



# Cybersecurity: un ecosistema fatto di persone

28

gennaio

ore 17.30

2020

Auditorium Casa dell'Economia,  
Via Tonale 30, Lecco

### Agenda

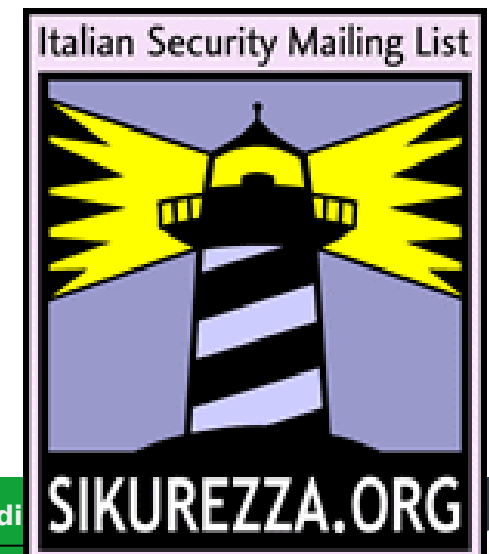
- **Industry 4.0**
- **Quali sono i rischi?**
- **Come proteggere i nostri impianti?**
- **Riferimenti**
- **Q&A**

# Igor Falcomatà

ifalcomata@enforcer.it

- **attività professionale:**
  - **analisi delle vulnerabilità e penetration testing**
  - **security consulting**
  - **formazione**
- **altro:**
  - **ISACA Venice**
  - **sikurezza.org**
  - **(f|er-|bz-)lug**

free advertising >



# Industry 4.0 Insecurity

## Agenda

- **Industry 4.0**
- Quali sono i rischi?
- Come proteggere i nostri impianti?
- Riferimenti
- Q&A

# Introduzione

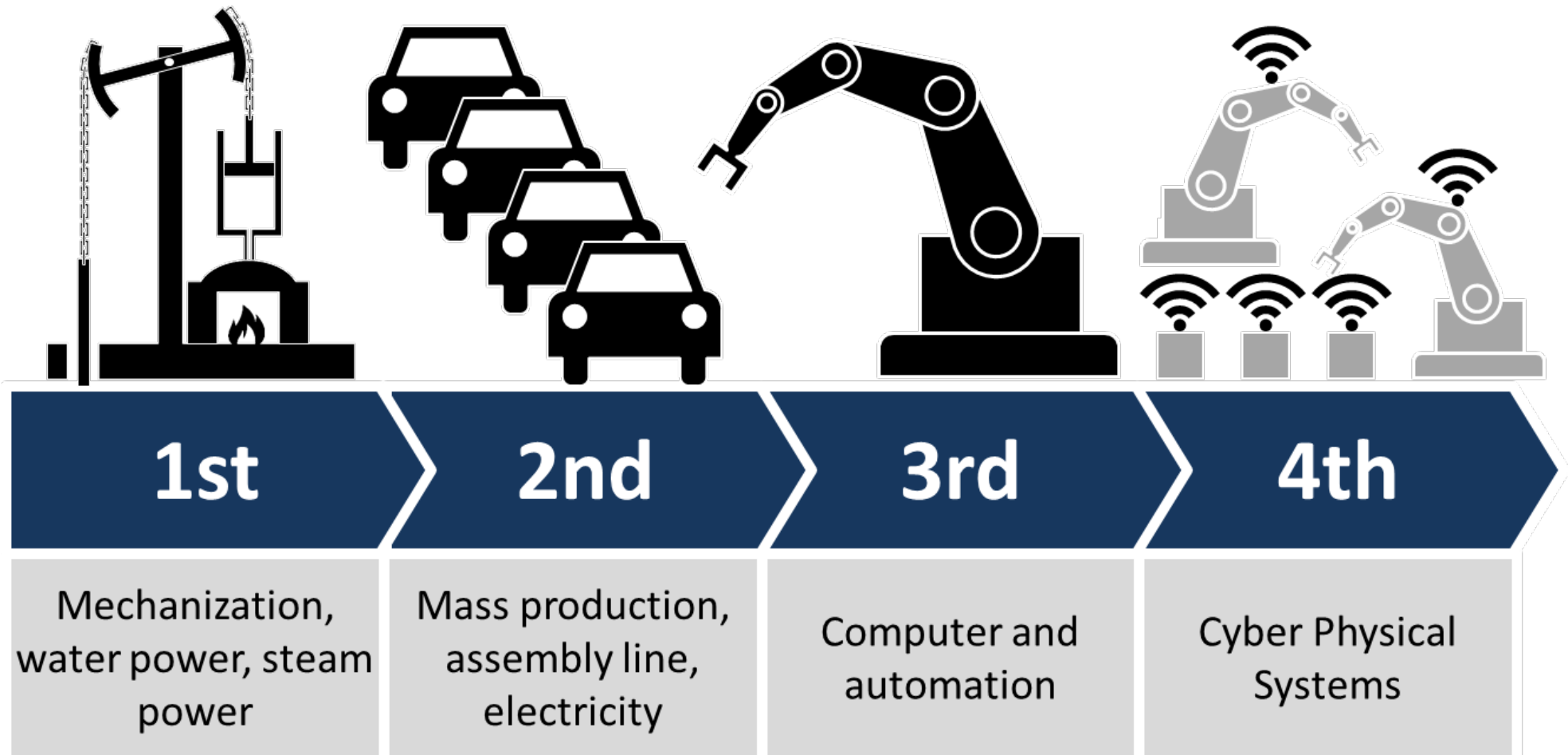
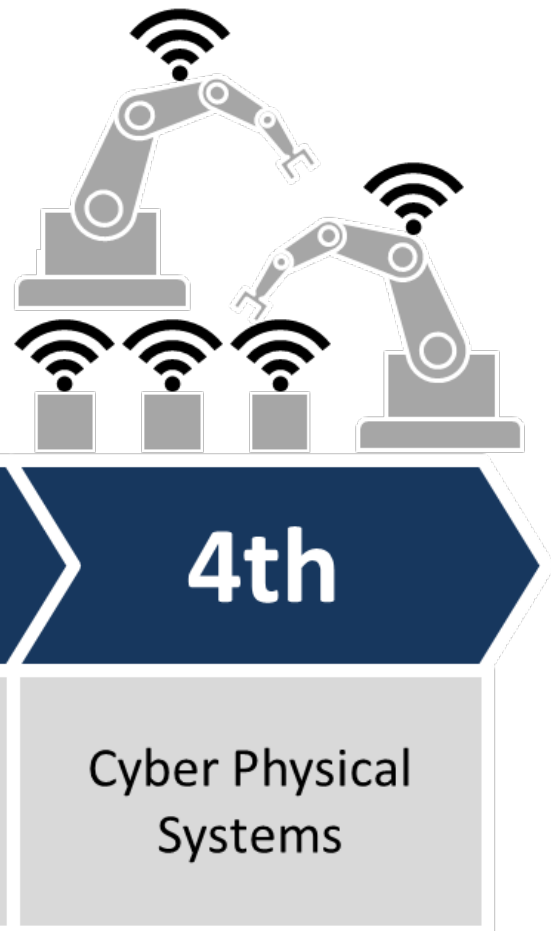


Image by ChristophRoser. Please credit "Christoph Roser at AllAboutLean.com".  
Own work, CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=47640595>

# Industry 4.0



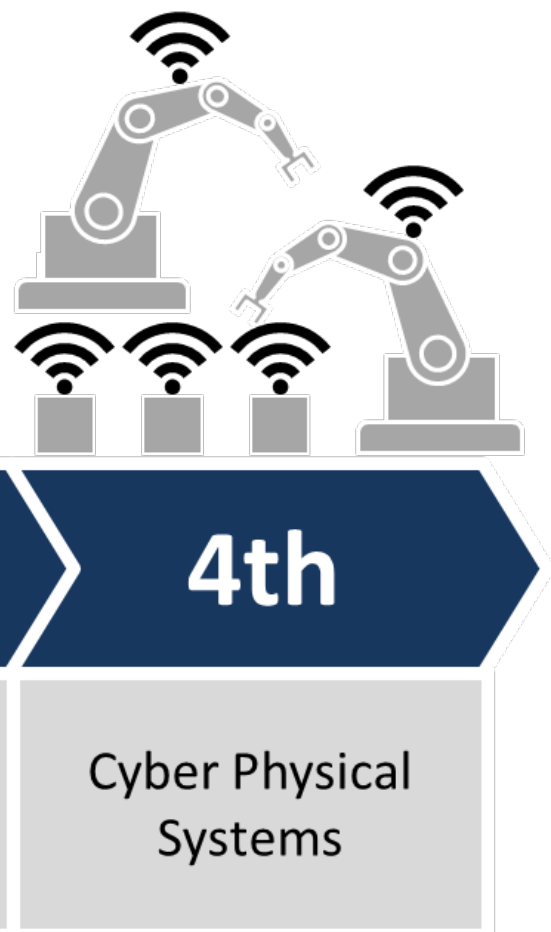
## Scambio di dati tra impianti industriali ed altre infrastrutture:

- **rete locale**
- **rete geografica / intranet**
- **Internet**

- **molti vantaggi**
- **molti rischi**

Image by ChristophRoser. Please credit "Christoph Roser at AllAboutLean.com".  
Own work, CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=47640595>

# Rete fabbrica



## Infrastruttura **complessa**:

- **tecnologia tradizionali “fabbrica”**
  - **PLC, ICS, SCADA, bus di comunicazione e interfacce “industriali”, sw dedicati, ..**
- **tecnologie tradizionali ICT**
  - **Ethernet, WiFi, TCP/IP, OS “server” e “workstation”, sw general purpose, virtualizzazione, storage, remote desktop e telecontrollo, ecc.**

Image by ChristophRoser. Please credit "Christoph Roser at AllAboutLean.com".  
Own work, CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=47640595>

# Industry 4.0 Insecurity

## Agenda

- Industry 4.0
- **Quali sono i rischi?**
- Come proteggere i nostri impianti?
- Riferimenti
- Q&A



Table 1: Threats affecting ICS/SCADA systems

[ENISA]

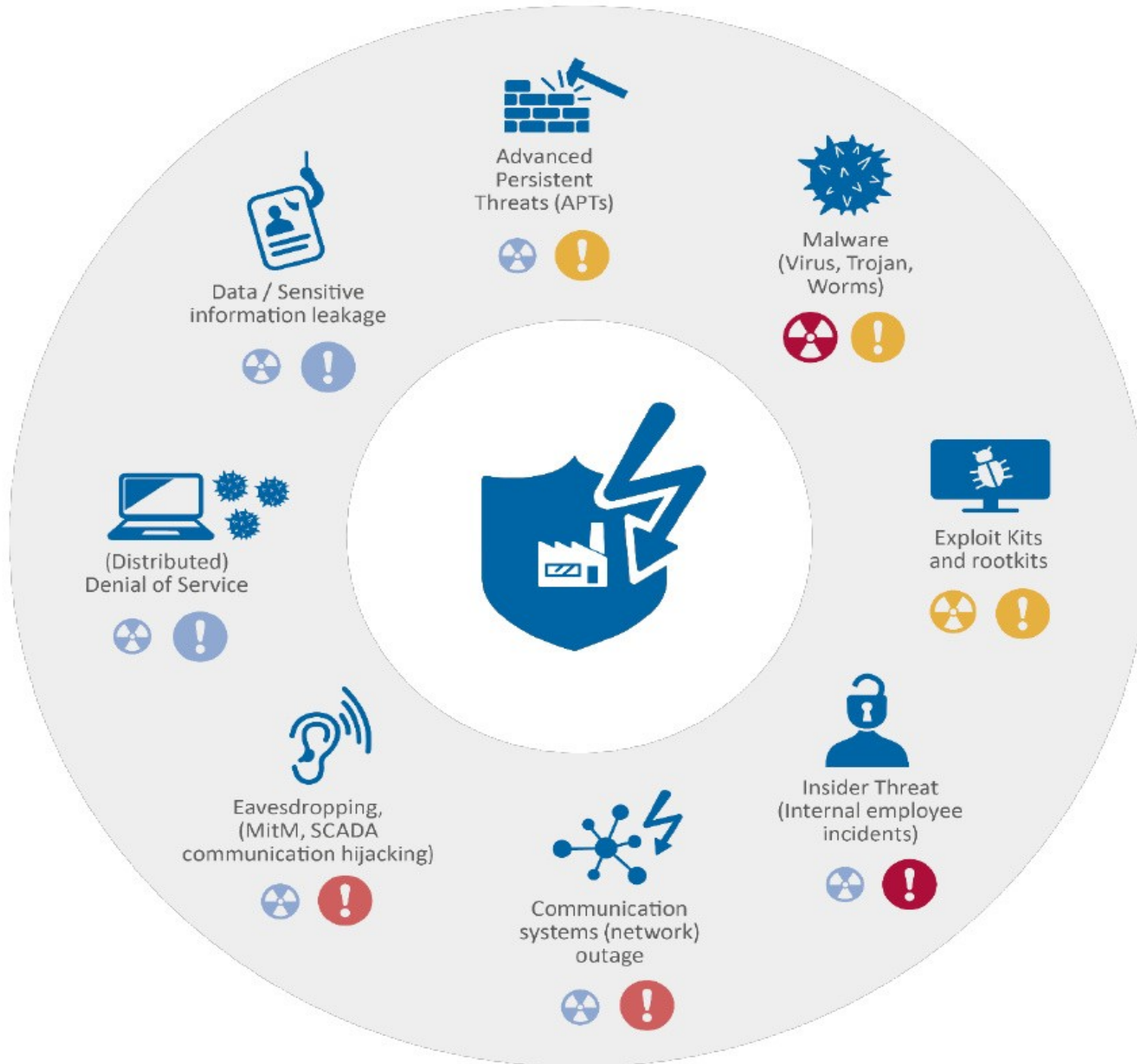


Image by ENISA,  
Communication network  
dependencies for ICS/SCADA  
Systems, pg. 29

**Spesso l'anello più debole (per la sicurezza informatica) sono le componenti dell'ambito "fabbrica":**

- non sono state pensate per essere utilizzate in ambienti potenzialmente "ostili" e "inaffidabili" (p. es. Internet)**
- il loro design è mirato a garantirne l'affidabilità nel processo produttivo**
- difficilmente integrano - almeno di default - meccanismi che garantiscano la segretezza delle comunicazioni**
- configurazioni "di default"**

Image by ENISA,  
Communication network  
dependencies for ICS/SCADA  
Systems, pg. 29

# Scenari di attacco

[ENISA]

Table 3: Sample Attack Scenarios

SAMPLE ATTACK SCENARIOS	IMPORTANCE LEVEL
1. Against the administration systems of SCADA	Crucial
2. Against actuators	High / Crucial
3. Against the network link between sensors/actuators and HMI or controller	High
4. Against sensors	Medium / Crucial
5. Against the information transiting the network	Medium / Crucial
6. Compromised ICT components as backdoors	Medium / Crucial
7. Exploit Protocol vulnerabilities	Medium / High
8. Against Control Data Historians, Local HMIs or controllers	Medium

Image by ENISA,  
Communication network dependencies for ICS/SCADA Systems, pg. 32

# Alcuni esempi..

HD Moore: Hackable Serial Port Servers Lack Authentication | Threatpost - Mozilla Firefox

File Edit View History Bookmarks Tools Help

threatpost.com/open-serial-port-connections-to-scada-ics-and-it-gear-discovered

## OPEN SERIAL PORT CONNECTIONS TO SCADA, ICS AND IT GEAR DISCOVERED

by **Michael Mimoso** [Follow @mike\\_mimoso](#) April 24, 2013 , 2:06 pm

Serial port servers are admittedly old school technology that you might think had been phased out as new IT, SCADA and industrial control system equipment has been phased in. Metasploit creator HD Moore cautions you to think again.

**Moore recently revealed** that through his Critical IO project research, he discovered 114,000 such devices connected to the Internet, many with little in the way of authentication standing between an attacker and a piece of critical infrastructure or a connection onto a corporate network. More than 95,000 of those devices were exposed over mobile connections such as 3G or GPRS.

Serial port servers, also known as terminal

**Data Requests**  
September 6, 2013

**Report: Online A**  
2013  
September 9, 2013

**NSA Bought Expl**  
**VUPEN, Contract**  
September 16, 2013

**Experts Lukewar**  
**Fingerprint Scan**  
September 11, 2013

**Critical SharePo**  
**Priority on Patch**  
September 10, 2013

**Ubuntu Forums F**  
**Password Breach**  
July 22, 2013 , 11:07

<http://threatpost.com/open-serial-port-connections-to-scada-ics-and-it-gear-discovered>

# Alcuni esempi..

Shodan - Mozilla Firefox

Shodan

Shodan Developers Book View All...

SHODAN

Explore Enterprise Access Contact Us

New to Shodan? Login or Register

## The search engine for the Web

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

### Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

### Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

### See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

### Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

**56% of Fortune 100**

**1,000+ Universities**

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

<https://www.shodan.io/>

# Alcuni esempi..

The screenshot shows the Shodan search engine interface in a Mozilla Firefox browser. The search query is 'siemens'. The page displays a summary of results and three detailed entries.

**TOTAL RESULTS**  
11,500

**TOP COUNTRIES**

Pakistan	2,676
United States	1,704
Czech Republic	1,066
France	837
Germany	667

**TOP SERVICES**

HTTP	1,715
HTTPS	1,289
SSH	1,285
SNMP	724
1028	516

**TOP ORGANIZATIONS**

Augere Pakistan, Qubee ...	1,936
Frontier Communications	1,095
AUGERE-Pakistan	728
Orange	518
Deutsche Telekom AG	201

**TOP OPERATING SYSTEMS**

**91.183.227.23**  
23.227-183-91.adsl-static.isp.belgacom.be  
**Skynet Belgium**  
Added on 2018-02-21 04:52:18 GMT  
Belgium, Haacht  
Technologies:   
[Details](#)

**SSL Certificate**  
Issued By:  
|- Common Name: **ccp.siemens.com**  
|- Organization: **Siemens Schweiz AG**  
Issued To:  
|- Common Name:  
**ozw.ccp.siemens.com**  
|- Organization: **Siemens Schweiz AG**  
**Supported SSL Versions**  
TLSv1.2

HTTP/1.1 200 OK  
Content-Type: text/html  
Accept-Ranges: bytes  
ETag: "1603869751"  
Last-Modified: Thu, 09 Mar 2017 08:29:30 GMT  
Content-Length: 565  
Date: Wed, 21 Feb 2018 04:52:17 GMT  
Server: **Siemens** Switzerland Ltd.

**84.144.12.126**  
p54900C7E.dip0.t-ipconnect.de  
**Deutsche Telekom AG**  
Added on 2018-02-20 13:13:53 GMT  
Germany, Hamburg  
[Details](#)

HTTP/1.1 301 Moved Permanently  
Location: https://84.144.12.126:8080/  
Content-Length: 0  
Date: Tue, 20 Feb 2018 13:02:29 GMT  
Server: **Siemens** Switzerland Ltd.

**91.183.229.217**  
217.229-183-91.adsl-static.isp.belgacom.be  
**Skynet Belgium**  
Added on 2018-02-20 12:08:31 GMT  
Belgium, Nivelles  
[Details](#)

HTTP/1.1 200 OK  
Content-Type: text/html  
Accept-Ranges: bytes  
ETag: "-278311248"  
Last-Modified: Tue, 24 Jul 2012 07:24:49 GMT  
Content-Length: 380  
Date: Tue, 20 Feb 2018 11:46:13 GMT  
Server: **Siemens** Switzerland Ltd.

<https://www.shodan.io/>

# Alcuni esempi..

The screenshot shows a web browser window displaying the Shodan search engine results for the query 'schneider'. The page layout includes a navigation bar with 'SHODAN' logo and search input, and a main content area with several sections:

- TOTAL RESULTS:** 1,425
- TOP COUNTRIES:** A world map with a table listing countries and their result counts:

Brazil	248
United States	238
France	223
Spain	97
Italy	75
- TOP SERVICES:** A table listing services and their result counts:

Modbus	703
Automated Tank Gauge	184
HTTP	116
BACnet	99
SNMP	45
- TOP ORGANIZATIONS:** A table listing organizations and their result counts:

Orange	183
Verizon Wireless	71
Turkcell	54
Vivo	37
Telefonica de Espana Sta...	27
- RELATED TAGS:** 'scada' and 'pci' buttons.
- Search Results:** Two detailed entries for 'Schneider Electric' devices. The first entry is for 'Netline Peru SA' (IP: 143.137.147.97) with details for Unit ID 1, 2, 3, and 4. The second entry is for 'Turkcell' (IP: 5.26.219.136) with details for Unit ID 1, 2, 3, and 4.

<https://www.shodan.io/>

# Alcuni esempi..

The screenshot shows the Shodan search engine interface in a Mozilla Firefox browser. The search query is 'modbus'. The page displays a summary of 243 total results, a world map highlighting top countries (United States, Poland, France, Germany, Greece), and a list of top services (FTP, Telnet, ntop, etc.). The main content area shows four specific search results for IP addresses: 82.143.151.2, 82.143.153.230, 207.148.211.83, and 195.25.103.138. Each result includes the IP address, a link to the host, the service name (Metro Ethernet Access Services or Bullseye Telecom), the location, and a list of detected services and their status.

**modbus - Shodan Search - Mozilla Firefox**

modbus - Shodan Se... x +

https://www.shodan.io/search?query=modbus

SHODAN | modbus | Explore | Enterprise Access | Contact Us | New to Shodan? | Login or Register

Exploits | Maps

**TOTAL RESULTS**  
243

**TOP COUNTRIES**

United States	70
Poland	64
France	16
Germany	16
Greece	15

**TOP SERVICES**

FTP	93
Telnet (Lantronix)	35
ntop	21
Telnet	19
SNMP	12

**TOP ORGANIZATIONS**

Metro Ethernet Access S...	22
Telefonia Dialog sp.z.o.o.	21
AT&T Internet Services	11
Orange	10
Deutsche Telekom AG	10

**TOP PRODUCTS**

**82.143.151.2**  
h82-143-151-2-static.e-wro.net.pl  
**Metro Ethernet Access Services**  
Added on 2018-02-18 06:54:14 GMT  
Poland, Nowy Dwor  
**Details**

- 220 Modbus-GPRS-Gateway FTP Server Ready
- 530 Not logged in.
- 502 Command not implemented
- 211-Features:
  - SIZE
- 211 End

**82.143.153.230**  
h82-143-153-230-static.e-wro.net.pl  
**Metro Ethernet Access Services**  
Added on 2018-02-18 06:43:14 GMT  
Poland, Nowy Dwor  
**Details**

- 220 Modbus-GPRS-Gateway FTP Server Ready
- 530 Not logged in.
- 502 Command not implemented
- 211-Features:
  - SIZE
- 211 End

**207.148.211.83**  
**Bullseye Telecom**  
Added on 2018-02-18 05:15:56 GMT  
United States, New Baltimore  
**Details**

- Lantronix Inc. - Modbus Bridge

**195.25.103.138**  
**Orange**  
Added on 2018-02-18 03:59:38 GMT  
France  
**Details**

- Lantronix Inc. - Modbus Bridge
- MAC address 00204ADFEA67
- Software version 02.4 (080807) XPTEX
- Press Enter to go into Setup Mode

<https://www.shodan.io/>



# Alcuni esempi..

The screenshot shows the Shodan search engine interface in a Mozilla Firefox browser. The search query is 'simatic', and there are 869 total results. The page is divided into several sections: a top navigation bar, a sidebar with filters, and a main content area with search results.

**SHODAN** simatic [Search] Explore Enterprise Access Contact Us New to Shodan? Login or Register

Exploits Maps

**TOTAL RESULTS**  
869

**TOP COUNTRIES**

Italy	92
Germany	88
United States	75
Spain	60
Taiwan	57

**TOP SERVICES**

SNMP	446
Siemens S7	375
Modbus	36
PPTP	6
NetBIOS	3

**TOP ORGANIZATIONS**

Deutsche Telekom AG	54
Taiwan Fixed Network	42
Open Computer Network	21
Telefonica de Espana Sta...	13
Orange	13

**TOP PRODUCTS**

**83.224.140.175**  
Vodafone Italy ask to use the space unassignment bu  
Added on 2018-02-20 10:15:43 GMT  
Italy  
Details  
Siemens, SIMATIC S7, CPU-1200, 6ES7 215-1BG40-0XB0, HW: 1, FW: V.4.0.0, S C-EOSC1735

**193.253.37.160**  
L'Puteaux-657-1-164-160.w193-253.abo.wanadoo.fr  
Orange  
Added on 2018-02-18 07:39:22 GMT  
France  
Details  
ICS  
Copyright: Original Siemens Equipment  
PLC name: SIMATIC 300  
Module type: CPU 313C  
Unknown (129): Boot Loader A  
Module: 6ES7 313-5BF03-0AB0 v.0.1  
Basic Firmware: v.2.6.3  
Module name: CPU 313C  
Serial number of module: S C-V9G433362007  
Plant identification:  
Basic Hardware: 6ES7 313-5BF03...

**166.130.153.204**  
mobile-166-130-153-204.mycingular.net  
AT&T Wireless  
Added on 2018-02-18 07:39:11 GMT  
United States  
Details  
Siemens, SIMATIC S7, CPU-1200, 6ES7 214-1HG40-0XB0, HW: 4, FW: V.4.1.3, S C-H2SC3963

**117.158.54.143**  
Henan Mobile Communications Co.,Ltd  
Added on 2018-02-18 07:13:57 GMT  
China, Zhengzhou  
Details  
Siemens, SIMATIC S7, CPU-200 SMART, 6ES7 288-1SR20-0AA0, HW: 5, FW: V.2.2.0, S V-J7AX7802

**131.117.150.75**  
075-150-117-131.ip-addrinexio.net  
Siemens SIMATIC S7 CPU1513-1 PN 6ES7 513-1AL00-0AB0 HW: 2 FW: V1.1.0 S C-D7SM35862013

<https://www.shodan.io/>

# Alcuni esempi..

The screenshot shows a web browser window displaying the Shodan search engine results for the query 'wago pfc'. The page layout includes a navigation bar with 'SHODAN' and search options, a sidebar with filters for 'Exploits' and 'Maps', and a main content area with a list of search results. Each result includes an IP address, organization name, product name, vendor ID, serial number, device type, and device IP. A world map highlights the top countries: Germany (15), Poland (10), France (9), Austria (8), and Italy (4). Other filters include 'TOP SERVICES' (SNMP: 37, EtherNetIP: 30) and 'TOP ORGANIZATIONS' (Telekom Austria: 7, mdex AG: 5, Orange: 5, Deutsche Telekom AG: 5, Orange Polska: 3). The 'TOP PRODUCTS' section lists 'Wago Corporation' with 19 results.

IP Address	Organization	Product Name	Vendor ID	Serial Number	Device Type	Device IP
80.122.225.250	Telekom Austria	WAGO 750-881 PFC ETHERNET	Wago Corporation	0xde06a48a	Communications Adapter	192.168.0.91
46.16.217.8	mdex AG	WAGO 750-881 PFC ETHERNET	Wago Corporation	0xde0ca3d3	Communications Adapter	192.168.0.100
193.216.131.14	Tele2 Croatia	WAGO 750-880 PFC Telecontr. ECO	Wago Corporation	0xde029b69	Communications Adapter	10.29.1.59
1.34.18.247	HiNet	WAGO 750-880 PFC ETHERNET				
79.232.114.122	Deutsche Telekom AG	WAGO 750-873 PFC Serial Modbus	Wago Corporation			

<https://www.shodan.io/>

# “ma saranno dispositivi poco importanti..”

Power Plants and Other Vital Systems Are Totally Exposed on the Internet | WIRED - Mozilla Firefox

Power Plants and Other Vital Systems Are Totally Exposed on the Internet

SHARE

11

TWEET

COMMENT

EMAIL

**Longtime Shut Down Active !!!!!**

1 / 17 Equipment at a facility in Mexico appears to have been shut down for a while, based on the red banner at the top of the screen, but that wouldn't necessarily prevent intruders from manipulating the settings. It's unclear what the equipment is, but Moldow, based in Denmark, makes industrial filter and ventilation systems as well as industrial fans.

**AIRFRANCE**

WUHAN FROM €474

RTN INC TAXES

DEPARTING FROM ROME

BOOK NOW

SEE CONDITIONS

**MOST POPULAR**

**BUSINESS**

Facebook Executive Rob Goldman Apologizes After Russia Tweets

NICHOLAS THOMPSON

**CULTURE**

The Math Behind Pennsylvania's Gerrymandered Map

ISSIE LAPOWSKY

<https://www.wired.com/2013/11/internet-exposed/>

# “ma a me non capiterà, non espongo ..”

Tesla's Cloud Hacked, Used to Mine Cryptocurrency - Mozilla Firefox

Tesla's Cloud Hacke... x +

https://gizmodo.com/teslas-cloud-hacked-used-to-mine-cryptocurrency-1823155247


Search

PRIVACY AND SECURITY

## Tesla's Cloud Hacked, Used to Mine Cryptocurrency

Dell Cameron  
Yesterday 11:05am • Filed to: TESLA

23.6K 21 4



STRUCTURE REIMAGINED

DESIGN STUDIO

MODEL S MODEL S PERFORMANCE

Hackers infiltrated Tesla's cloud environment and stole computer resources to mine for cryptocurrency, according to the security firm RedLock.

Facebook Share Twitter Tweet

<https://gizmodo.com/teslas-cloud-hacked-used-to-mine-cryptocurrency-1823155247>

**“ma a me non capiterà, non espongo ..”**

- **e i vostri fornitori?**
  - **sistemi di telecontrollo (Internet, 3/4G, ..)**
  - **“VpN”**
  - **infrastruttura Cloud**
  - **sicurezza della loro rete?**
  
- **e dal perimetro interno (LAN) ?**
  - **\$ nmap -sS -p 22,23,80,443,502,1433,5900,..**

# Agli hacker SCADA piace..

The screenshot shows a Mozilla Firefox browser window displaying the ConCollector website. The address bar shows the URL [cc.thinkst.com/searchMore/scada/](http://cc.thinkst.com/searchMore/scada/). The page title is "ConCollector" and the logo for "thinkst applied research" is visible in the top right. A navigation bar includes a search field with "Everything" selected and links for "Speakers", "Conferences", "Topics", "Contributors", "Analytics", "Folklore", "About", and "Login". The search results section shows "279 hits in 3.61830 seconds searching for scada". Below this, a section titled "Talk Titles and Abstracts: 279 results" lists various conference presentations related to SCADA security, such as "Hacking Smartwater Wireless Water Networks" and "Scada And Ics For Security Experts: How To Avoid Cyberdouchery".

**Search Results:** 279 hits in 3.61830 seconds searching for scada

**Talk Titles and Abstracts: 279 results**

- [Hacking Smartwater Wireless Water Networks — John McNabb at ShmooCon 2011](#)
- [Scada And Ics For Security Experts: How To Avoid Cyberdouchery — James Arlen at DEF CON 18](#)
- [Exploiting Scada Systems — Jeremy Brown at DEF CON 18](#)
- [Modscan: A Scada Modbus Network Scanner — Mark Bristow at DEF CON 16](#)
- [Unraveling Scada Protocols: Using Sulley Fuzzer — Ganesh Devarajan at DEF CON 15](#)
- [Scada And Ics For Security Experts: How To Avoid Cyberdouchery — James Arlen at Notacon 7](#)
- [Scada And Ics For Security Experts: How To Avoid Cyberdouchery — James Arlen at Blackhat USA 2010](#)
- [Wardriving The Smart Grid: Practical Approaches To Attacking Utility Packet Radios — Nathan Keltner, Shawn Moyer at Blackhat USA 2010](#)
- [Electricity For Free? The Dirty Underbelly Of Scada And Smart Meters — Jonathan Pollet at Blackhat USA 2010](#)
- [Hacking With Gnu Radio — David \( VideoMan \) Bryan at THOTCON 1](#)
- [Hacking Scada — Mayhem , Raoul "Nobody" Chiesa at Chaos Communication Congress 24](#)
- [Scada And National Critical Infrastructures: Is Security An Optional? — Raoul "Nobody" Chiesa at TROOPERS 2008](#)
- [Generic Electric Grid Malware Design - Attacking Scada System — Eyal Udassin at SysScan 2008](#)
- [Scada And Ics For Security Experts: How To Avoid Being A Cyber Idiot — James Arlen at Blackhat Europe 2010](#)
- [Hacking Scada: How To OWn Critical National Infrastructure — Alessio Mayhem at HITBSecConf Malaysia 2007](#)
- [Utilities, Oil & Gas, And Process Manufacturing — Gary Sevounts at SOURCE Boston 2008](#)
- [Scada And Ics For Security Experts: How To Avoid Cyberdouchery — James Arlen at SecTor 2010](#)


<http://cc.thinkst.com/>

# .. vulnerabilità pubbliche

http://nullcon.net the next security thing! nju

## Vulnerability Analysis of 2013 SCADA issues

Amol Sarwate  
Director of Vulnerability Labs, Qualys Inc.



International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 1

http://nullcon.net the next security thing! nju

## Agenda

SCADA components  
2013 Vulnerability Analysis  
Recommendations and Proposals

International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 2

http://nullcon.net the next security thing! nju

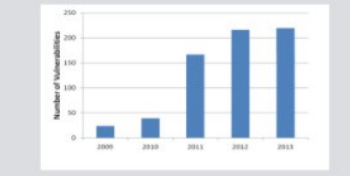


International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 3

http://nullcon.net the next security thing! nju

## 2009 - 2013 SCADA Vulnerabilities

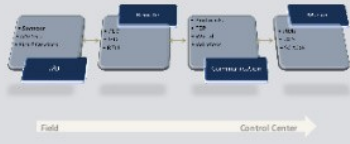


International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 4

http://nullcon.net the next security thing! nju

## Components



International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 5

http://nullcon.net the next security thing! nju

## Acquisition

Convert parameters like light, temperature, pressure or flow to analog signals



International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 6

http://nullcon.net the next security thing! nju

## Conversion

Converts analog and discrete measurements to digital information



International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 7

http://nullcon.net the next security thing! nju

## Communication

Front end processors (FER) and protocols  
Wired or wireless communication



International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 8

http://nullcon.net the next security thing! nju

## Presentation & Control

Control, monitor and alarming using human machine interface (HMI)



International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 9

http://nullcon.net the next security thing! nju

## 2013 Vulnerabilities by category




International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 10

http://nullcon.net the next security thing! nju

## Acquisition

- Requires physical access
- Field equipment does not contain process information
- Information like valve 16 or breaker 9B
- Without process knowledge leads to nuisance disruption




International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 11

http://nullcon.net the next security thing! nju

## Emerson ROC800 Vulnerabilities

- CVE-2013-0813: Network Session Invalidation allows detection
- CVE-2013-0812: OS Debug port service
- CVE-2013-0814: Hardcode accounts with passwords
- Access: HTTP, ACL, A/CN
- Impact: C/C, I/C, A/C
- Patch available from Emerson



International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 12

http://nullcon.net the next security thing! nju

## Siemens CP 1604 / 1616 Interface Card Vulnerability

- Siemens security advisory: SSA-038113
- CVE-2013-0619: Open Debugging Port in CP 1604/1616
- UDP port 37385
- Access: A/CN, ACL, A/CN
- Impact: C/C, I/C, A/C
- Patch available from Siemens



International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 13

http://nullcon.net the next security thing! nju

## Communication




International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 14

http://nullcon.net the next security thing! nju

## ModBus Vulnerabilities

- CVE-2013-2794: Triangle Research: Nario 10 PLC Crafted Packet Handling Remote DoS
- CVE-2013-3039: Gull 810-47100 PLC Crafted Modbus Packet Handling Remote DoS
- IES 2013-003: Schneider Electric Multiple Modbus MMAP DoS and RCE



International Security Conference Goa 2014

2014-The-year-in-which-we-cannot-ignore-SCADA  
A-by-Amol-Sarwate  
page 15

<https://nullcon.net/website/archives/pdf/2014-The-year-in-which-we-cannot-ignore-SCADA-by-Amol-Sarwate.pdf>

# .. continuamente ..

**CVE Details**  
The ultimate security vulnerability datasource

Log In Register Vulnerability Feeds & Widgets<sup>New</sup> [www.itsecdb.com](http://www.itsecdb.com)

**Schneider-electric : Security Vulnerabilities**

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9  
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : 90 Page : 1 (This Page) 2  
[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	<a href="#">CVE-2017-14024</a> <a href="#">119</a>			Exec Code Overflow	2017-11-13	2017-12-01	10.0	Admin	Remote	Low	Not required	Complete	Complete	Complete
A Stack-based Buffer Overflow issue was discovered in Schneider Electric InduSoft Web Studio v8.0 SP2 Patch 1 and prior versions, and InTouch Machine Edition v8.0 SP2 Patch 1 and prior versions. The stack-based buffer overflow vulnerability has been identified, which may allow remote code execution with high privileges.														
2	<a href="#">CVE-2017-13997</a> <a href="#">306</a>			Exec Code Bypass	2017-10-02	2017-11-02	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
A Missing Authentication for Critical Function issue was discovered in Schneider Electric InduSoft Web Studio v8.0 SP2 or prior, and InTouch Machine Edition v8.0 SP2 or prior. InduSoft Web Studio provides the capability for an HMI client to trigger script execution on the server for the purposes of performing customized calculations or actions. A remote malicious entity could bypass the server authentication and trigger the execution of an arbitrary command. The command is executed under high privileges and could lead to a complete compromise of the server.														
3	<a href="#">CVE-2017-9962</a> <a href="#">119</a>			Overflow	2017-09-25	2017-10-10	5.0	None	Remote	Low	Not required	None	None	Partial
Schneider Electric's ClearSCADA versions released prior to August 2017 are susceptible to a memory allocation vulnerability, whereby malformed requests can be sent to ClearSCADA client applications to cause unexpected behavior. Client applications affected include ViewX and the Server Icon.														
4	<a href="#">CVE-2017-9961</a> <a href="#">284</a>			Exec Code	2017-09-25	2017-10-10	4.6	None	Local	Low	Not required	Partial	Partial	Partial
A vulnerability exists in Schneider Electric's Pro-Face GP Pro EX version 4.07.000 that allows an attacker to execute arbitrary code. Malicious code installation requires an access to the computer. By placing a specific DLL/OCX file, an attacker is able to force the process to load arbitrary DLL and execute arbitrary code in the context of the process.														
5	<a href="#">CVE-2017-9960</a> <a href="#">200</a>			+Info	2017-09-25	2017-09-27	5.0	None	Remote	Low	Not required	Partial	None	None
An information disclosure vulnerability exists in Schneider Electric's U.motion Builder software versions 1.2.1 and prior in which the system response to error provides more information than should be available to an unauthenticated user.														



# Industry 4.0 Insecurity

## Agenda

- Industry 4.0
- Quali sono i rischi?
- **Come proteggere i nostri impianti?**
- Riferimenti
- Q&A

# Best practices

[ENISA]

## **Include security as a main consideration during the design phase of ICS/SCADA systems.**

**Traditionally, only safety is included as one of the main considerations during the design of the ICS/SCADA systems, infrastructures or assets (alongside efficiency, real-time constraints, etc.), but security was usually omitted. The objective is to ensure that security is included as one of these main considerations not only during the design phase but also during the update of the systems.**

Communication network dependencies for ICS/SCADA Systems, pg. 8

# Best practices

[ENISA]

## Identify and establish roles of people operating in ICS/SCADA systems.

**The management of the access privileges of users in ICS/SCADA systems is a critical process. The objective is to improve this process to ensure that the privilege assignation is adequately controlled and unauthorised access to systems, either intentional or accidental, is reduced to a minimum.**

Communication network dependencies for ICS/SCADA Systems, pg. 8

# Best practices

[ENISA]

## Define network communication technologies and architecture with interoperability in mind.

**As ICS/SCADA systems are becoming more interconnected with other systems, not only from the same organisation but also with external ones, interconnectivity and compatibility become critical factors.**

**The objective is to focus on promoting the use of common protocols and technologies that are compatible across different devices from multiple manufacturers, avoiding locked proprietary protocols and technologies.**

Communication network dependencies for ICS/SCADA Systems, pg. 8

# Best practices

[ENISA]

**Establish brainstorming and communication channels for the different participants in the lifecycle of the devices to exchange needs and solutions.**

**Another point of concern is that there is usually a lack of communication between the different actors involved across the lifecycle of the ICS/SCADA assets and devices. The need to improve between all these parties involved is a factor that would definitely improve the security of the systems, as needs and solutions would be shared across all.**

Communication network dependencies for ICS/SCADA Systems, pg. 8

# Best practices

[ENISA]

## **Include the periodic ICS/SCADA device update process as part of the main operations of the systems.**

**The process of updating the software and firmware of ICS/SCADA devices is a relatively new process, and a very delicate one. Traditionally, this was not needed as there was no interconnection and the threats were limited to physical tampering. Nowadays, the update process needs to be added as part of the lifecycle of the devices, including periodical update processes, to ensure that they are protected against the threats they are exposed to.**

Communication network dependencies for ICS/SCADA Systems, pg. 8

# Best practices

[ENISA]

## **Establish periodic ICS/SCADA security training and awareness campaign within the organisation.**

**The concept of cyber-security is relatively new in ICS/SCADA environments, as it was not needed traditionally. Therefore, there is a need to ensure that the staff is aware of the threats that they are exposed to on a daily basis, both in their operations and in the systems they operate with.**

Communication network dependencies for ICS/SCADA Systems, pg. 8

# Best practices

[ENISA]

## **Promote increased collaboration amongst policy decision makers, manufacturers and operators at an EU Level.**

**Nowadays, critical infrastructures have become linked with the cyberspace, taking advantage of the functionality and benefits it offers. However, this brings about the need to make critical systems and infrastructures safer and more reliable, in order to protect them from the new threats that have arisen from this new interconnectivity level. This also needs to be addressed by policy makers, manufacturers and operators in order to ensure that they are aligned with this objective.**

Communication network dependencies for ICS/SCADA Systems, pg. 8



# Best practices

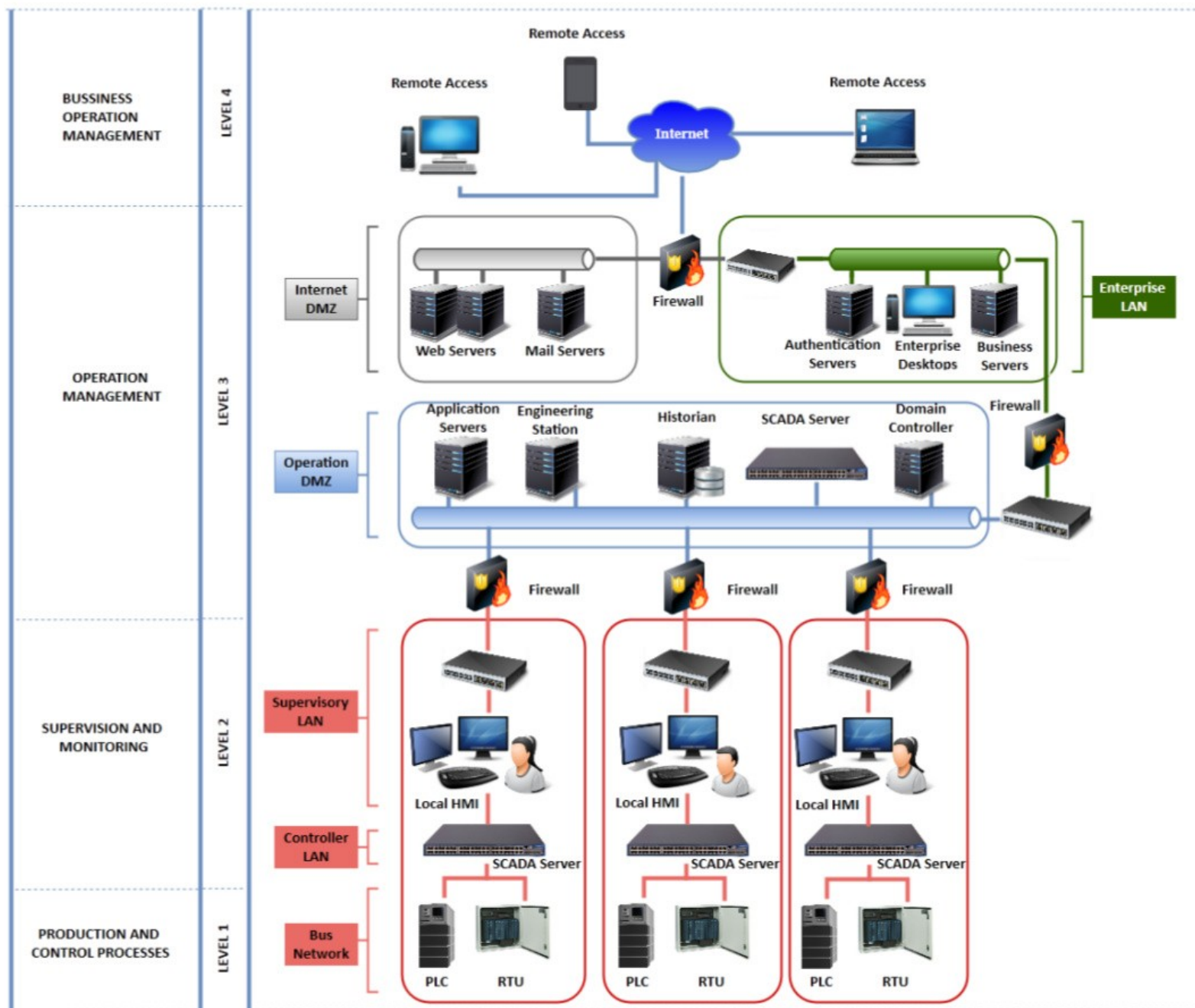
[ENISA]

## Define guidelines for the establishment of reliable and appropriate cybersecurity insurance requirements.

**The critical infrastructures of the organisations are now more exposed than ever to threats and attackers worldwide due the use of network communications and the Internet. This leads to the appearance of insurance solutions to protect the assets in case of an incident. For this purpose, it is recommended to establish guidelines on proper insurance coverage to help both organisations and companies in providing and making use of these services.**

Communication network dependencies for ICS/SCADA Systems, pg. 8

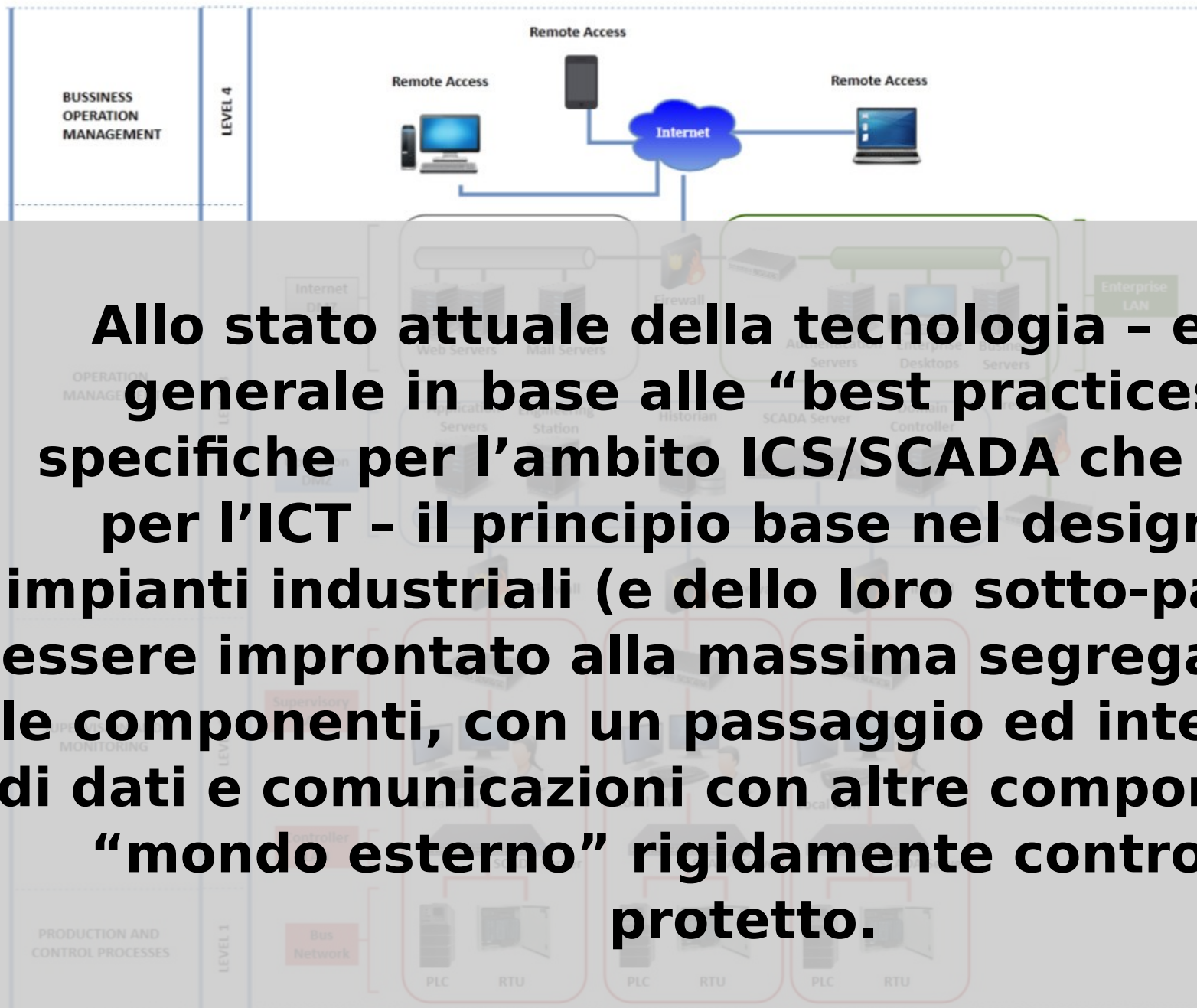
Figure 2: ISA95 levels applied to a SCADA architecture.



[ENISA]

Image by ENISA,  
Communication network  
dependencies for ICS/SCADA  
Systems, pg. 17

Figure 2: ISA95 levels applied to a SCADA architecture.



[ENISA]

**Allo stato attuale della tecnologia - e più in generale in base alle “best practices” sia specifiche per l’ambito ICS/SCADA che generali per l’ICT - il principio base nel design degli impianti industriali (e dello loro sotto-parti) deve essere improntato alla massima segregazione tra le componenti, con un passaggio ed interscambio di dati e comunicazioni con altre componenti ed il “mondo esterno” rigidamente controllato e protetto.**

Image by ENISA,  
Communication network  
dependencies for ICS/SCADA  
Systems, pg. 17

# Progettazione

- **Security “by design” (linee guida..)**
- **Collaborazione con lo staff ICT**
- **Sicurezza fisica e logica**
- **Collaborazione con fornitori terzi (clausole contrattuali..)**
- **Audit e revisione..**
- **.. da una terza parte autorevole e indipendente**

# Messa in opera

- **Documentazione dettagliata asset**
- **Aggiornamenti (firmware, OS, applicazioni)**
- **Utenze (“di default” o “deboli”)**
- ***Hardening***
- **(Remote) management**
- **Monitoraggio e log management**

# Particolare attenzione a..

- **Affidabilità (networking/apparati HA, ..)**
- **Ciclo di vita apparati**
- **Contratti di supporto hw/sw**
- **Copie di sicurezza config/dati**
- **Comunicazioni *wireless***
- ***(No) Internet***

# Gestione della sicurezza

- **Business Impact Analysis**
- **Analisi del rischio (informatico)**
- **Analisi delle vulnerabilità**
- **Simulazione di attacco**
- **Analisi e risposta agli incidenti**

# VA e PT

- **VA != PT**
- **Competenze specialistiche**
- **particolare “delicatezza” per ICS/SCADA**
- **Effettuato da una “terza parte”**

*“Molti apparati industriali, soprattutto quelli più vecchi, potrebbero bloccarsi o funzionare in maniera inaspettata se sottoposti senza cautele alle tecniche di analisi delle vulnerabilità o simulazione di attacco utilizzate in ambito ICT.”*



# Industry 4.0 Insecurity

## Agenda

- Industry 4.0
- Quali sono i rischi?
- Come proteggere i nostri impianti?
- **Riferimenti**
- **Q&A**

# Riferimenti

## **Communication network dependencies for ICS/SCADA Systems (ENISA)**

<https://www.enisa.europa.eu/publications/ics-scada-dependencies>

## **Guide to Industrial Control Systems (ICS) Security (NIST, SP-800-82 r2)**

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf>

## **Securing Industrial Control Systems-2017 (SANS Institute)**

<https://www.sans.org/reading-room/whitepapers/analyst/securing-industrial-control-systems-2017-37860>

## **ISO/IEC 27001:2013**

<https://www.iso.org/standard/54534.html>

## **CIS Critical Security Controls**

<https://www.sans.org/critical-security-controls>

## **OWASP (Open Web Application Security Consortium)**

<https://www.owasp.org/>

# Domande ?



<http://creativecommons.org/licenses/by-sa/2.0/it/deed.it>