



# Security in Industry 4.0: Control Systems and Robots

Stefano Zanero, PhD

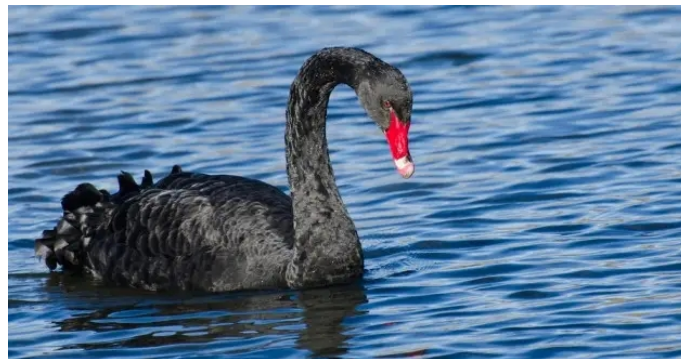
Associate Professor, Politecnico di Milano



- All systems are vulnerable
- *Vulnerabilities*, their *exploitability* and the existence and prevalence of *threats* combine with the potential of *damage* to create *risks*

$$• R = A * V * T$$

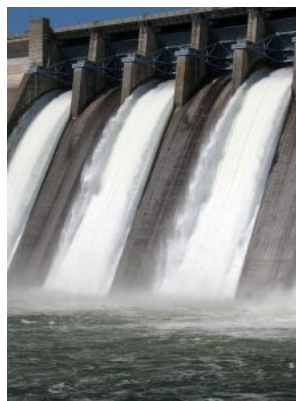
- The issue of securing *critical systems* is that it is very difficult to gauge the product of very low probabilities times very high potential damage







## A: Critical infrastructure





# T: Quasi-accidental catastrophes

DAVID CENCIOTTI WEBLOG

# THE AVIATIONIST®


HOMEABOUTSPECIAL REPORTSCONTACTSADVERTISE WITH US

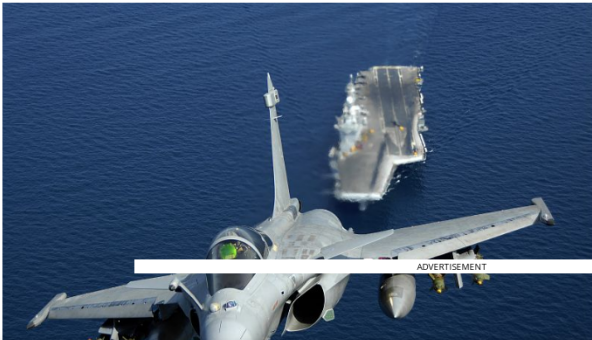
NEWS TICKER >February 25, 2021ATAC Mirage F1B Has Crashed Off The End Of The Flight Line At TyndallSEARCH ...

HOME > AVIATION > French Navy Rafales grounded by a computer virus








## French Navy Rafales grounded by a computer virus

February 13, 2009Aviation, Aviation Safety / Air Crashes, Hacking, Information Security, Information Warfare, Military Aviation

DAVID CENCIOTTI  
TWITTERFACEBOOKINSTAGRAM



### STAY CONNECTED



### CATEGORIES

Select Category▼

### ARCHIVE

Select Month▼

# THE WALL STREET JOURNAL.

English Edition | Print Edition | Video | Podcasts | Latest Headlines

HomeWorldU.S. PoliticsEconomyBusinessTechMarketsOpinionLife & ArtsReal Estate

## Computer Viruses Disrupt Railroad and Air Traffic

By Robert A. Guth and Daniel MachalabaStaff Reporters of The Wall Street Journal  
Aug. 21, 2003 4:21 pm ET

 PRINT  TEXT

An onslaught of rogue computer programs continued to clog computer networks, disrupting important commercial infrastructure as the problem escalated beyond a mere office nuisance in some cases.

In one of the most serious incidents, [CSX Corp.](#), the third-largest railroad company in North America, said it temporarily stopped service Wednesday after one of the fast-moving computer viruses struck this week. The day before, some passengers of [Air Canada](#)



# The power grid...

[Mobile UPI](#) | [About UPI](#) | [UPI en Español](#) | [UPIU - University Media Alliance](#) | [My Account](#)

Search:

**UPI.com**  
100 YEARS OF JOURNALISTIC EXCELLENCE

**PROINSO**  
IMMEDIATE AVAILABILITY!  
[www.proinso.net](http://www.proinso.net)

11000 TL  
**SMA**



+



230 Wp Poly  
**Trinasolar**

**SECURE YOUR PROJECT**  
BOOK YOUR MODULES AND INVERTERS NOW  
[www.proinso.net](http://www.proinso.net)

[Home](#) | [Top News](#) | [Entertainment](#) | [Odd News](#) | [Business](#) | [Sports](#) | [Science](#) | [Health](#) | [Real Estate](#) | [Photos](#) | [Videos](#)

Resource Wars    Global Water Issues

You are here: [Home](#) / [Energy Resources](#) / [Computer virus in Australian power grid](#)

## Energy Resources

### Computer virus in Australian power grid

Published: Oct. 2, 2009 at 4:22 PM

SYDNEY, Oct. 2 (UPI) -- A "sinister" computer virus has infected computers controlling Australia's Integral Energy power grid

1

**PROINSO** IMMEDIATE AVAILABILITY!  
**SECURE YOUR PROJECT**  
11000 TL **SMA** +  230 Wp Poly **Trinasolar**  
[www.proinso.net](http://www.proinso.net)  
BOOK YOUR MODULES AND INVERTERS NOW  
[www.proinso.net](http://www.proinso.net)



Internet





# T: Financially-motivated attacks



[Aluminium](#) [Energy](#)

[Sustainability](#)

[Careers](#)

[Investors](#)

[Media](#)

[About Hydro](#)



[Contact us](#)

[EN](#)

[Other countries](#) ▾

[Media](#) / [Topics](#) / [Cyber-attack on Hydro](#)

## Media

[Media contacts](#)

[News](#)

[Topics](#)

[Cyber-attack on Hydro](#)

[The Alunorte situation](#)

[Karmøy technology pilot](#)

[Media gallery](#)

[Podcast: Hydro talks](#)

[Events](#)

[Hydro at a glance](#)

[Brand Center](#)

## Cyber-attack on Hydro

Hydro became victim of an extensive cyber-attack in the early hours of Tuesday, March 19, 2019, impacting operations in several of the company's business areas.

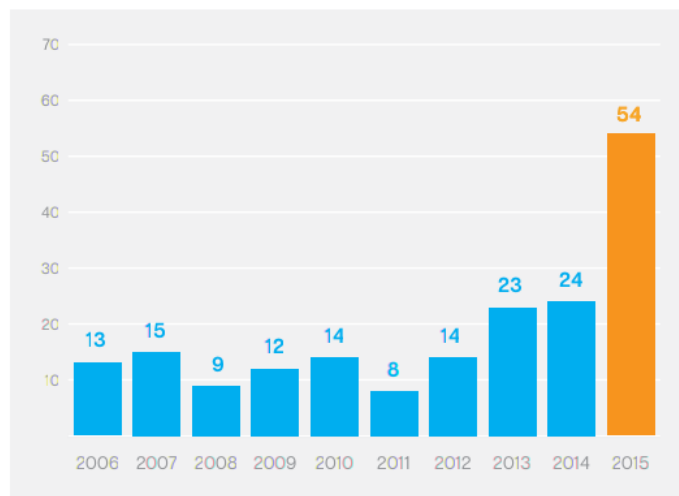




# Targeted attacks for everyone

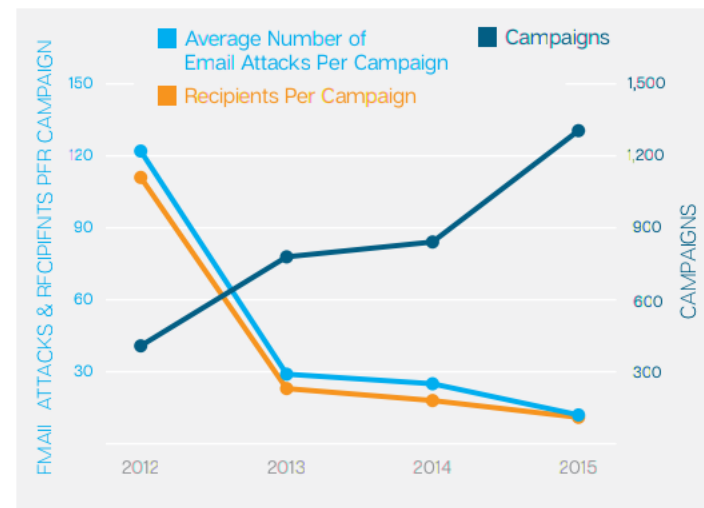
## Zero-Day Vulnerabilities, Annual Total

- The highest number of zero-day vulnerabilities was disclosed in 2015, evidence of the maturing market for research in this area.



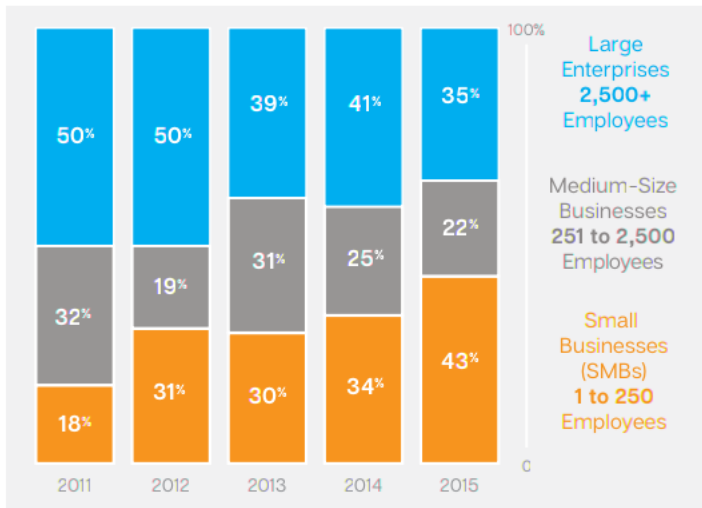
## Spear-Phishing Email Campaigns

- In 2015, the number of campaigns increased, while the number of attacks and the number of recipients within each campaign continued to fall. With the length of time shortening, it's clear that these types of attacks are becoming stealthier.



## Spear-Phishing Attacks by Size of Targeted Organization

- Attacks against small businesses continued to grow in 2015, although many of these attacks were directed to fewer organizations, increasing by 9 percentage points.



Source: Symantec Internet Security Threat Report 2016



# T: State-sponsored (and hacktivist) actors



Blog Bulletin VB T

## Last-minute paper: Back in BlackEnergy: 2014 targeted attacks in the Ukraine and Poland

Thursday 25 September 12:00 - 12:30, Green room.

Robert Lipovsky ESET  
Anton Cherepanov ESET

A large number of state organizations and businesses from various industry fields in the Ukraine and Poland have been targeted in recent attacks. What would otherwise be a mundane scenario in today's world of cybercrime is spiced up by the fact that the malware-spreading campaigns have leveraged the tense current geopolitical situation in Eastern Ukraine and the use of a malware family with a rich history. The most recent campaigns are dated.

BlackEnergy is a trojan which has undergone significant functional changes since its debut in 2007. It has evolved from a relatively simple DDoS trojan into a more sophisticated tool with a modular architecture, making it a suitable tool for sending spam and for launching attacks. BlackEnergy version 2, which featured rootkit techniques, was documented in a paper. Recent attacks recently discovered are proof that the trojan is still alive and kicking in

## Threat Research

### Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure

December 14, 2017 | by Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer

MALWARE ICS SECURITY

#### Introduction

Mandiant recently responded to an incident at a critical infrastructure organization where an attacker deployed malware designed to manipulate industrial safety systems. The targeted systems provided emergency shutdown capability for industrial processes. We assess with moderate confidence that the attacker was developing the capability to cause physical damage and inadvertently shutdown operations. This malware, which we call TRITON, is an attack framework built to interact with Triconex Safety Instrumented System (SIS) controllers. We have not attributed the incident to a threat actor, though we believe the activity is consistent with a nation state preparing for an attack.

TRITON is one of a limited number of publicly identified malicious software families targeted at industrial control systems (ICS). It follows Stuxnet which was used against Iran in 2010 and Industroyer which we believe was deployed by Sandworm Team against Ukraine in 2016. TRITON is consistent with these attacks, in that it could prevent safety mechanisms from executing their intended function, resulting in a physical consequence.



Data Centre Cloud Software Hardware Networks Security Jobs Business Policy Science Bootnotes

Print Tweet Like 44

Alert

Hack on Saudi Aramco hit 30,000 workstations, oil firm admits  
First hacktivist-style assault to use malware?

By John Leyden • Get more from this author

Posted in Security, 29th August 2012 09:18 GMT

**Analysis** Saudi Aramco said that it had put its network back online on Saturday, 10 days after a malware attack flooded 30,000 workstations at the oil giant.

In a statement, Saudi Arabia's national oil firm said that it had "restored all its main internal network services" hit by a malware outbreak that struck on 15 August. The firm said its core business of oil production and exploration was not affected by the attack, which resulted in a decision to suspend



# It's not just about the business

## How Stuxnet Spreads

Experts who have disassembled the code of the Stuxnet worm say it was designed to target a specific configuration of computers and industrial controllers, likely those of the Natanz nuclear facility in Iran.

### INITIAL INFECTION

Stuxnet can enter an organization through an infected removable drive. When plugged into a computer that runs Windows, Stuxnet infects the computer and hides itself.

### UPDATE AND SPREAD

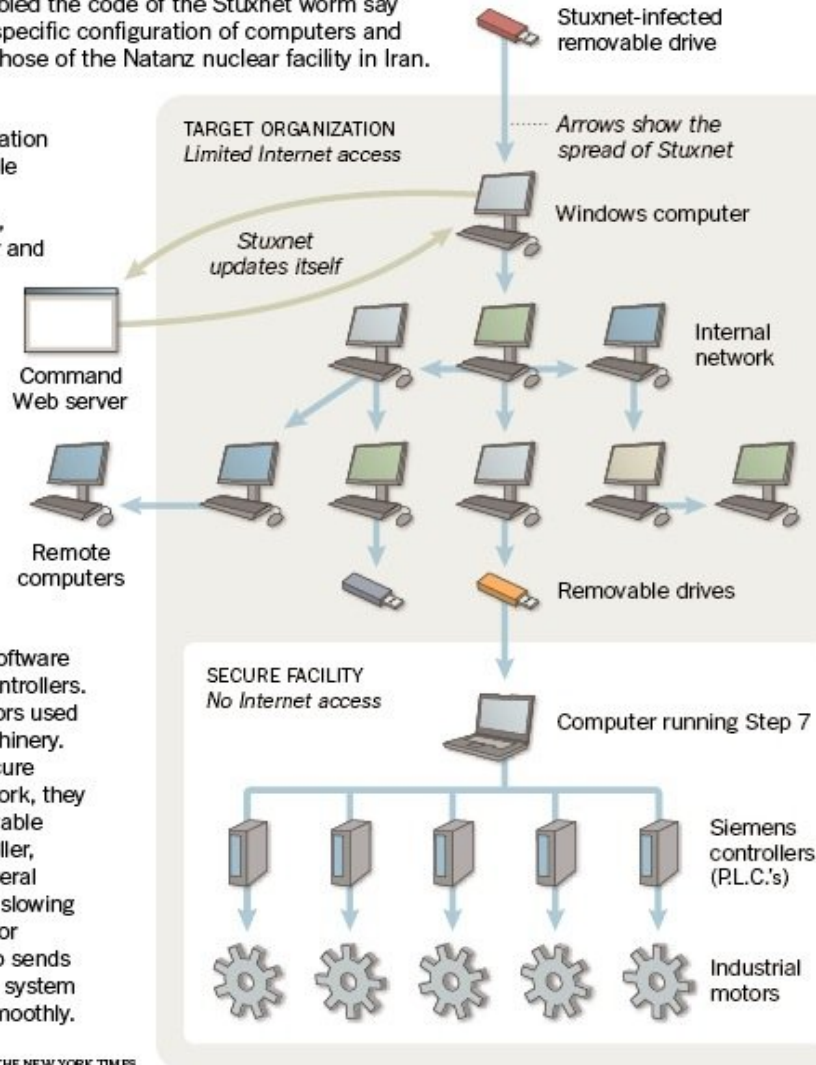
If the computer is on the Internet, Stuxnet may try to download a new version of itself. Stuxnet then spreads by infecting other computers, as well as any removable drives plugged into them.

### FINAL TARGET

Stuxnet seeks out computers running Step 7, software used to program Siemens controllers. The controllers regulate motors used in centrifuges and other machinery. While the computers in a secure facility may not be on a network, they can be infected with a removable drive. After infecting a controller, Stuxnet hides itself. After several days, it begins speeding and slowing the motors to try to damage or destroy the machinery. It also sends out false signals to make the system think everything is running smoothly.

Source: Symantec

THE NEW YORK TIMES







## V: no human in the middle



BRIDGE  
CHECKERS  
CHESS  
POKER  
FIGHTER COMBAT  
GUERRILLA ENGAGEMENT  
DESERT WARFARE  
AIR-TO-GROUND ACTIONS  
THEATERWIDE TACTICAL WARFARE  
THEATERWIDE BIOTOXIC AND CHEMICAL WARFARE  
GLOBAL THERMONUCLEAR WAR





In the real world...

# DealB%k

ANDREW ROSS SORKIN  
EDITOR-AT-LARGE

The New York Times

SEARCH DEALBOOK

Go

MERGERS & ACQUISITIONS

INVESTMENT BANKING

PRIVATE EQUITY

HEDGE FUNDS

I.P.O./OFFERINGS

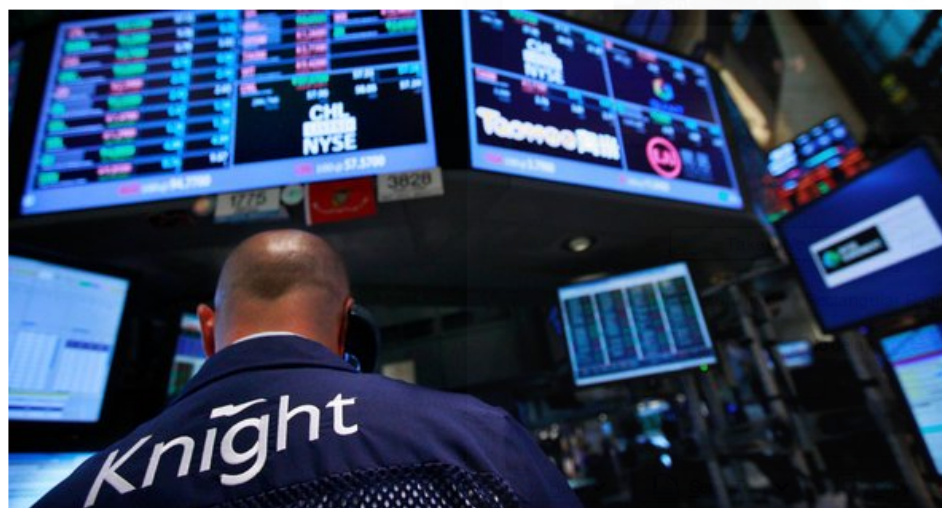
VENTURE CAPITAL

LEGAL/REGULATORY

LEGAL/REGULATORY | AUGUST 2, 2012, 9:07 AM | 357 Comments

## Knight Capital Says Trading Glitch Cost It \$440 Million

BY NATHANIEL POPPER



Brendan McDermid/Reuters

< 1 2 3 4 >

Errant trades from the Knight Capital Group began hitting the New York Stock Exchange almost as soon as the opening bell rang on Wednesday.

4:01 p.m. | Updated

\$10 million a minute.

PREVIOUS ARTICLE

Former Treasury  
Official to Join  
Romney Campaign

NEXT ARTICLE

Apollo's 2nd-Quarter  
Profit Falls 84%

### The Wire

- AUG 15, 12:53 PM .... **Punk Band Crashes Russia's Investment Case**  
WSJ.COM
- AUG 15, 12:50 PM .... **Deere and Drought: An Outlook for Crop Demand**  
AP
- AUG 15, 12:50 PM .... **AIG Not on the Hook for Policyholders' Madoff Claims: U.S. Court**  
NYTIMES
- AUG 15, 12:40 PM .... **Tencent Profit Rises Despite Headwinds**  
WSJ.COM
- AUG 15, 12:14 PM .... **That Ten Commandments Statue Isn't Going Anywhere Fast**  
WSJ.COM

### News by Sector

- |                            |                 |
|----------------------------|-----------------|
| Energy                     | Technology      |
| Industrials                | Financials      |
| Cyclical Goods & Services  | Real Estate     |
| Autos                      | Basic Materials |
| Media                      | Health Care     |
| Non-Cycl. Goods & Services | Telecom         |
| Food & Beverage            | Utilities       |

### More New York Times News by Sector

GLOBAL ENERGY MEDIA TECH HEALTH CARE

State of the Art: Samsung's Rival for the iPad Loads on the Features  
Samsung's new iPad rival, the Galaxy Note 10.1, is loaded



# V: Complexity of networks



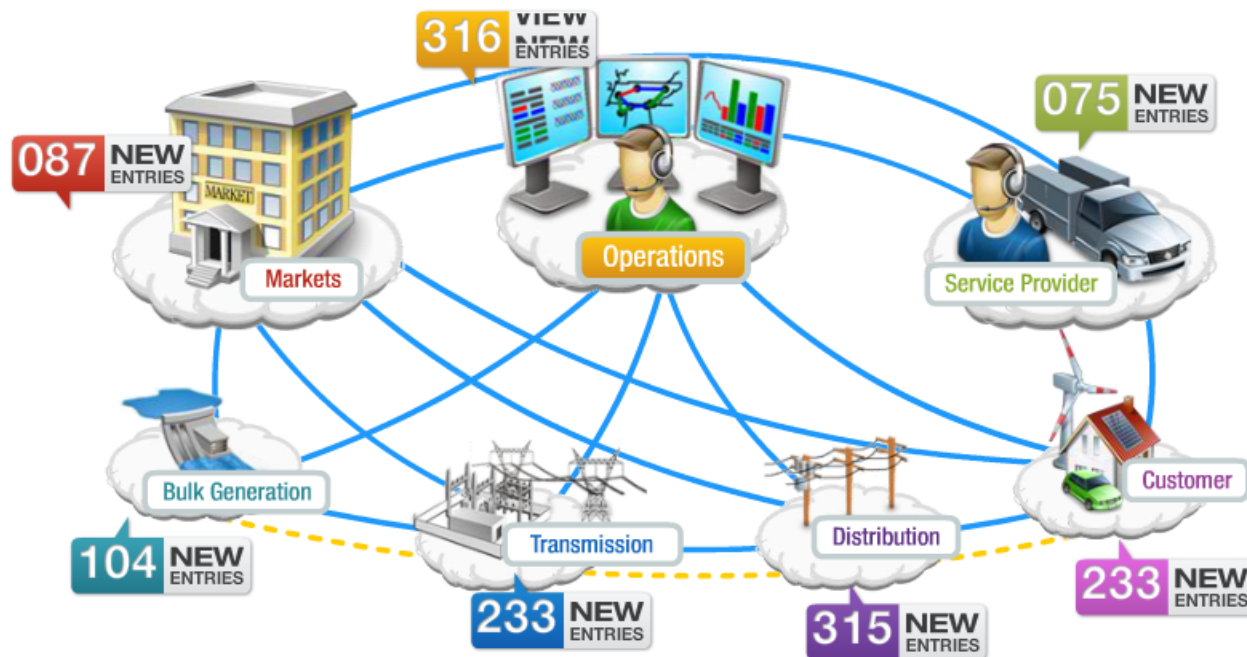
IEEE & Smart Grid	Conferences	Publications	Standards	Societies	Resources
-------------------	-------------	--------------	-----------	-----------	-----------

Search  Smart Grid  [Share this](#) [f](#) [t](#) [You Tube](#) [in](#) [Get Involved in IEEE Smart Grid](#)

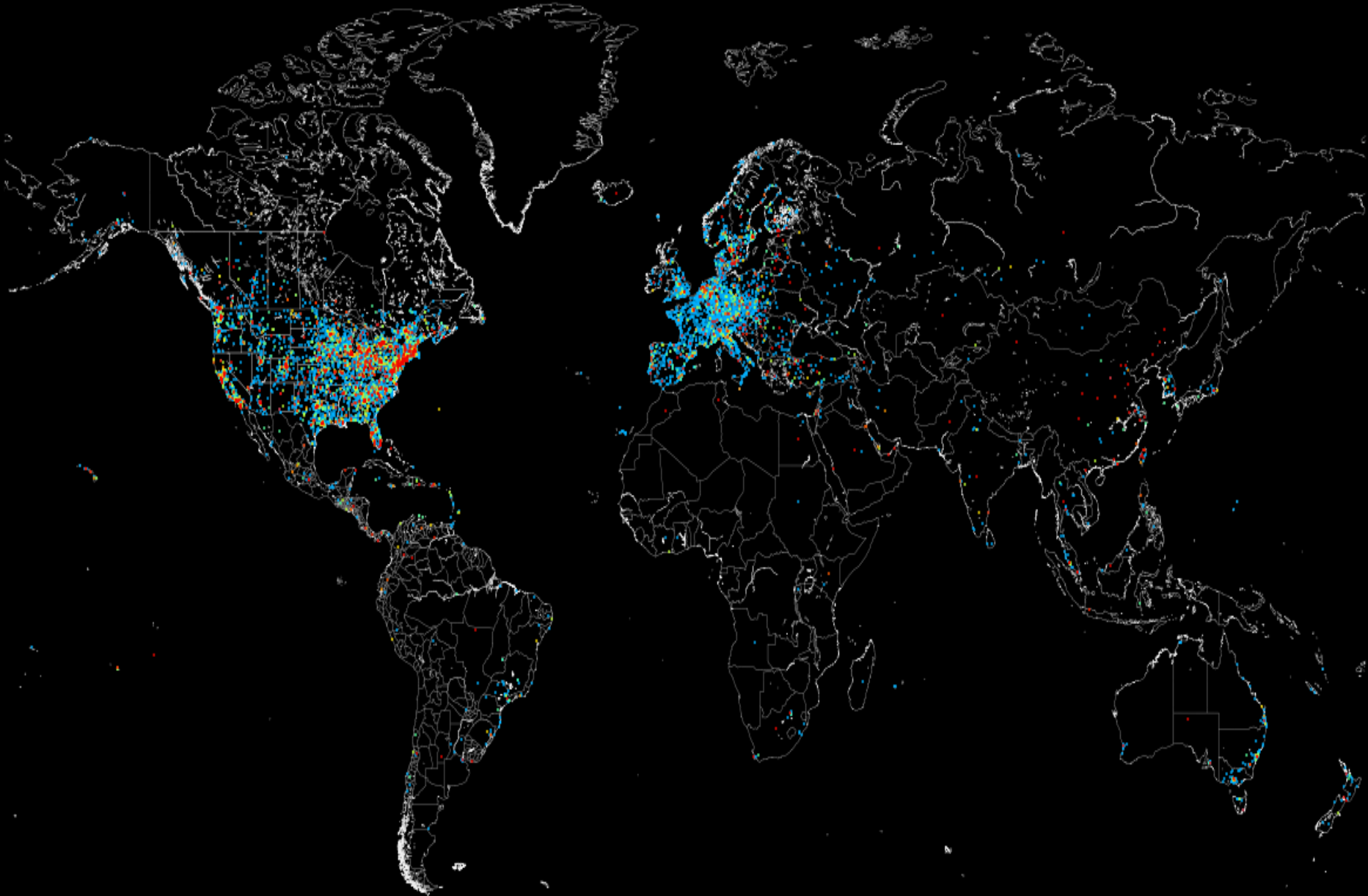
IEEE: The expertise to make **smart grid** a reality

IEEE Smart Grid → Publications → Interactive Search Tool

FILTER BY:



# V: ICS on the Internet







*The IoT is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data*



# Personal things...



Ring





# Home things...





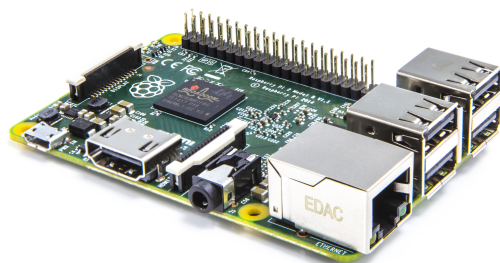


# Medical things (ouch!)





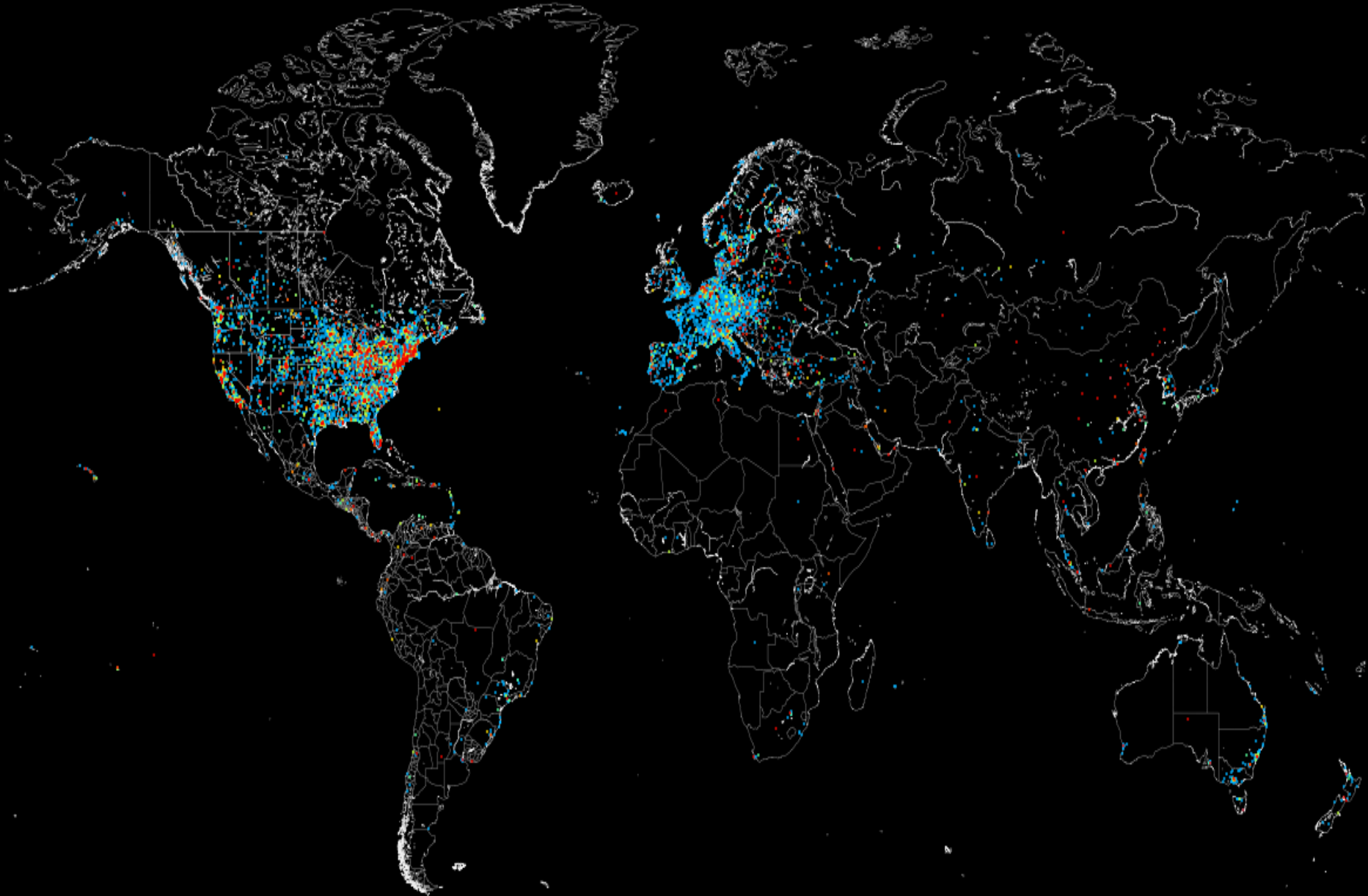
# But also industrial things...!





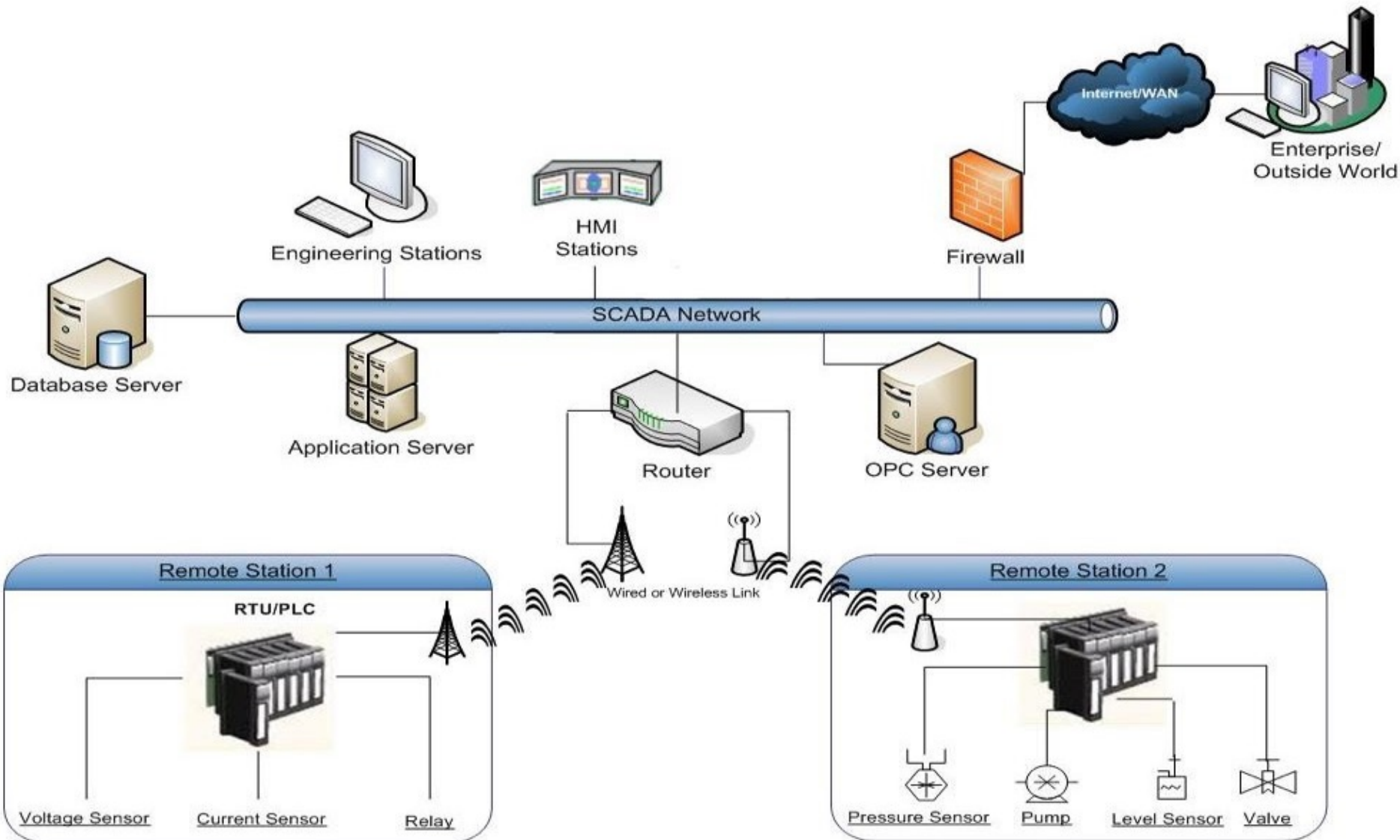
- **Originally-disconnected systems now “opening” to the Internet**
- Critical infrastructure and safety-critical systems
- (sometimes) no humans in the middle
- → Influence environment and humans ( $\neq$  data security!)

# ICS on the Internet





# Typical SCADA ecosystem





## Attacks against ICS share some characteristics

- 2014: Steel mill incident
  - Spear phishing leads to compromise of corporate network
  - Pivot into plant network
  - Exploitation phase (compromise network controllers)
- 23rd December 2015: Ukraine power outage
  - Black energy malware
  - Spear phishing leads to compromise of corporate network
  - BlackEnergy malware steals VPN credentials
  - Pivot into plant networks
  - Exploitation phase (modification of UPS controller firmware)





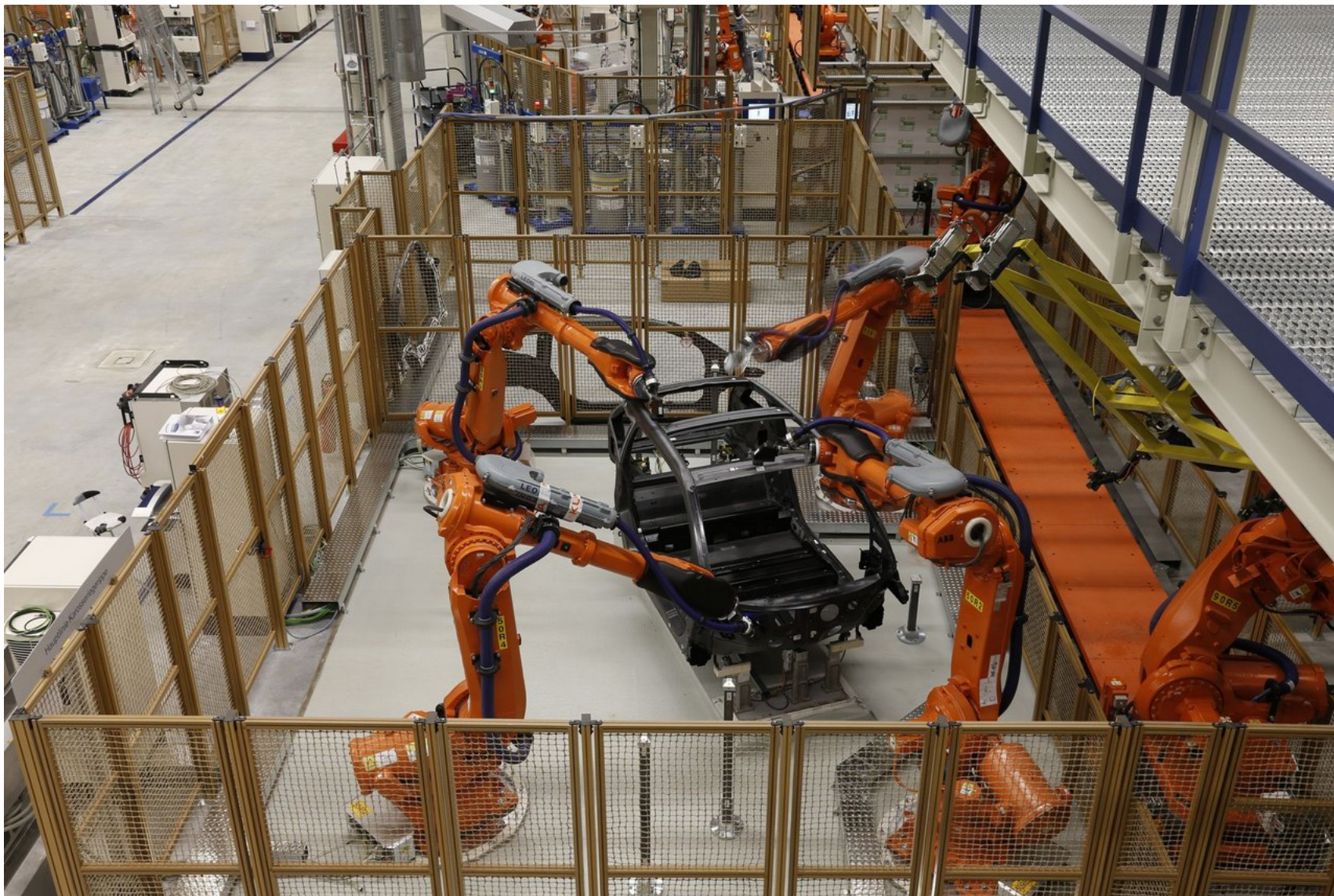
## Example: industrial robots







# From cages...





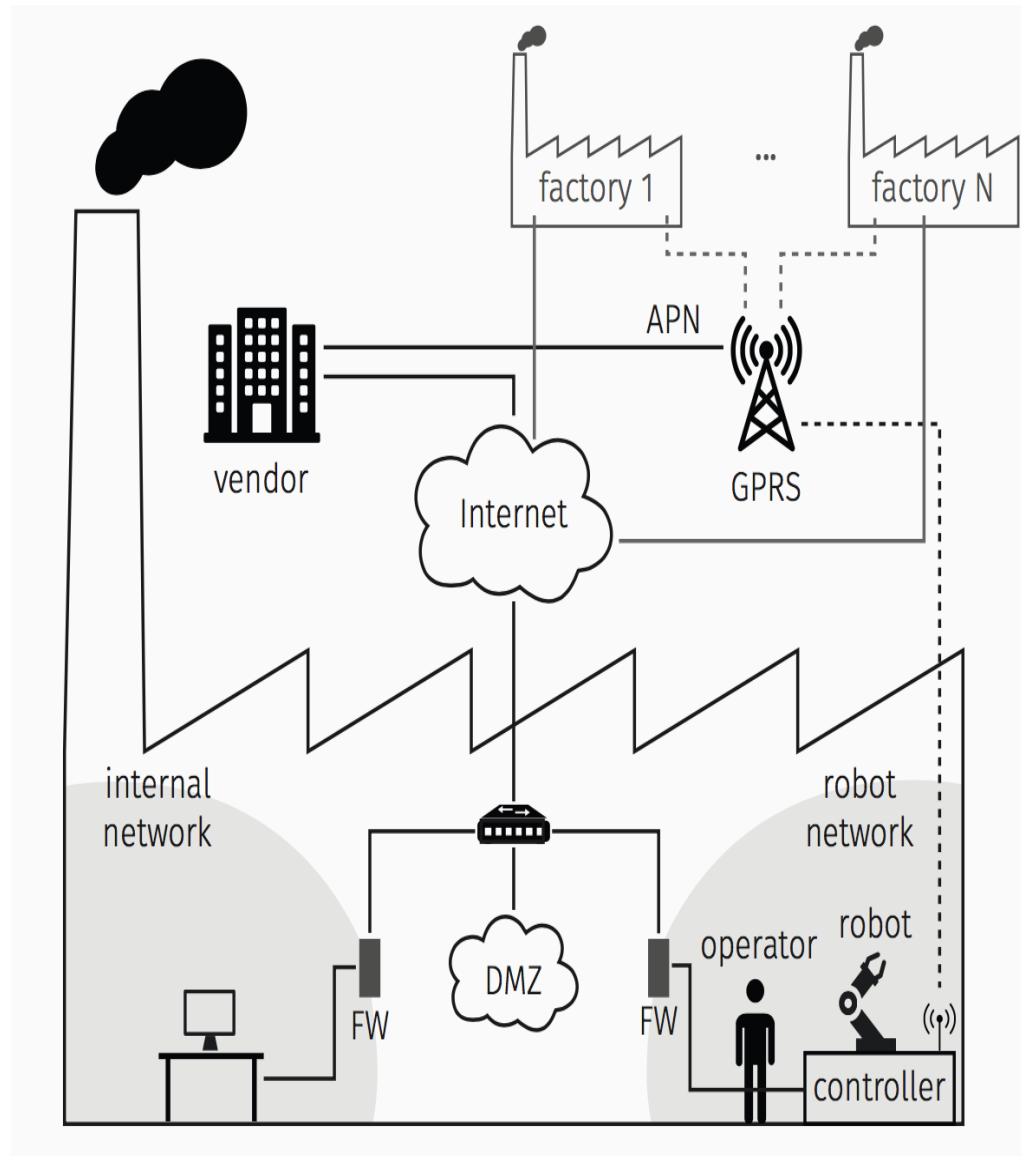


## To cooperation with humans





# Modern factory



## 17.4 Sending PDL2 commands via e-mail

The user is allowed to send PDL2 commands to the C4G Controller Unit, via e-mail. To do that, the required command is to be inserted in the e-mail title with the prefix 'CL' and the same syntax of the strings specified in SYS\_CALL built-in. Example: if the required

.fm

I Functionality

command is ConfigureControllerRestartCold, the user m the e-mail title: 'CL CCRC'.

The authentication is performed by inserting a text which *c4gmp* program (on a PC), in the message body. Such system identifier (\$BOARD\_DATA[1].SYS\_ID), the send the required command, the user login and password; i inserted into the message body, and it will work as an a time and the Controller time (as well as the corrs synchronized, because the message returned by *c4gr* interval of half an hour, more or less, since the generatic

## 17.3 Sending/receiving e-mails on C4G Controller

A PDL2 program called "email" is shown below ("[email](#)" program): it allows to send and receive e-mails on C4G Controller.

[DV4\\_CNTRL Built-In Procedure](#) is to be used to handle such functionalities.



See [DV4\\_CNTRL Built-In Procedure](#) in [Chap. BUILT-IN Routines List](#) section for further information about the e-mail functionality parameters.

### 17.3.1 "email" program

```
PROGRAM email NOHOLD, STACK = 10000
CONST ki_email_cnfg = 20
    ki_email_send = 21
    ki_email_num = 22
    ki_email_recv = 23
    ki_email_del = 24
    ki_email_hdr = 25
    ki_email_footer = 26
```



[Home](#) [Store](#) [Developers](#) [Knowledge Base](#) [Ras Blog](#) [Robopedia](#) [My Account](#) [About](#) [\[ Log In \]](#)

# Robot App Store

BETA

OK, now that you've developed the coolest app for your robot, why not making some money out of it?  
RobotAppStore is the home for every Robot-App™ whether it's for a vacuum cleaner, or the latest humanoid.

[Upload Robot App](#)

\* We're open only for developers for now.



Share: [Tweet](#) 549 [Email](#) 21 [f Share](#) 2 [f Like](#) 1.3K [G+](#) 70

## Twitter Updates

[Follow @RobotAppStore](#) 1,753 followers

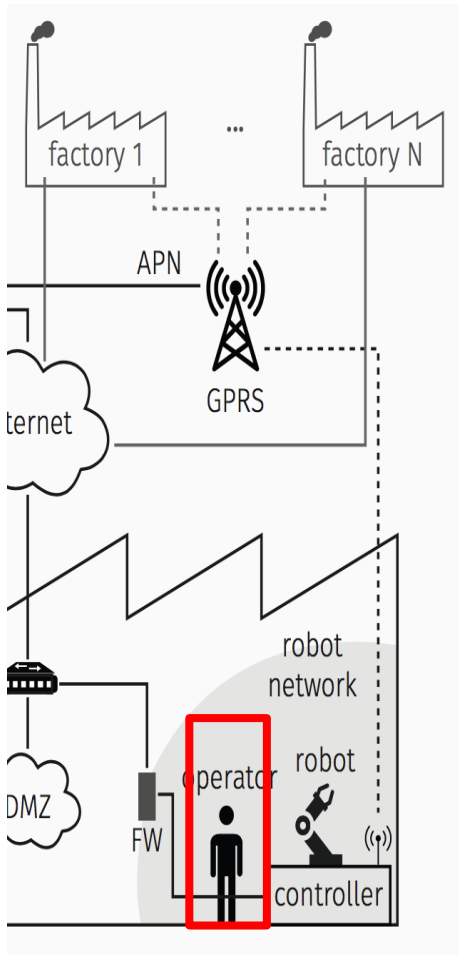
## Developer Stories



Everyone can develop applications for robots. Even the robot NAO!. We encourage developers from all around the world to join us now. Opening an account is free and easy. So [join us](#) now, and start generating revenues from your Apps!



# Factories (and robots) ARE connected



Brand	Overall	Auth. Disabled
eWON	2,800	1,160
Welotec	1	0
Moxa	12,300	2,300
Virtual Access	260	0
Belden	500	0
Westermo	4,000	1,200
NetModule	530	135
Eurotech	0	-
InHand	608	0
Digi	1,200	0
Robustel	2,900	0
Sierra Wireless	0	0





- 1) Production Plant Halting (“up to 20,000\$/min”)
  - 2) Production Outcome Alteration
  - 3) Physical Damage
  - 4) Unauthorized Access
- And, of course, there is the ransomware scheme, but that’s not too interesting in the era of “oh, I could ransom that, too!”





# Sometimes, even untargeted attacks...

Articolo »

Cronaca 10 maggio 2019 Casale Monferrato

Nella notte tra martedì e mercoledì

## Attacco informatico alla EPTA (IARP)

*L'azienda: "Dopo gli opportuni test le normali attività riprenderanno gradualmente a partire da lunedì mattina."*



di Massimiliano Francia

**Aggiornamento sabato 11 maggio ore 19,30** – Sono stati ripristinati nel corso del pomeriggio di oggi, venerdì alcuni servizi aziendali, tra cui l'accesso al sito aziendale che nel primo pomeriggio risultava oscurato ed è tornato accessibile. Dall'ufficio stampa dell'azienda, verso le 18,30, hanno fatto sapere che alcune attività sono state riprese e che comunque non tutto il gruppo – è stato bloccato dall'attacco hacker. Il ritorno alla normalità, insomma sembra essere iniziato e l'auspicio è che la produzione possa riprendere a pieno ritmo al più presto.



# Renault sta riprendendo la produzione dopo un attacco informatico globale

Renault annuncia, dopo la sospensione della produzione da 5 suoi stabilimenti per gli attacchi informatici di venerdì, che tutto sta tornando alla normalità

di [Andrea Senatore](#), pubblicato il 15 Maggio 2017 alle ore 19:47



Il gruppo transalpino **Renault** e la partner nipponica **Nissan** hanno dichiarato questo lunedì che le cose stanno tornando alla normalità in quasi tutti i propri impianti, dopo un attacco informatico globale che ha causato danni estesi e la sospensione della produzione in diversi stabilimenti. Renault e il suo partner giapponese sono le uniche case automobilistiche più importanti che finora hanno segnalato problemi di produzione derivanti da **WannaCry ransomware**, l'attacco sul web senza fine che da venerdì si è diffuso in più di **150 paesi**.

GUIDA: **Renault**

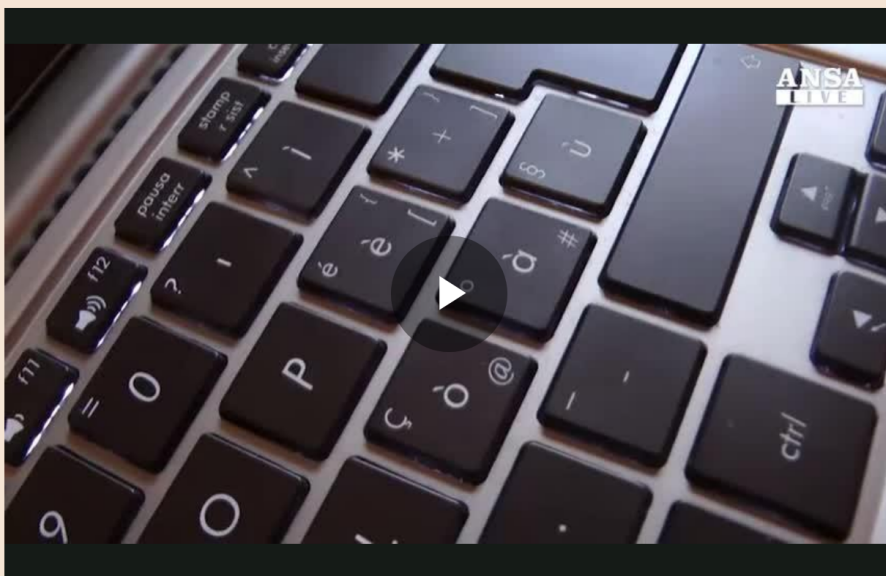
01. [Audi, Renault e Volvo: novità importanti dal mondo dei motori](#)
02. [Skoda Vision E Concept: ecco come sarà interno ed esterno del veicolo](#)
03. [Volkswagen mantiene lontane PSA e Renault, risultati stupefacenti nel primo trimestre 2017](#)
04. [Renault e Nissan: collaborazione importante per il futuro dell'auto](#)
05. [Renault sta riprendendo la produzione dopo un attacco informatico globale](#)
06. [Renault Nissan prevede di superare Volkswagen e Toyota entro fine 2017](#)



# Sometimes, even untargeted attacks...

## Cyberattacco contro Norsk Hydro, alluminio ai massimi da 3 mesi

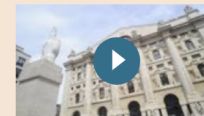
—di Sissi Bellomo | 20 marzo 2019



**N**uovo scossone sul mercato dell'alluminio, questa volta a causa del cybercrime. La norvegese **Norsk Hydro**, gigante mondiale attivo in tutta la filiera del metallo, ha rivelato di aver subito un «grave» attacco informatico che l'ha costretta a sospendere la produzione in diversi impianti e a farne funzionare altri in modalità manuale.

Gli hacker sono riusciti a violare i sistemi di sicurezza lunedì sera, presumibilmente negli Stati Uniti, per poi infettare quasi tutta la rete di

### VIDEO



15 maggio 2019

Nelle sale operative di Mts, dove si forma lo spread

### I PIÙ LETTI DI FINANZA & MERCATI

1. **SERVONO 64 MILIARDI IN DUE MESI** | 19 maggio 2019  
Titoli di Stato, le tre ragioni che possono fare salire la tensione
2. **IL MERCATO** | 19 maggio 2019  
Il mito del debito giapponese: perché non regge il confronto con Tokyo
3. **TRADING DALLO SPAZIO PROFONDO** | 18 maggio 2019  
Profitti stellari: in Borsa con le foto dal satellite guadagni fino al 5% in più
4. **FINANZA** | 19 maggio 2019  
Benetton, cambia l'ad della holding: via Patuano
5. **LA GIORNATA DEI MERCATI** | 17 maggio 2019  
Settimana positiva per Piazza Affari nonostante caro-spread, corre la Juve

### ULTIME NOVITÀ

Dal catalogo del Sole 24 Ore



- 1.Username Enumeration (really?)
- 2.Weak Passwords (you can't be serious)
- 3.Account Lockout (didn't we figure out this in 1970?)
- 4.Unencrypted Services (Snowden, anyone?!)
- 5.Two-factor Authentication (even my bank can do this)
- 6.Poorly Implemented Encryption (so, if it's not in clear, it's weak...)
- 7.Update Sent Without Encryption (...)
- 8.Update Location Writable (yup, why not executing random code?)
- 9.Denial of Service (on your oven, to burn your cake)
- 10.Removal of Storage Media (you can't make this stuff up)
- 11.No Manual Update Mechanism (fine, it's probably autom...)
- 12.Missing Update Mechanism (... or maybe not)
- 13.Firmware Version Display and/or Last Update Date (but in any case you don't even know)

- 1.Username Enumeration (really?)**
- 2.Weak Passwords (you can't be serious)**
- 3.Account Lockout (didn't we figure out this in 1970?)
- 4.Unencrypted Services (Snowden, anyone?!)**
- 5.Two-factor Authentication (even my bank can do this)**
- 6.Poorly Implemented Encryption (so, if it's not in clear, it's weak...)**
- 7.Update Sent Without Encryption (...)**
- 8.Update Location Writable (yup, why not executing random code?)**
- 9.Denial of Service (on your oven, to burn your cake)**
- 10.Removal of Storage Media (you can't make this stuff up)
- 11.No Manual Update Mechanism (fine, it's probably autom...)
- 12.Missing Update Mechanism (... or maybe not)
- 13.Firmware Version Display and/or Last Update Date (but in any case you don't even know)**





- The usual vulnerabilities (buffer overflows, command injection)
- “Outdated” coding practices
- Hardcoded credentials (and no real account lockout in place)
- No encryption (or, worse, placebo cryptography)
- Software and updates not signed
- No hardening: no privilege separation, nothing
- No physical security (physical access == full compromise)
- Read the full research report at <http://robosec.org>



- Information disclosure (way too verbose banners, detailed technical material)
- Outdated everything (kernel, compilers, libraries, ...)
- Weak \ known \ static credentials
- Poor or misconfigured transport encryption (e.g., VPN with static auth keys, pre-generated certs, ...)
- Insecure web interface (no input sanitization... and even security critical code copied straight from blog posts!)
- **No better than consumer IoT devices!**
- Read the full research report at <http://robosec.org>



# Questions?

- Thank you for your attention!
- You can reach me at [stefano.zanero@polimi.it](mailto:stefano.zanero@polimi.it)
- Or just tweet @raistolo

