The CrISTAL Project

Critical Infrastructures Security Testing & Analysis LAB

SCADA (in)Security:
Hacking Critical Infrastructures

Raoul Chiesa
raoul@mediaservice.net

Alessio L.R. Pennasilico
mayhem@alba.st

http://cristal.recursiva.org/

HITB SecConf2007 - Malaysia
3rd - 6th September 2007 - Kuala Lumpur
Deep Knowledge Security Conference

$ whois raoul

Founder @ mediaservice.net
CORPORATE SECURITY & IMAGE

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

$ whois mayhem

Security Evangelist @ alba

Alba S.T. srl

Member / Board of Directors:

AIP, AIPSI, CLUSIT, ILS, IT-ISAC, LUGVR, OPSI, Metro Olografix, No1984.org, OpenBeer, Sikurezza.org, Spippolatori, VoIPSA.

CrISTAL, HPP, Recursiva.org

What is SCADA?

http://cristal.recursiva.org/

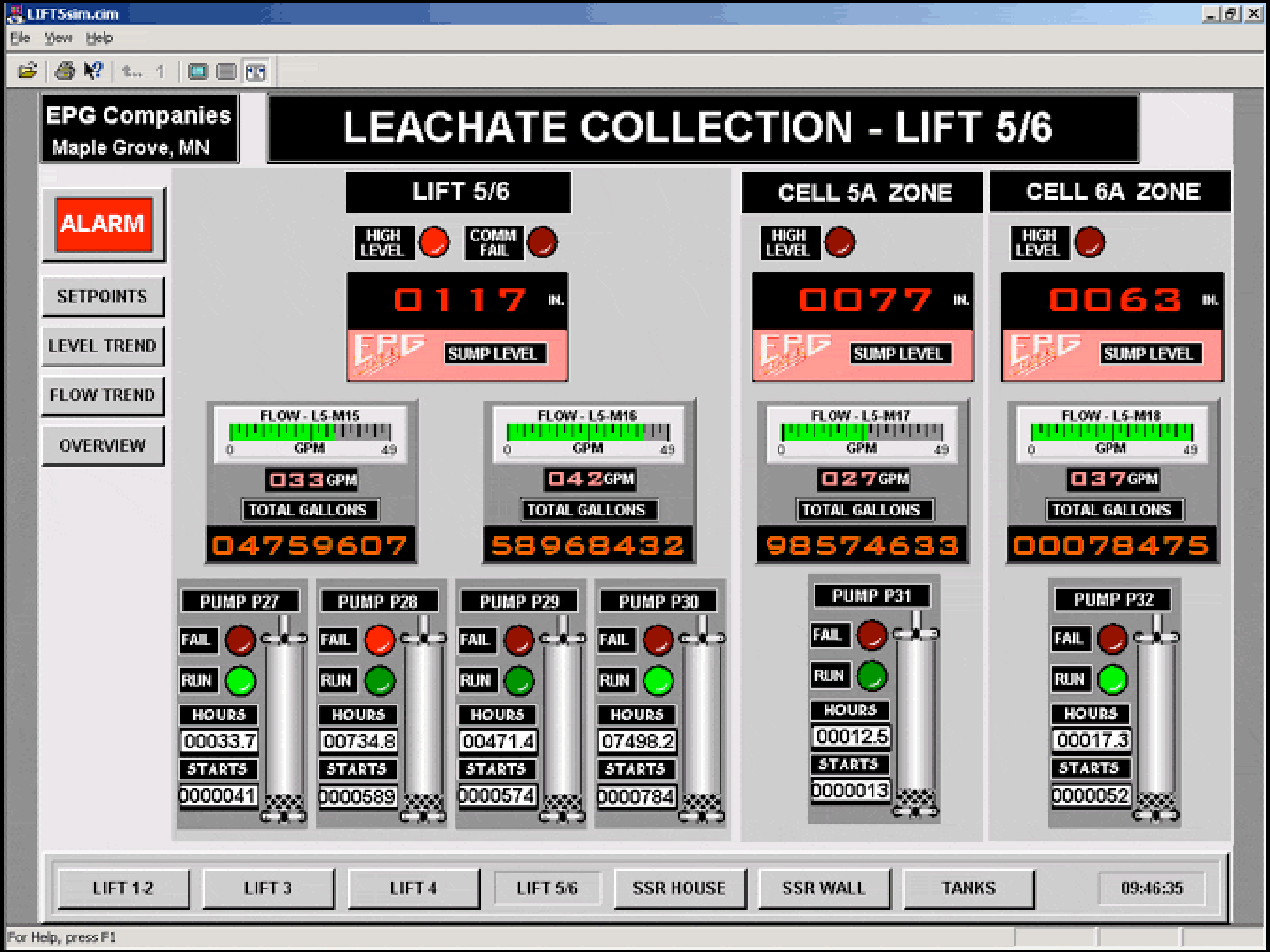
SCADA

“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...



EPG Companies
Maple Grove, MN

LEACHATE COLLECTION - LIFT 5/6

LIFT 5/6	CELL 5A ZONE	CELL 6A ZONE
HIGH LEVEL ● COMM FAIL ●	HIGH LEVEL ●	HIGH LEVEL ●
0117 IN. SUMP LEVEL	0077 IN. SUMP LEVEL	0063 IN. SUMP LEVEL

	FLOW - L5-M15	FLOW - L5-M16	FLOW - L5-M17	FLOW - L5-M18
GPM	033 GPM	042 GPM	027 GPM	037 GPM
TOTAL GALLONS	04759607	58968432	98574633	00078475

	PUMP P27	PUMP P28	PUMP P29	PUMP P30	PUMP P31	PUMP P32
FAIL	●	●	●	●	●	●
RUN	●	●	●	●	●	●
HOURS	00033.7	00734.8	00471.4	07498.2	00012.5	00017.3
STARTS	0000041	0000589	0000574	0000784	0000013	0000052

09:46:35

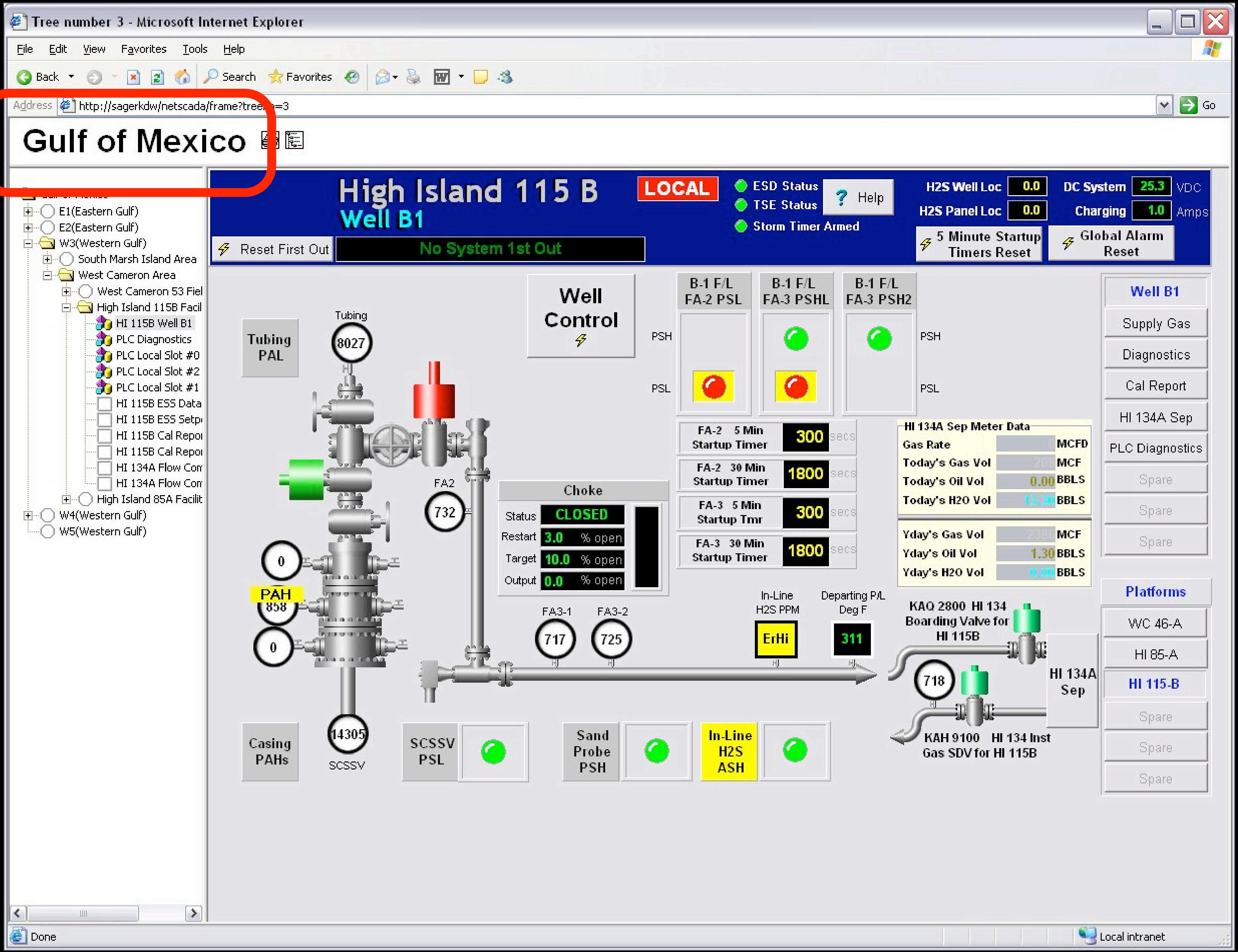
http://www.nbtinc.com/Software/telemetry-software.html

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

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

Gulf of Mexico

High Island 115 B
Well B1

LOCAL

No System 1st Out

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

Choke

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

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

HI 134A Sep Meter Data

Gas Rate	[illegible]	MCFD
Today's Gas Vol	200	MCF
Today's Oil Vol	0.00	BBLS
Today's H20 Vol	13.30	BBLS
Yday's Gas Vol	2358	MCF
Yday's Oil Vol	1.30	BBLS
Yday's H20 Vol	0.00	BBLS

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..

Parts of SCADA systems

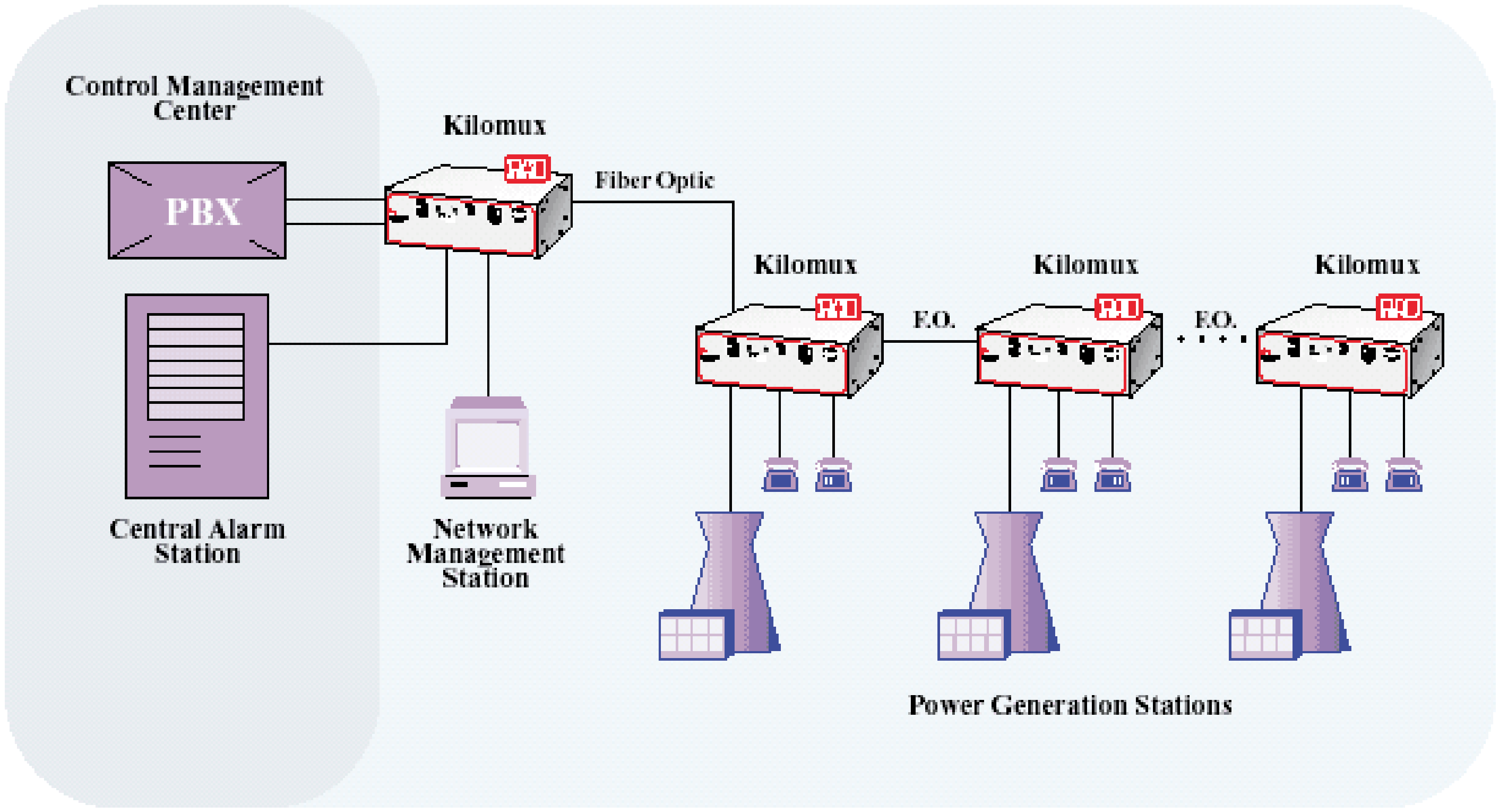
Human Machine Interface (HMI)

Remote Terminal Unit (RTU)

Programmable Logic Controller (PLC)

Communication infrastructure

A complex infrastructure: Enel


Control Management Center
Kilomux
PBX
Fiber Optic
Kilomux
Kilomux
Kilomux
F.O.
F.O.
Central Alarm Station
Network Management Station
Power Generation Stations

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

Enel is the biggest power distributor in Italy

SCADA Issues

going commercial...

Terroristic video spot about SCADA security

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…

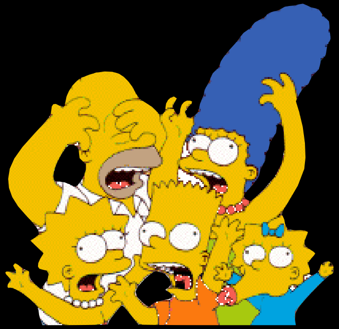
It seems that the outside world is really worried about us :)

Problems caused by ...

Vendors

People

Technology



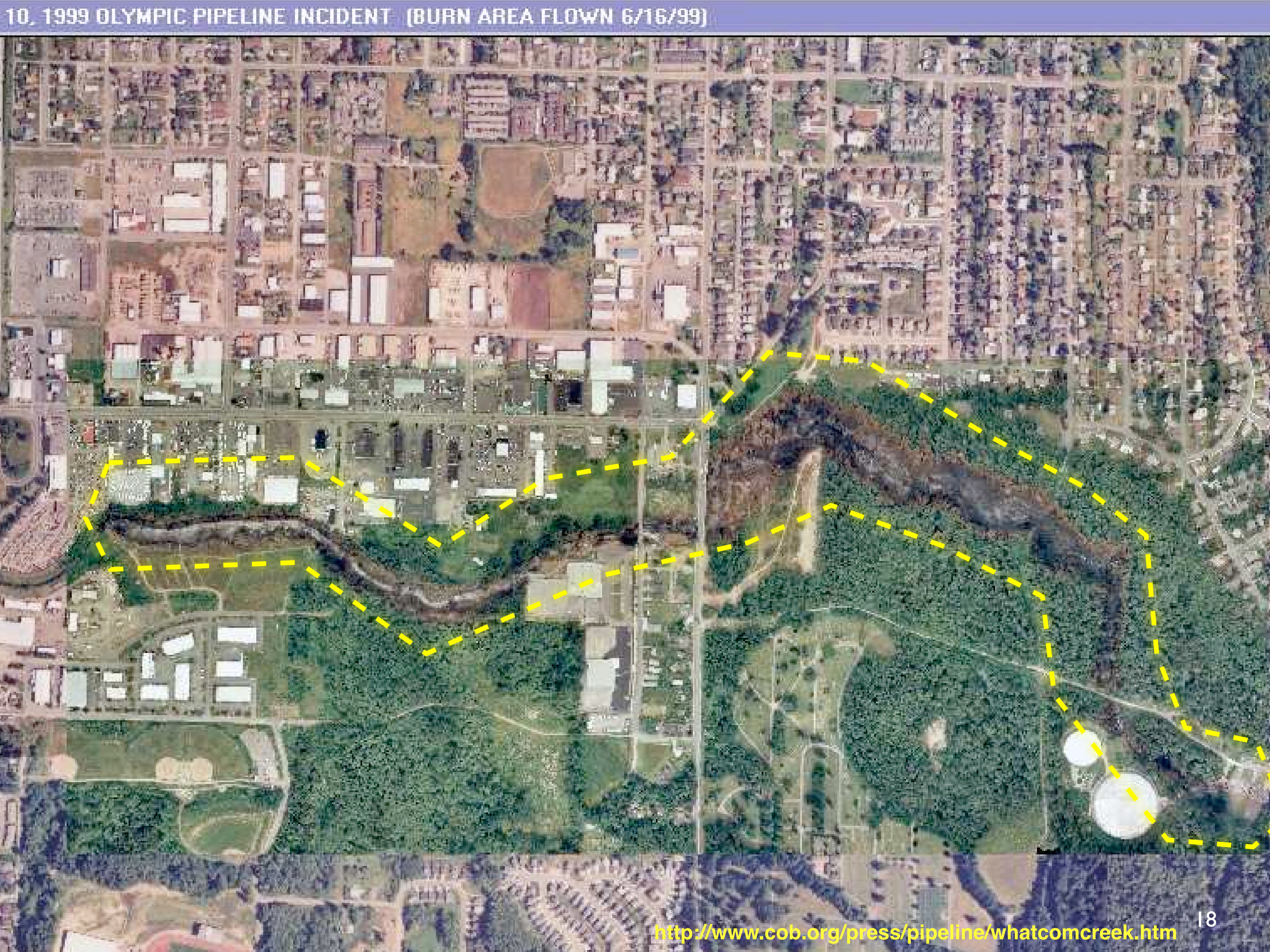
Incidents

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 Bellinghamís water treatment plant were severely damaged. As of January 2002, Olympic estimated that **total property damages were at least $45 million**.”



10, 1999 OLYMPIC PIPELINE INCIDENT (BURN AREA FLOWN 6/16/99)

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

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

http://cristal.recursiva.org/

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

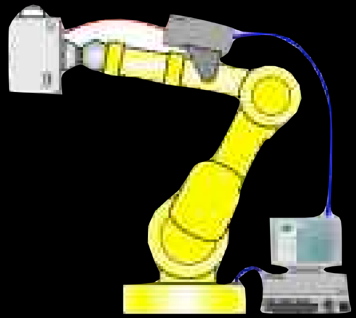
PenTesting old, small, very simple, projected-to-be-isolated devices **may lead to service disruption**.

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

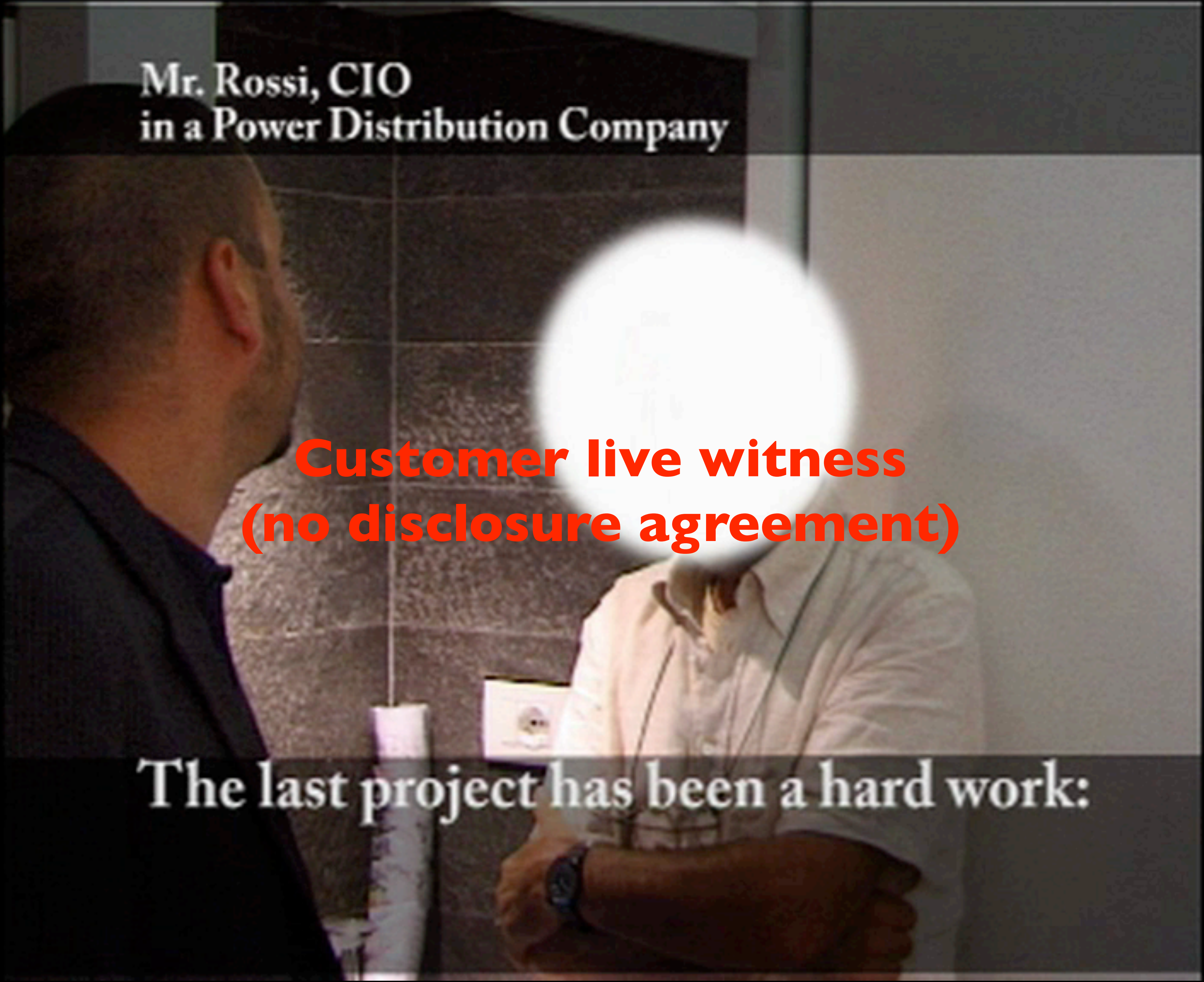
No authentication

No accounting

Modbus Hacking video

Customers

http://cristal.recursiva.org/



Mr. Rossi, CIO
in a Power Distribution Company

Customer live witness
(no disclosure agreement)

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...

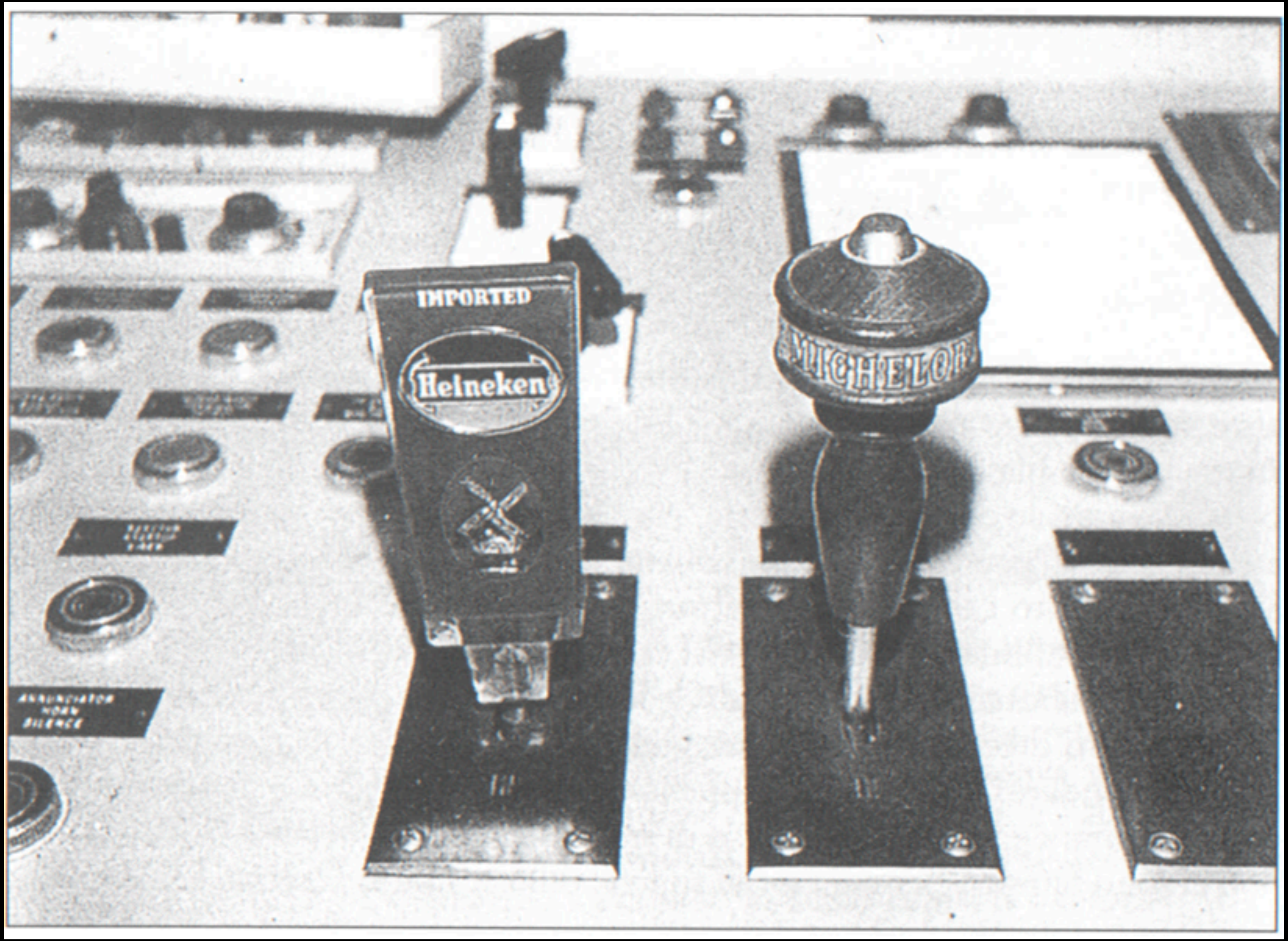
http://www.ihcsystems.com/section_n/images/efficientdredgingnewsapril2005_Page_09_Image_0002.jpg

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 values 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

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

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

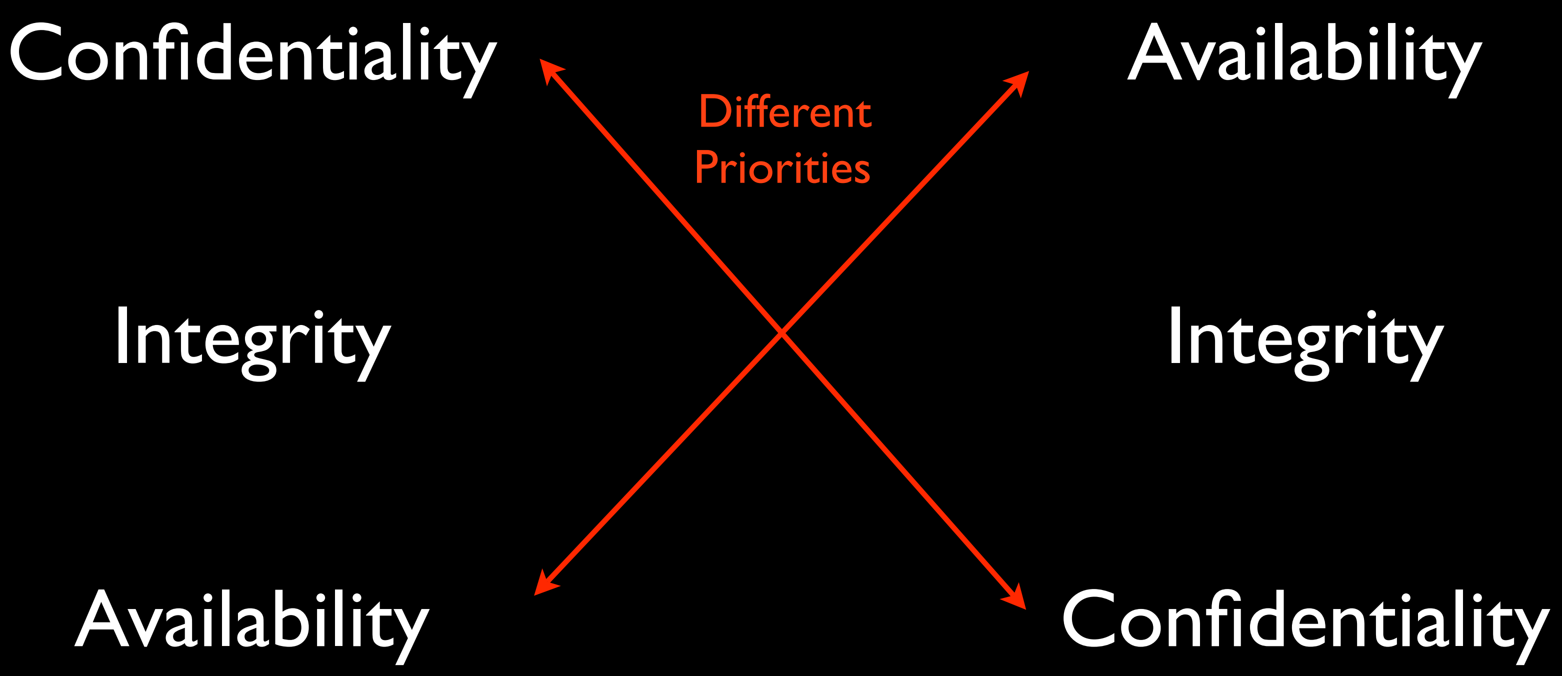
ISPE/GAMP4 – Good Automated Manufacturing Practices

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

IS027000 vs. ISA-99.00.01

Traditional IT systems

Manufactoring and Control System



Confidentiality

Integrity

Availability

Different Priorities

Availability

Integrity

Confidentiality

The CrISTAL Project

http://cristal.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 and 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

Team - Key People

Elisa Bortolani

Raoul Chiesa

Alessio L.R. Pennasilico

Enzo M. Tieghi

Competences

Technical	Organizational
Analysis	Measurement
Security Testing	Education
Hardening	Ergonomics

Team - Organizations

AIPSI, ISSA Italian Chapter

AIP, Italian Association of IT Professionals

University of Verona (I.T. Science Dpt, Robotic Dpt, Psycho Dpt)

Alba S.T. - implements and hardens infrastructures

@Mediaservice.net - security testing

Servitecno - designs and implements SCADA products

Trilance - GAS & Elettrical Company Software House

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)

Melegatti (Food)

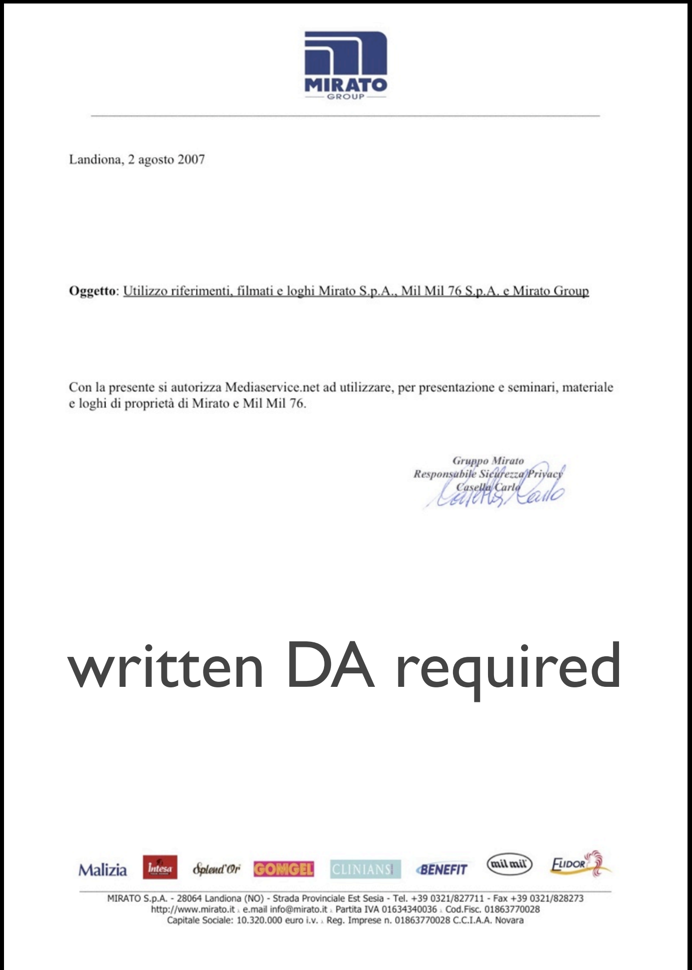
Revello, Tecres (Medical)

Sovema (Manufacturing)

Multiutility (Power & Gas)

Sant Luis (Manufactoring)

Others (NDA signed)



Landiona, 2 agosto 2007

Oggetto: Utilizzo riferimenti, filmati e loghi Mirato S.p.A., Mil Mil 76 S.p.A. e Mirato Group

Con la presente si autorizza Mediaservice.net ad utilizzare, per presentazione e seminari, materiale e loghi di proprietà di Mirato e Mil Mil 76.

Gruppo Mirato
Responsabile Sicurezza Privacy
Casella Carlo
Casella Carlo

MIRATO S.p.A. - 28064 Landiona (NO) - Strada Provinciale Est Sesia - Tel. +39 0321/827711 - Fax +39 0321/828273
http://www.mirato.it . e.mail info@mirato.it . Partita IVA 01634340036 . Cod.Fisc. 01863770028
Capitale Sociale: 10.320.000 euro i.v. . Reg. Imprese n. 01863770028 C.C.I.A.A. Novara

written DA required

Sovema case history video

Case History:

SoVeMa®
Battery Manufacturing Equipment

"… 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

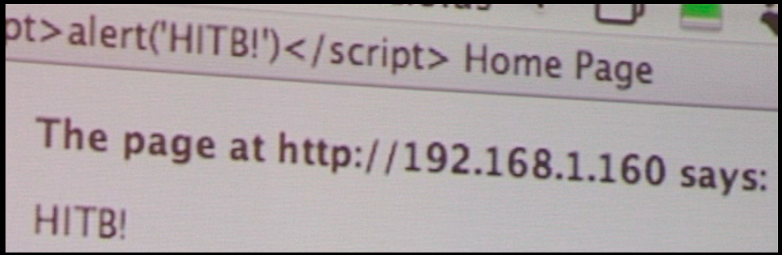
A new internal test-bed

A PLC with expansion card

An operator panel

Visual alert about PLC operations

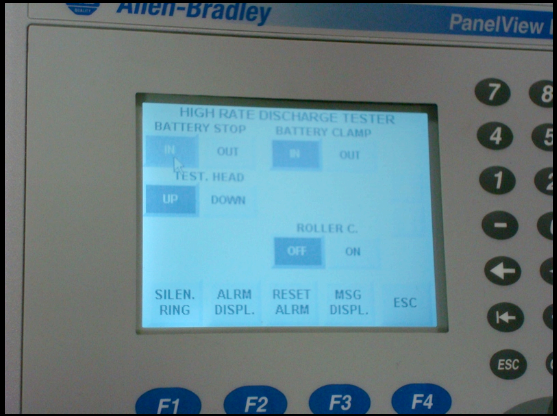
The TestBed

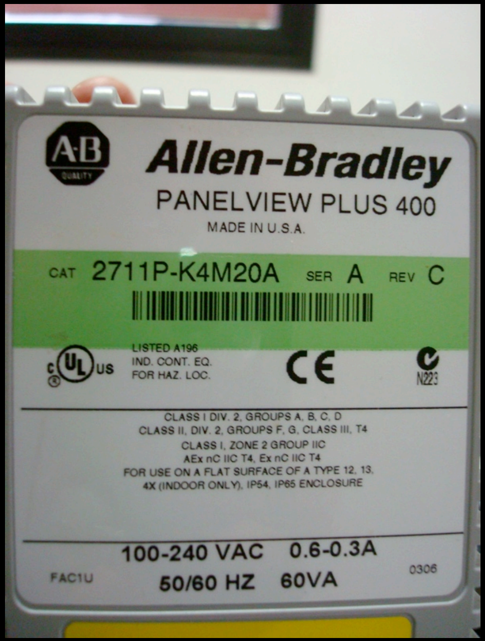


pt>alert('HITB!')</script> Home Page

The page at http://192.168.1.160 says:

HITB!





Allen-Bradley
PANELVIEW PLUS 400
MADE IN U.S.A.

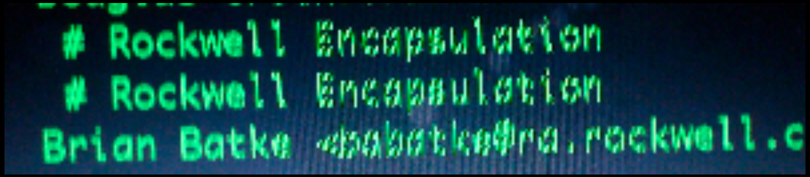
CAT 2711P-K4M20A SER A REV C

LISTED A196
IND. CONT. EQ.
FOR HAZ. LOC.

N223

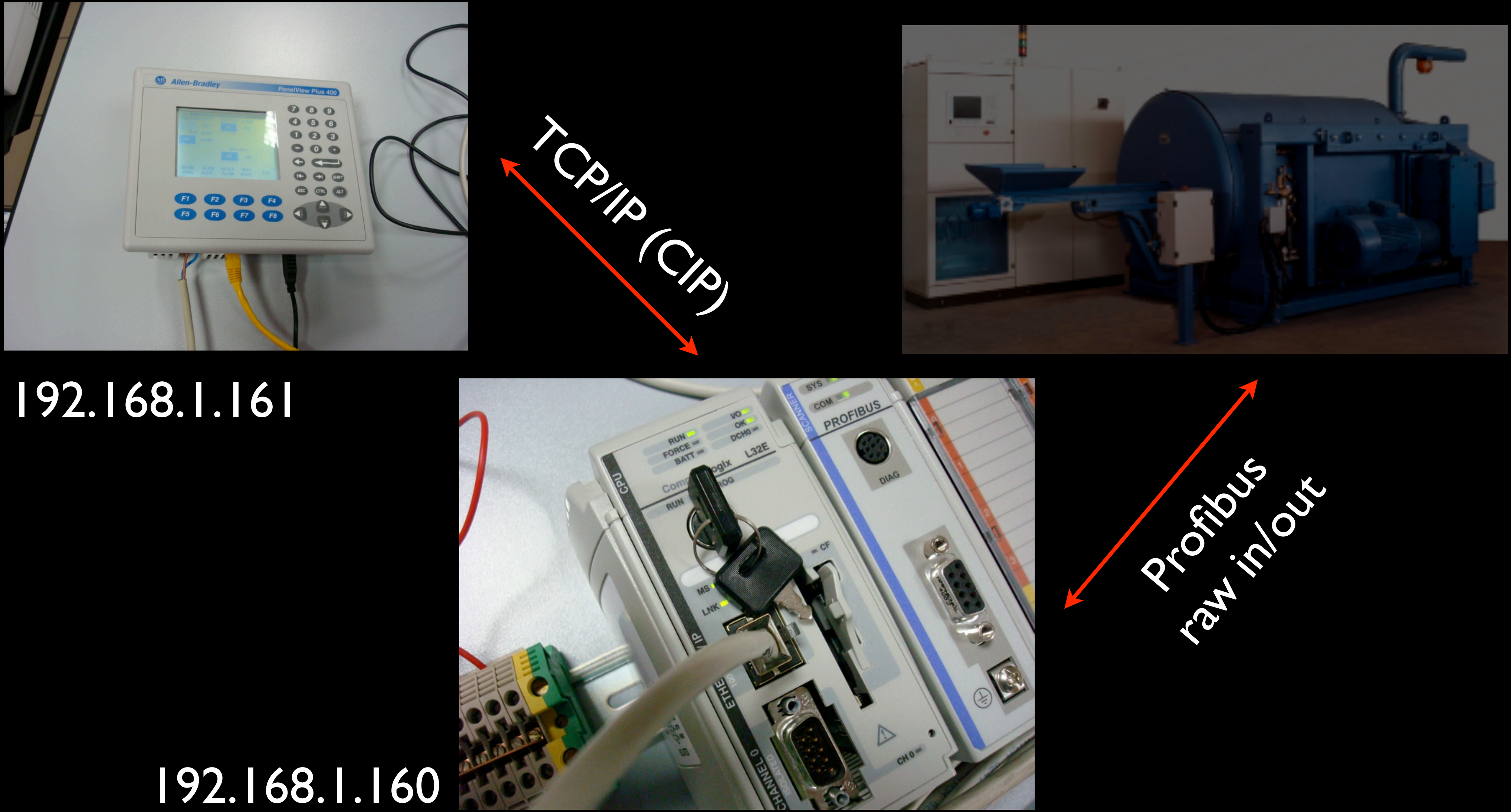
CLASS I DIV. 2, GROUPS A, B, C, D
CLASS II, DIV. 2, GROUPS F, G, CLASS III, T4
CLASS I, ZONE 2 GROUP IIC
AEx nC IIC T4, Ex nC IIC T4
FOR USE ON A FLAT SURFACE OF A TYPE 12, 13,
4X (INDOOR ONLY), IP54, IP65 ENCLOSURE

100-240 VAC 0.6-0.3A
FAC1U 50/60 HZ 60VA 0306



```
  # Rockwell Encapsulation
  # Rockwell Encapsulation
Brian Batke <babatke@ra.rockwell.c
```

Topology



TCP/IP (CIP)

192.168.1.161

Profibus raw in/out

192.168.1.160

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)

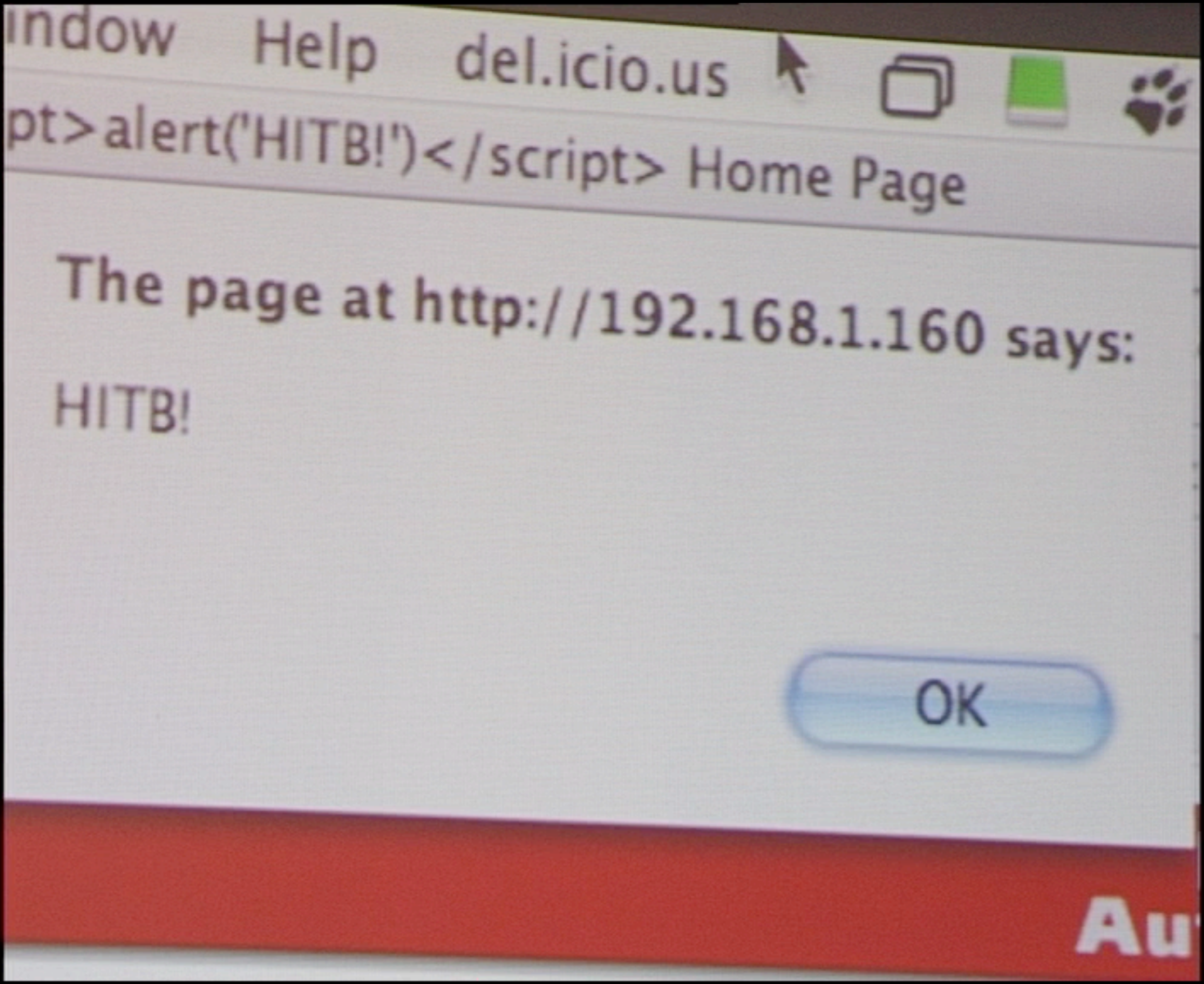
# intersan (1331/tcp)

# netbios-ns (137/udp)

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

Honours the source-route option / File server available

XSS

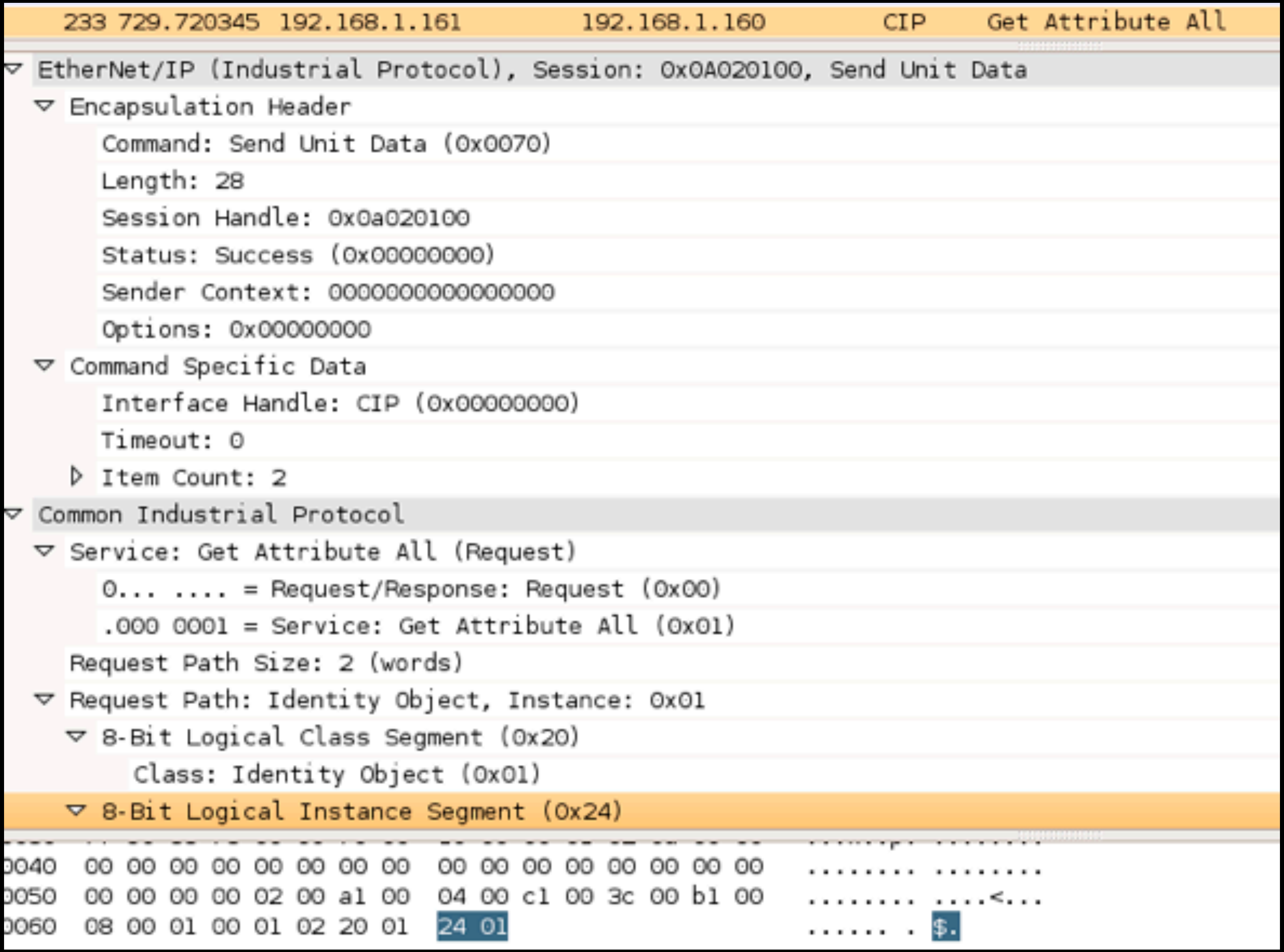


pt>alert('HITB!')</script> Home Page

The page at http://192.168.1.160 says:

HITB!

Clear Text 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

- 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

http://cristal.recursiva.org/

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.apogeonline.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

Visual Credits

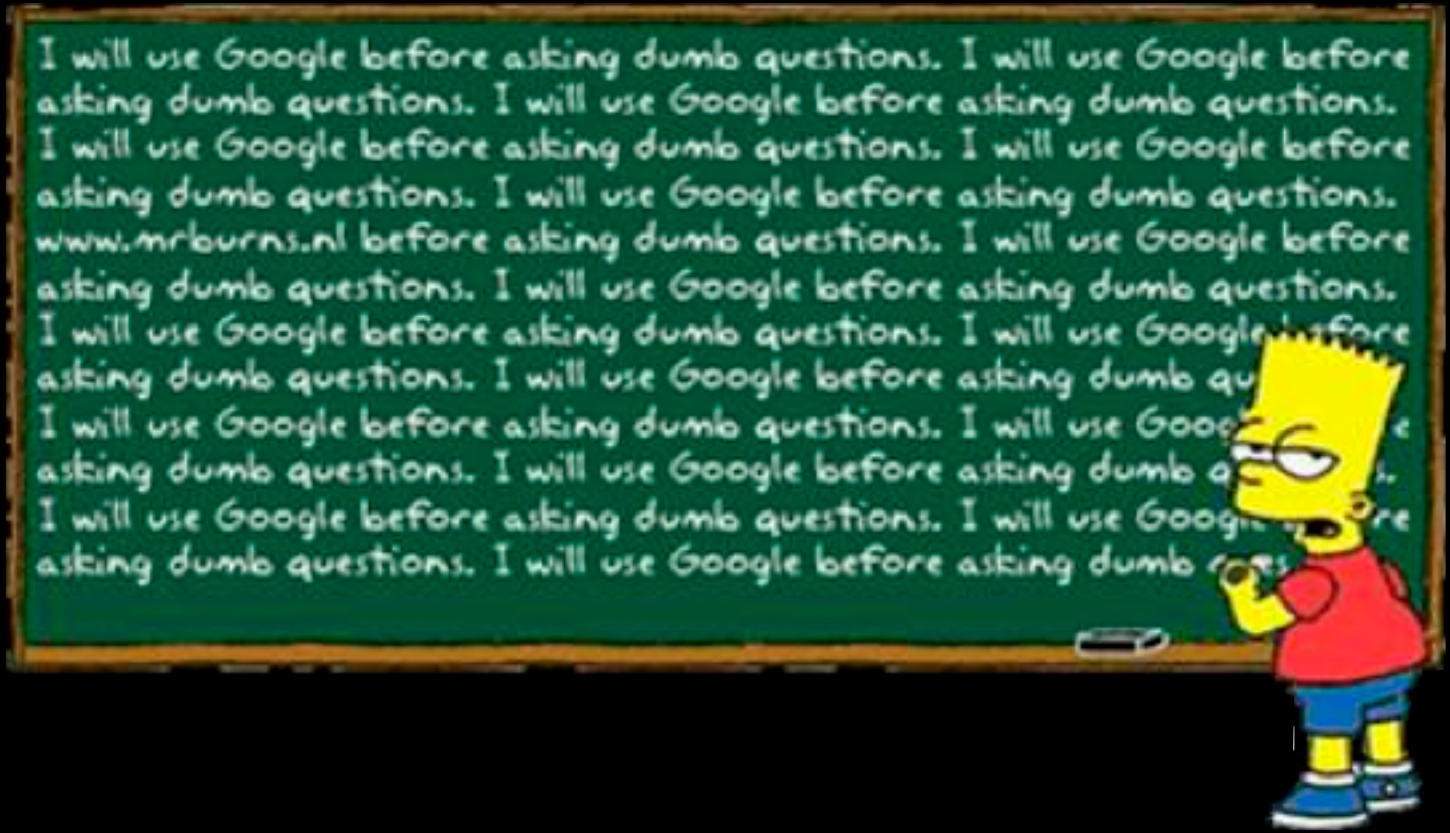
For graphics, video and ideas thanks to

Studio Miliani

http://www.miliani.it/

video@miliani.it

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. 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 Google before
asking dumb questions. I will use Google before asking dumb qu
I will use Google before asking dumb questions. I will use Goog
asking dumb questions. I will use Google before asking dumb q
I will use Google before asking dumb questions. I will use Goog
asking dumb questions. I will use Google before asking dumb

Thank You!

Raoul Chiesa
raoul@mediaservice.net

Alessio L.R. Pennasilico
mayhem@alba.st