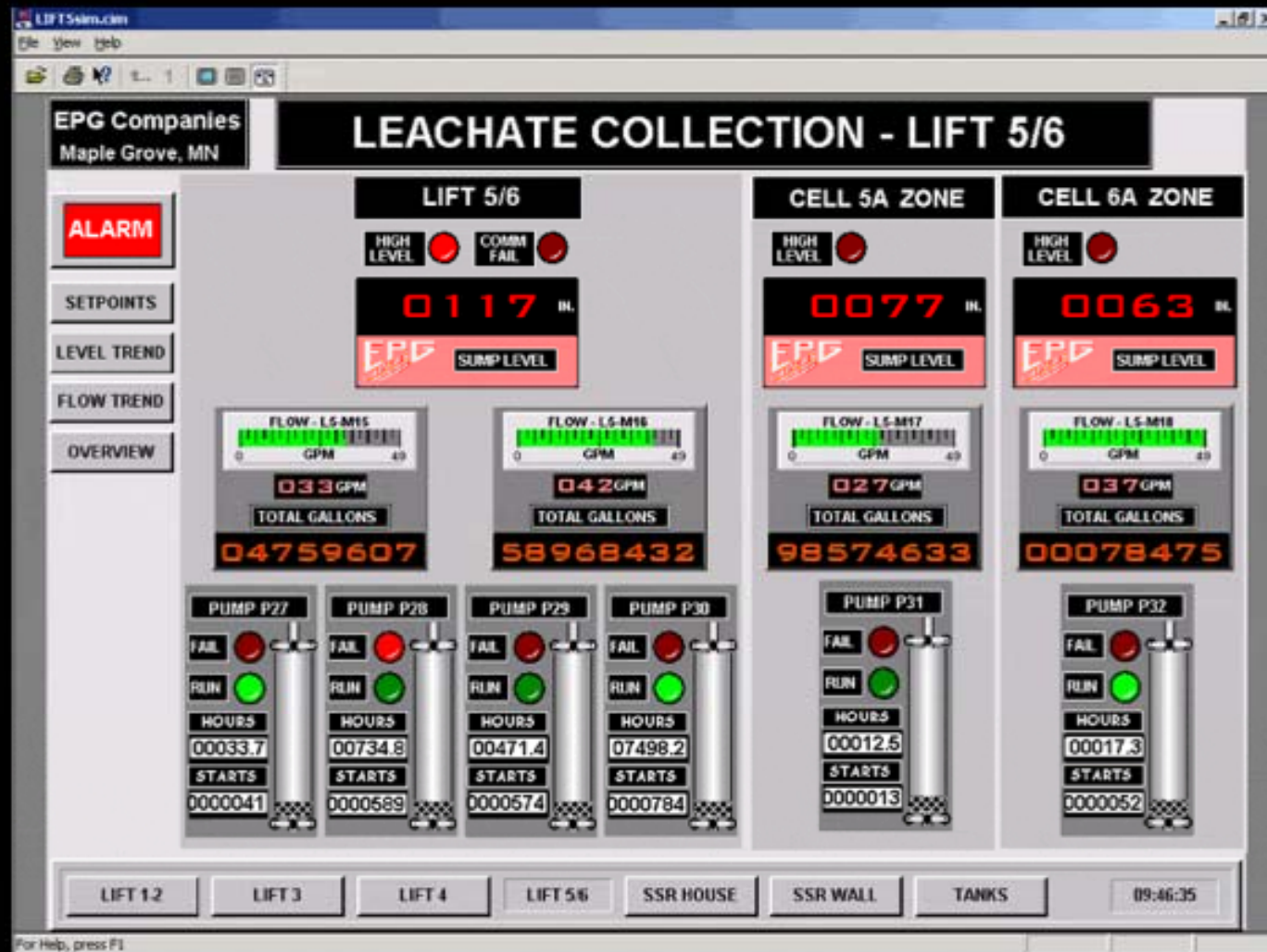
Terroristic video spot about SCADA security

SCADA

“Supervisory Control And Data Acquisition”.

It's the monitoring branch of an automated infrastructure that decides “what to do” on the basis of “what is happening” (event driven).

Managing pumps...



<http://www.nbtinc.com/Software/telemetry-software.html>

Industrial Automation

It is reality since many years

But market is migrating **infrastructures:**

from proprietary, obscure and **isolated** systems
towards standard, documented and **connected** ones

Tree number 3 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address http://sagerkdw/netscada/frame?tree=3

Gulf of Mexico

- Gulf of Mexico
 - E1(Eastern Gulf)
 - E2(Eastern Gulf)
 - W2(Western Gulf)
 - South Marsh Island Area
 - West Cameron Area
 - West Cameron 53 Fld
 - High Island 115B Fld
 - HE 115B Well B1
 - PLC Diagnostics
 - PLC Local Slot #0
 - PLC Local Slot #2
 - PLC Local Slot #1
 - HE 115B ESS Data
 - HE 115B ESS Setp
 - HE 115B Cal Repor
 - HE 115B Cal Repor
 - HE 134A Flow Con
 - HE 134A Flow Con
 - High Island 05A Fld
 - W4(Western Gulf)
 - W5(Western Gulf)

High Island 115 B Well B1 LOCAL

ESD Status TSE Status Steam Tamer Armed

H2S Well Loc 0.0 DC System 25.3 VDC

H2S Panel Loc 0.0 Charging 1.0 Amps

5 Minute Startup Timers Reset Global Alarm Reset

Reset First Out No System 1st Out

Well Control

Well B1

Supply Gas Diagnostics Cal Report HI 134A Sep PLC Diagnostics Spare Spare Spare

Platforms WC 46-A HI 85-A HI 115-B Spare Spare Spare

Well Control

B-1 F/L FA-2 PSL	B-1 F/L FA-3 PSHL	B-1 F/L FA-3 PSHZ
PSH	PSH	PSH
PSL	PSL	PSL

Choke

Status: CLOSED

Restart: 3.0 % open

Target: 10.0 % open

Output: 0.0 % open

FA-2 5 Min Startup Timer	300
FA-2 30 Min Startup Timer	1800
FA-3 5 Min Startup Timer	300
FA-3 30 Min Startup Timer	1800

HI 134A Sep Meter Data

Gas Rate: MCFD

Today's Gas Vol: MCF

Today's Oil Vol: 0.00 BBLs

Today's H2O Vol: BBLs

Yday's Gas Vol: MCF

Yday's Oil Vol: 1.30 BBLs

Yday's H2O Vol: BBLs

KAO 2000 HI 134 Boarding Valve for HI 115B

710

KAH 9100 HI 134 Inst Gas SDV for HI 115B

In-Line H2S PPM: EtHI

Departing PL Deg F: 311

Tubing PAL

8027

Casing PAHs

14305

SCSSV PSL

Sand Probe PSH

In-Line H2S ASH

PAH 808

PAH 0

FA2 732

FA3-1 717

FA3-2 725

Local intranet

<http://www.scadalink.com/netscada%20EI-155%20Web%20image.jpg>

Tree number 3 - Microsoft Internet Explorer

Address: <http://sagerkdw/netscada/frame/tree=3>

Gulf of Mexico

High Island 115 B Well B1 LOCAL

ESD Status: ● TSE Status: ● Steam Tamer Armed: ●

H2S Well Loc: 0.0 DC System: 25.3 VDC
H2S Panel Loc: 0.0 Charging: 1.0 Amps

5 Minute Startup Timers Reset Global Alarm Reset

Reset First Out No System 1st Out

Well Control

Tubing PAL

Well Diagram: 8027, PAH 838, 14305, SCSSV, FA2 732, FA3-1 717, FA3-2 725, In-Line H2S PPM, Departing PL Deg F, KAO 2000 HI 134 Boarding Valve for HI 115B, HI 134A Sep, KAH 9100 HI 134 Inst Gas SDV for HI 115B

Well B1

Supply Gas
Diagnostics
Cal Report
HI 134A Sep
PLC Diagnostics
Spare
Spare
Spare

Platforms

WC 46-A
HI 85-A
HI 115-B
Spare
Spare
Spare

Choke Status: CLOSED
Restart: 3.0 % open
Target: 10.0 % open
Output: 0.0 % open

FA-2 5 Min Startup Timer: 300
FA-2 30 Min Startup Timer: 1800
FA-3 5 Min Startup Timer: 300
FA-3 30 Min Startup Timer: 1800

HI 134A Sep Meter Data
Gas Rate: MCFD
Today's Gas Vol: MCF
Today's Oil Vol: 0.00 BBLs
Today's H2O Vol: BBLs
Yday's Gas Vol: MCF
Yday's Oil Vol: 1.30 BBLs
Yday's H2O Vol: BBLs

Local intranet

<http://www.scadalink.com/netscada%20EI-155%20Web%20image.jpg>

Critical Infrastructures

Many SCADA infrastructures are **responsible** for:

**Power and Nuclear plants, Gas, Oil, Water
distribution, Transports**

but true life taught us that lack of communications
crated more **panic** than huge incidents..

Critical National Infrastructures

Sector	Sample Target Sub-sectors
Energy and Utilities	<i>Electrical power (generation, transmission, nuclear)</i> <i>Natural gas</i> <i>Oil production and transmission systems</i>
Communications and Information Technology	<i>Telecommunications (phone, fax, cable, satellites)</i> <i>Broadcasting systems</i> <i>Software</i> <i>Hardware</i> <i>Networks (Internet)</i>
Finance	<i>Banking</i> <i>Securities</i> <i>Investment</i>
Health Care	<i>Hospitals</i> <i>Health-care facilities</i> <i>Blood-supply facilities</i> <i>Laboratories</i> <i>Pharmaceuticals</i>

Critical National Infrastructures

Sector	Sample Target Sub-sectors
Food	<i>Food safety</i> <i>Agriculture and food industry</i> <i>Food distribution</i>
Water	<i>Drinking water</i> <i>Wastewater management</i>
Transportation	<i>Air</i> <i>Rail</i> <i>Marine</i> <i>Surface</i>
Safety	<i>Chemical, biological, radiological, and nuclear safety</i> <i>Hazardous materials</i> <i>Search and rescue</i> <i>Emergency services (police, fire, ambulance and others)</i> <i>Dams</i>

Critical National Infrastructures

Sector

Sample Target Sub-sectors

Government

Government facilities

Government services (for example meteorological services)

Government information networks

Government assets

Key national symbols (cultural institutions and national sites and monuments)

Manufacturing

Chemical industry

Defence industrial base

Parts of SCADA systems

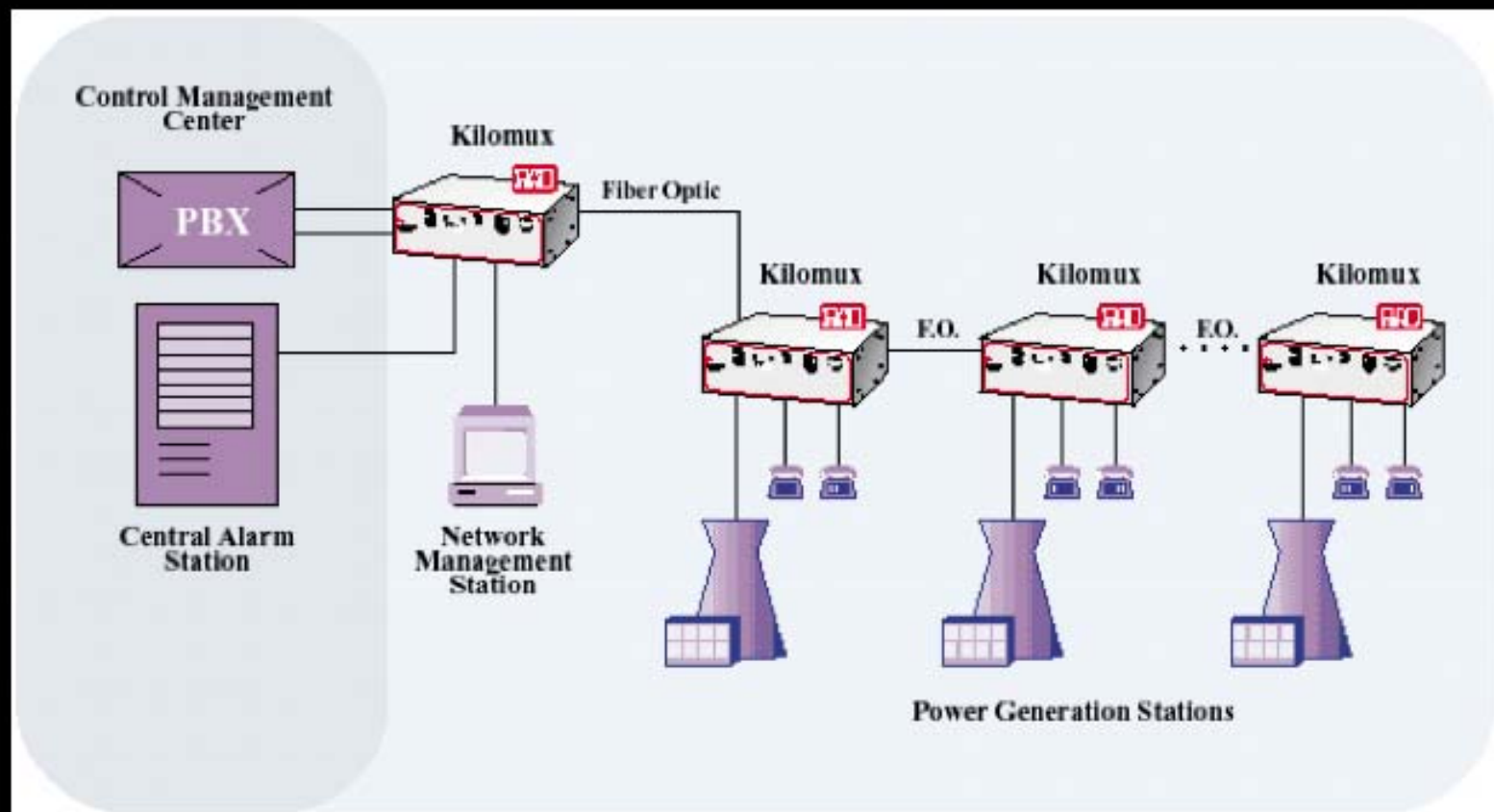
Human Machine Interface (HMI)

Remote Terminal Unit (RTU)

Programmable Logic Controller (**PLC**)

Communication **infrastructure**

A complex infrastructure: Enel



<http://www.radfiber.com/Article/0,6583,27608,00.html>

Enel is the biggest power distributor in Italy

SCADA Issues

<http://cristal.recursiva.org/>

Hackers know about it! :)

A lot of presentations by SCADA people talk about

- * DefCon, BlackHats and similar events
- * on-line password and vulnerability databases
- * legacy IT tools implementing SCADA scanning/testing/assessing features...

It seems that the outside world is really worried about **hackers :)**

Problems caused by ...



Vendors

People



Technology



Incidents

Customers



Incidents

“Shit happens!”

“About 3:28 p.m., Pacific daylight time, on June 10, 1999, a 16-inch-diameter steel pipeline owned by Olympic Pipe Line Company ruptured and released about 237,000 gallons of gasoline into a creek that flowed through Whatcom Falls Park in Bellingham, Washington. About 1.5 hours after the rupture, the gasoline ignited and burned approximately 1.5 miles along the creek. **Two 10-year-old** boys and an **18-year-old** young man **died** as a result of the accident. Eight additional injuries were documented. A single-family residence and the city of Bellingham’s water treatment plant were severely damaged. As of January 2002, Olympic estimated that total property damages were at least \$45 million.”

Tech details

“The Olympic Pipeline SCADA system consisted of Teledyne Brown Engineering²⁰ SCADA Vector software, version 3.6.1., running on **two** Digital Equipment Corporation (DEC) VAX Model 4000-300 computers with VMS operating system Version 7.1. In addition to the **two** main SCADA computers (OLY01 and 02), a similarly configured DEC Alpha 300 computer running Alpha/VMS was used as a host for the **separate** Modisette Associates, Inc., pipeline leak detection system software package.”

SCADA can save lives...

“5. **If** the supervisory control and data acquisition (SCADA) system computers had remained responsive to the commands of the Olympic controllers, the controller operating the accident pipeline **probably** would have been able to initiate actions that would have **prevented** the pressure increase that ruptured the pipeline.”

<http://www.cob.org/press/pipeline/whatcomcreek.htm>

Technical problems

Antivirus

SCADA systems need **real-time** performance.

Antivirus would **degrade** performances enough to make the system useless or dangerous.

Although SCADA systems are **vulnerable** to viruses!

Worms

“In August 2003 Slammer infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly five hours.”



NIST, Guide to SCADA

Patch

Patching systems is a known **problem** in the IT world

Changing anything is a **nightmare** in the SCADA world.

SLA :)

“Our service contractor provides us patches once a year.”

CSO of a power distribution company



PenTesting

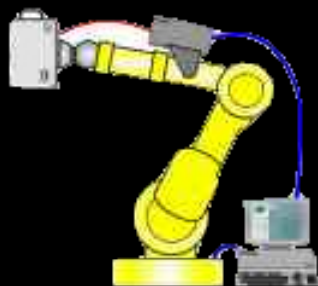
PenTesting old, small, very simple, projected-to-be-isolated devices may lead to service **disruption**.

The market is trying to provide a useful, but mainly “assured” method to assess SCADA networks security.

Although periodical security testing is a **need**, and cannot be simply ignored.

Zombie

“While a ping sweep was being performed on an active SCADA network that controlled 9-foot robotic arms, it was noticed that one arm became active and swung around 180 degrees. The controller for the arm was in standby mode before the ping sweep was initiated.”



NIST, Guide to SCADA

Physical separation

Because of all these reasons, SCADA networks
must be strongly protected from
a perimeter point of view:
VLANs, DMZs, filtering, content filtering, IDS...

Vendors

Vendor Live witness

Insecure by default?

Traffic in **clear** text


No data encryption

No authentication

No accounting

Customers

Customer live witness
(no disclosure agreement)



Mr. Rossi, CIO
in a Power Distribution Company

The last project has been a hard work:

Common mistakes

Merged IT and SCADA network

(no physical or logical separation)

RAS/VPNs provide too much **simple** remote access

Default configurations

No backups at all

No **tested** disaster recovery plan

People...

...were used to ...



<http://www.metroland.org.uk/signal/amer01.jpg>

...but now have to work with...



http://www.thcsystems.com/section_nv/images/effici ent/diredg ingnewsapril2005_ Page_09_ Image_0002.jpg

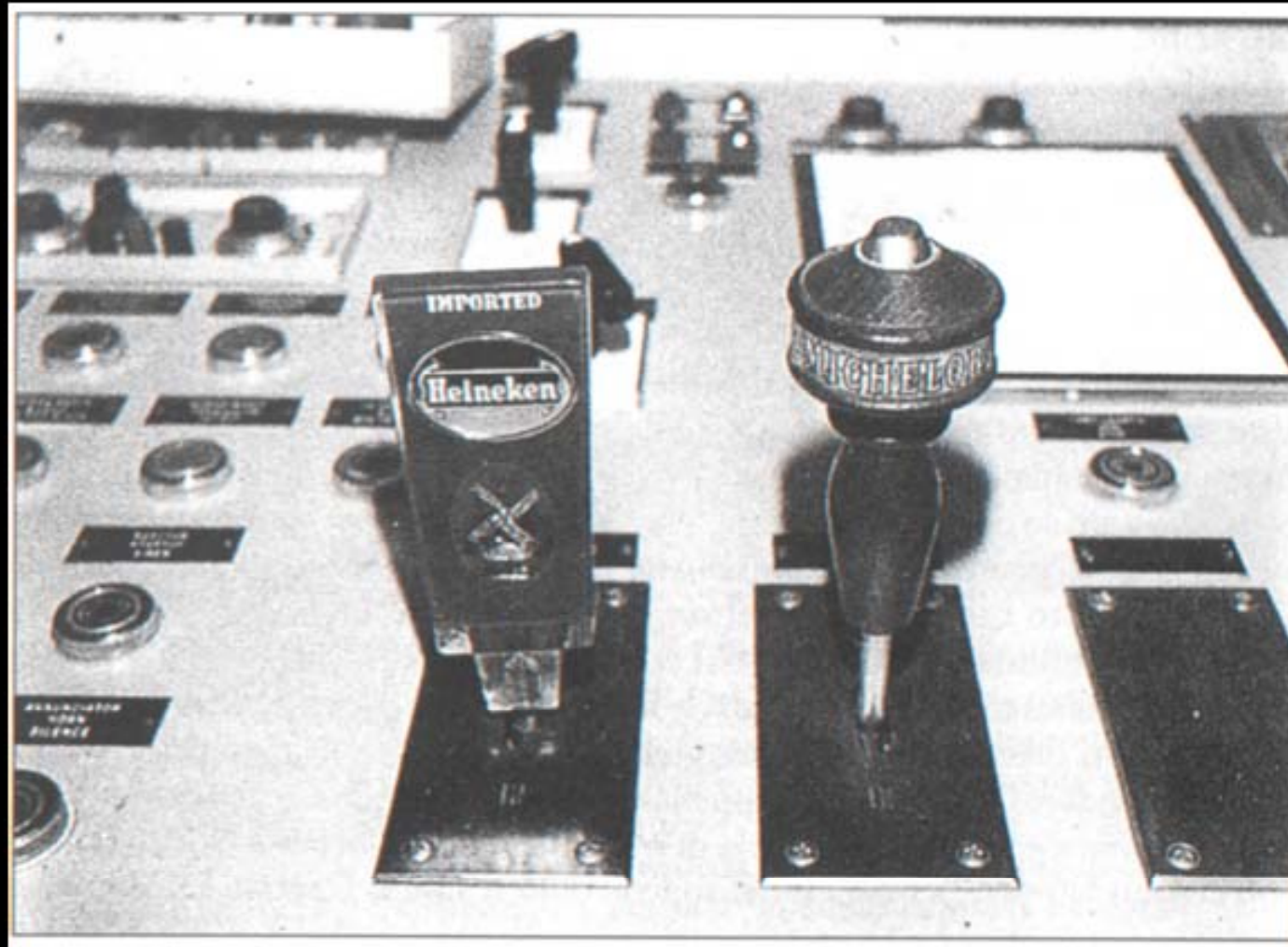
Blockbuster

“The power plant monitoring system was unresponsive. When emergency services arrived, they found the operator watching a DVD on the HMI system”.



CSO of a power distribution company

Ergonomics



D.A. Norman
"The design of
everyday things"

ISBN 8809210271

Disgruntled employee

Vitek Boden, in 2000, was **arrested**, convicted and jailed because he released millions of liters of untreated sewage using his **wireless** laptop. It happened in Maroochy Shire, Queensland, may be as a revenge against his last former employer.

http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

Sabotage

Thomas C. Reed, Ronald Regan's Secretary, described in his book "At the abyss" how the U.S. arranged for the Soviets to receive **intentionally** flawed SCADA software to manage their natural gas pipelines.

"The pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds."

A 3 kiloton **explosion** was the result, in 1982 in Siberia.

<http://www.themoscowtimes.ru/stories/2004/03/18/014.html>

Newspaper call them “Hackers”

“Russian authorities revealed this week that Gazprom, a state-run gas utility, came under the control of **malicious** hackers last year. [...]

The report said hackers used a **trojan** horse program, which stashes lines of harmful computer code in a benign-looking program.”

http://findarticles.com/p/articles/mi_qa3739/is_200403/ai_n9360106

Thieves

Lagos, Nigeria - “At least 40 people died because of fire injuries coming from a pipeline they were trying to open to steal petroleum.”

[...]

“One year ago more than 250 people died in the same circumstances near Lagos.”

<http://news.bbc.co.uk/2/hi/africa/6209845.stm>



Terrorists

“On August 2007 Anti Imperialist Team placed a complex and powerful home-made bomb at the pipeline in Vicenza, North of Italy, the one that take kerosene from the NATO base in Aviano to the Vicenza’s one”.



http://www.ansa.it/opencms/export/site/notizie/rubriche/daassociare/visualizza_new.html_127962764.html



**DON'T
PANIC!**

Security Standards

<http://cristal.recursiva.org/>

The IT 5-10 years ago ...

“The present state of security for SCADA is not commensurate with the threat or potential consequences. The industry has generated a large base of relatively **insecure** systems, with chronic and pervasive vulnerabilities that have been observed during security assessments. **Arbitrary** applications of technology, informal security, and the fluid **vulnerability** environment lead to unacceptable risk. [...] Security for SCADA is typically five to ten years **behind** typical information technology (IT) systems because of its historically **isolated** stovepipe organization.”

<http://www.tswg.gov/tswg/ip/SustainableSecurity.pdf>

Which future?

SCADA security **evolution** is at the same point IT security was 5 years ago.

Differences are to be understood, and a similar approach and security path has to be done

Does **exists** any SCADA Security Standard?

SCADA Security Standards

BS7799-ISO27000 Information sec. management systems – Specification with guidance for use

ISO/IEC 17799:2005 Information Technology – Code of practice for information sec. management

ANSI/ISA S.99.1 Security for Manufacturing and Control Systems

ANSI/ISA SP99 TR2 Integrating Electronic Sec. into Manufacturing and Control Systems Env.

ISO/IEC 15408 Common Criteria

NIST System Protection Profile for Industrial Control Systems (SPP-ICS)

CIDX Chemical Industry Data Exchange - Vulnerability Assessment Methodology (VAM) Guidance

ISPE/GAMP4 – Good Automated Manufacturing Practices

PCSF Process Control System Forum ; **NERC** standards ; **AGA** standards ; **NISCC** Guidelines

ISO27000 vs. ISA-99.00.01

Traditional IT systems

Manufacturing and Control System

Confidentiality

Availability

Integrity

Integrity

Availability

Confidentiality

Different
Priorities



The CrISTAL Project

<http://crystal.recursiva.org/>

CrISTAL

Critical Infrastructures Security Test & Analysis Lab was born in 2007 from some **everyday**-working-on-security and often-**working**-on-scada professionals, to inform the world about SCADA issues.



<http://cristal.recursiva.org/>

Project Objectives

- ◎ **talk** with people, as many people as possible
- ◎ exchanging **experiences** related to SCADA security
- ◎ perform more technical research
- ◎ measure the SCADA's market **real** security level
- ◎ **write** documents / white papers
- ◎ write necessary tools
- ◎ **create** a FDL methodology to pentest SCADA

Competences

Technical	Organizational
Analysis	Measurement
Security Testing	Education
Hardening	Ergonomics

First Steps

- ✓ released a paper for CLUSIT
- ✓ workshops at different events in Italy and Europe
- ✓ workshops for students at universities
- ✓ a first public case history, chosen among our available references and research partner companies

Companies

Airliquide.com (Cryogenics, Industrial and Medical Gas Distribution)

Mil Mil (Healthcare)

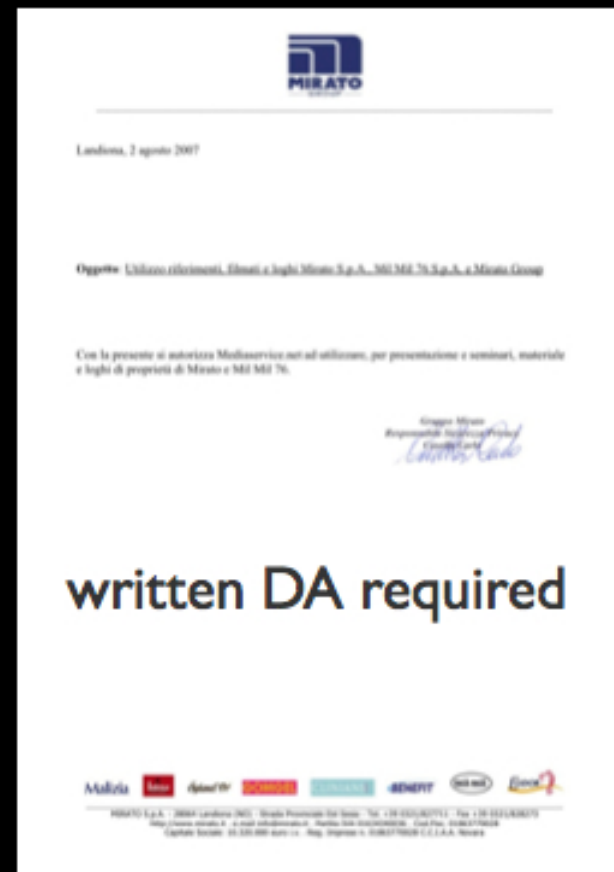
Mirato (Healthcare)

Sovema (Manufacturing)

Multiutility (Power & Gas)

Sant Luis (Manufacturing)

Others (NDA signed)



Sovema case history video

“... is the world **leader** committed with the manufacturing of battery making equipment ...”

*Established **38** years ago*

average 30 MLN US Dollars sales/year

Italy: about 100 employees, 10.000 sq

*Offices in **Europe**, Asia and U.S.A.*

Profibus towards ethernet

Sovema always used SIEMENS Profibus technologies
then some customers **demanded** for Ethernet
and they implemented a **new** solution...

Infrastructure details

A new **internal** test-bed

A PLC with expansion card

An operator panel

Visual alert about PLC operations

The Testbed



```
pt>alert('HITB!')</script> Home Page  
The page at http://192.168.1.160 says:  
HITB!
```



```
# Rockwell Encapsulation  
# Rockwell Encapsulation  
Brian Batke <bbatke@na.rockwell.com>
```

Topology



192.168.1.161

TCP/IP (CIP)



192.168.1.160

Profibus
raw in/out

Tools

brain - always needed!

nmap - let's meet ...

nessus - just to be sure about stupid things :)

wireshark - do you feel the net inside yourself? :)

custom scripts/commands/hacks/test/experience

.160 Open ports

rockwell-encap (44818/tcp)

http (80/tcp)

snmp (161/udp)

rockwell-csp2 (2222/udp)

rockwell-encap (44818/udp)

No access to PLC functions trough HTTP or SNMP /

No parameters can be changed trough HTTP /

No HTTP authentication / Remote monitor via CIP

.161 Open ports

rockwell-encap (44818/tcp)

streetperfect (1330/tcp)

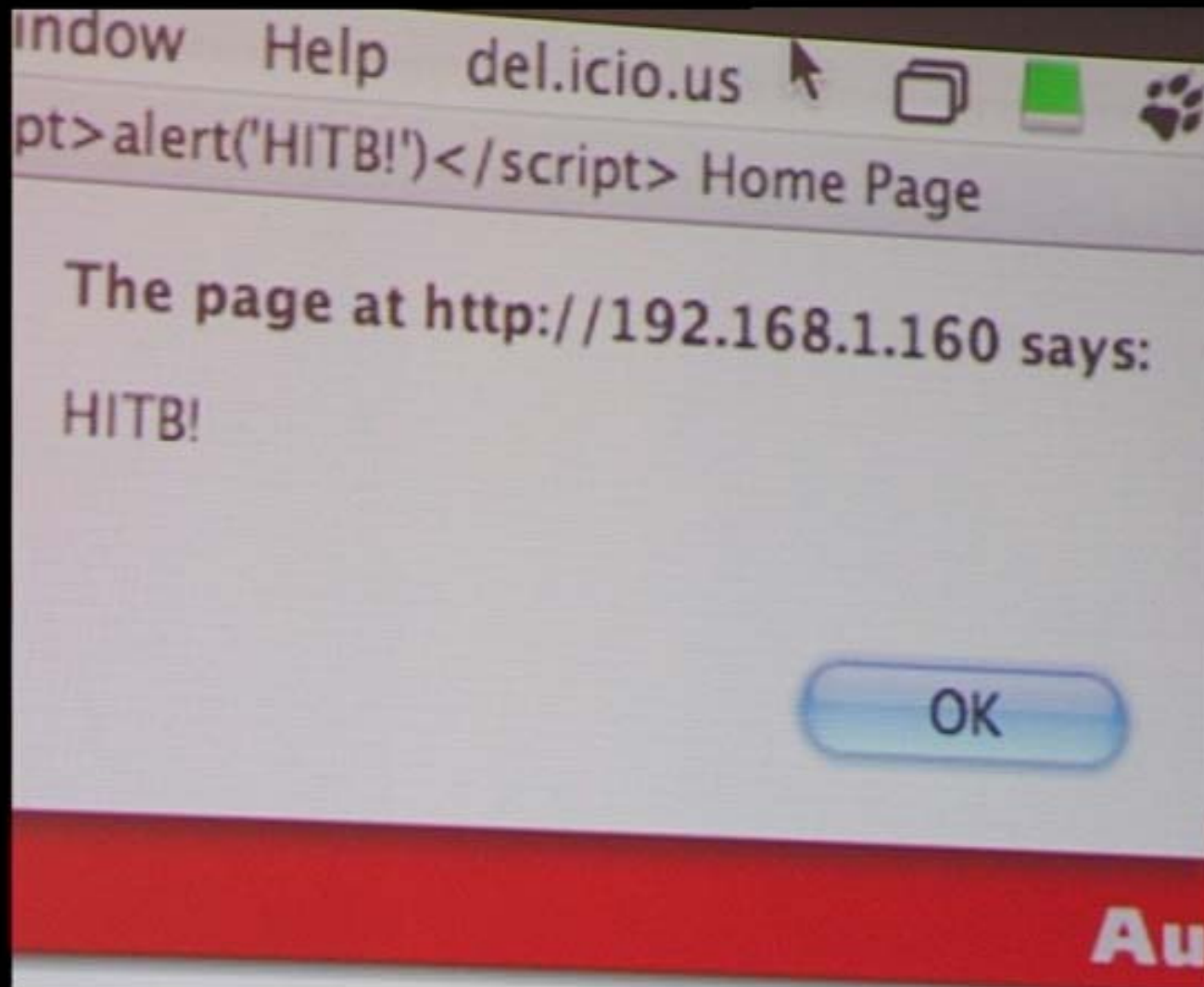
intersan (1331/tcp)

netbios-ns (137/udp)

Managed through the display / Monitored via CIP by a HMI /

Honours the source-route option / File server available

XSS



ClearText Traffic

233 729.720345 192.168.1.161 192.168.1.160 CIP Get Attribute All

- ▼ EtherNet/IP (Industrial Protocol), Session: 0x0A020100, Send Unit Data
 - ▼ Encapsulation Header
 - Command: Send Unit Data (0x0070)
 - Length: 28
 - Session Handle: 0x0a020100
 - Status: Success (0x00000000)
 - Sender Context: 0000000000000000
 - Options: 0x00000000
 - ▼ Command Specific Data
 - Interface Handle: CIP (0x00000000)
 - Timeout: 0
 - ▶ Item Count: 2
 - ▼ Common Industrial Protocol
 - ▼ Service: Get Attribute All (Request)
 - 0... = Request/Response: Request (0x00)
 - .000 0001 = Service: Get Attribute All (0x01)
 - Request Path Size: 2 (words)
 - ▼ Request Path: Identity Object, Instance: 0x01
 - ▼ 8-Bit Logical Class Segment (0x20)
 - Class: Identity Object (0x01)
 - ▼ 8-Bit Logical Instance Segment (0x24)

0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0050	00 00 00 00 02 00 a1 00	04 00 c1 00 3c 00 b1 00<...
0060	08 00 01 00 01 02 20 01	24 01\$.

DoS

- `nmap -sV / -O`
- `ping -f`
- `ping -s > 56200`
- `Traffic > 10 Mb/s`

All conditions that make both devices unresponsive

Results

DoS:

- ping -f, ping -s 56200, nmap -sV/-O

WEBugs2.0:

- xss, no auth, but no parameters to change

Protocol:

- cleartext, easily forgeable
- snmp, but useless on SCADA, only IP

Considerations

Very simple device (both HW&SW), very tailored:

- ▶ very **simple** to DoS
- ▶ some “silliness”, but nothing terrible
- ▶ no huge bugs
- ▶ emerged the need for **specific** tools ...

Todo

- ◎ **involve** more people
- ◎ release a periodic bulletin about market status
- ◎ write more tech&org articles/white papers
- ◎ create a **larger** pool of public case histories
- ◎ write some tools (i.e. CIP injector)
- ◎ release a PenTesting **methodology** under FDL

Conclusions

Best Practices /I

- ✓ **Split** into VLANs/DMZs
- ✓ Firewall / Content Filtering / IDS
- ✓ Implement device redundancy
- ✓ Take care about physical security
- ✓ Update and **verify** documentation
- ✓ ... and apply policies

Best Practices /II

- ✓ **Disable** unused services
- ✓ Adopt AAA solutions
- ✓ **Use** encryption (i.e.VPN)
- ✓ Implement Quality of Service
- ✓ Use test-bed for simulations/security tests
- ✓ **periodically** run security tests (with a declared and common methodology)

Bibliography /I

<http://csrc.nist.gov/publications/drafts/800-82/Draft-SP800-82.pdf>

<https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf>

<http://cansecwest.com/slides06/csw06-byres.pdf>

http://www.mayhem.hk/docs/scada_univr.pdf

<http://darkwing.uoregon.edu/~joe/scada/>

<http://www.physorg.com/news94025004.html>

<http://ethernet.industrial-networking.com/articles/articledisplay.asp?id=206>

<http://www.apogeeonline.com/libri/88-503-1042-0/ebook/libro>

http://www.sans.org/reading_room/whitepapers/warfare/1644.php

http://www.digitalbond.com/SCADA_Blog/SCADA_blog.htm



Bibliography /II

<http://www.securityfocus.com/news/11402>

<http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf>

<http://www.visionautomation.it/modules/AMS/article.php?storyid=32>

<http://www.cob.org/press/pipeline/whatcomcreek.htm>

<http://www.securityfocus.com/news/6767>

http://www.iscom.istsupcti.it/index.php?option=com_content&task=view&id=16&Itemid=1

<http://books.google.it/books?id=xL3Ye3ZORbgC>



The CrISTAL Project

Critical Infrastructures Security Testing & Analysis LAB

Thank You!

Raoul Chiesa

raoul@mediaservice.net

Alessio L.R. Pennasilico

mayhem@alba.st