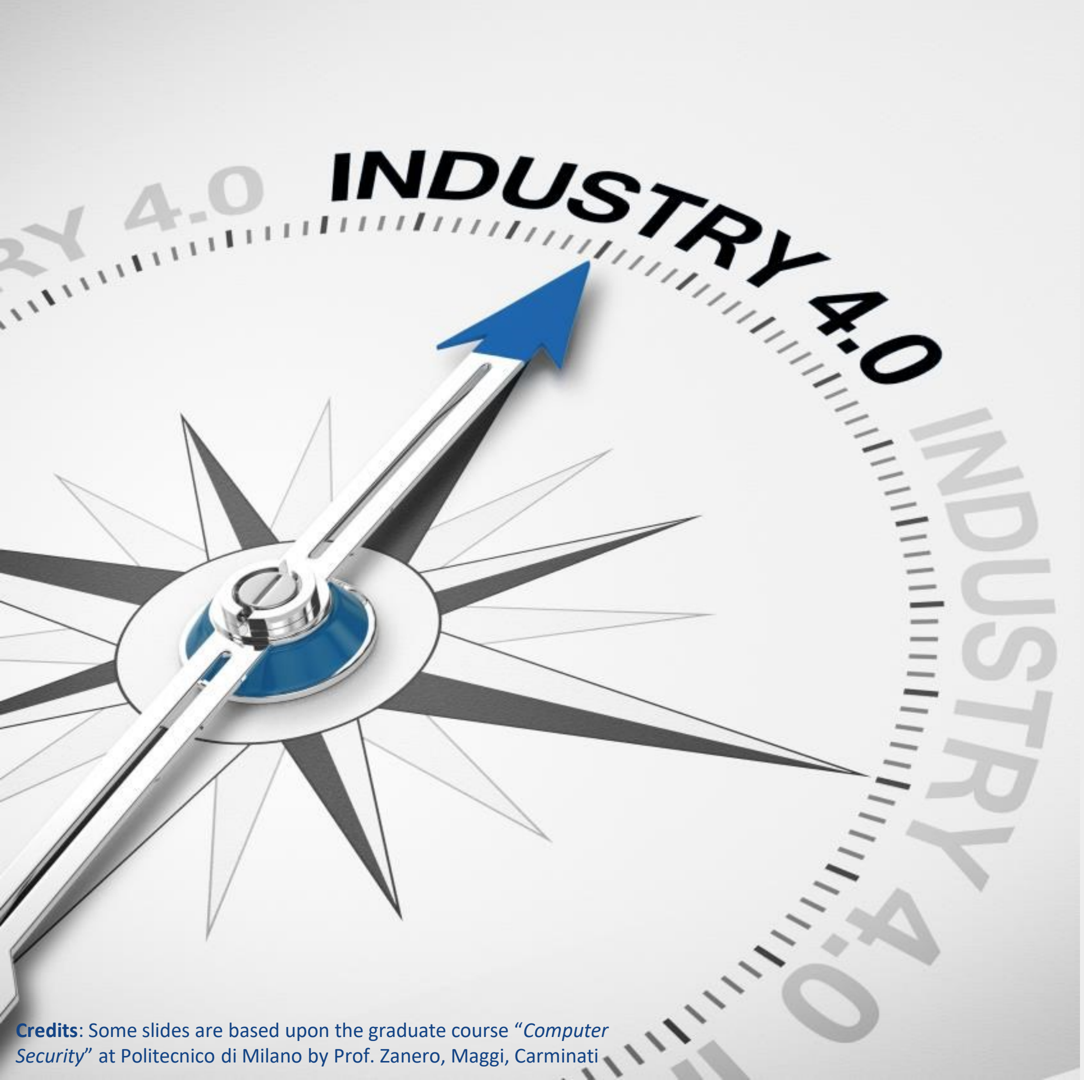


THE ‘C’ IN ‘INDUSTRY 4.0’ STANDS FOR CYBERSECURITY

June 17th, 2020

Marcello Pogliani, Ph.D.

Research Collaborator, **Politecnico di Milano**
Security Engineer, **Secure Network Srl**

marcello.pogliani@polimi.it

Organizzato da

Credits: Some slides are based upon the graduate course “*Computer Security*” at Politecnico di Milano by Prof. Zanero, Maggi, Carminati

INDUSTRY 4.0

Fourth Industrial Revolution (Industry 4.0)
Smart Manufacturing
(IIoT)

Digitalization
Connectivity

WHAT IS (CYBER)SECURITY

- **Protection** of information, processes and assets from **threats**
- **Basic Requirements** (about data)

Confidentiality

Integrity

Availability

TERMINOLOGY

- How does a **threat actor** violate a system’s **C**, **I**, **A** requirements (**attack**)?
  - By **exploiting** one or more **vulnerabilities**

- **Vulnerability**: “error” that *makes it possible* for a threat actor to violate the C, I, A properties
- **Exploit**: a specific way to use one or more vulnerabilities to accomplish a specific goal
- **Attack**: an intentional use of one or more exploits to violate C, I, A

TERMINOLOGY

- **There's no secure system** (in absolute terms)
- Security is about risk management

Risk = assets x threats x vulnerabilities

- Security = balance [reduction of vulns + damage containment] vs. **cost**

ASSETS IN A MANUFACTURING SYSTEMS

Safety

People
Environment
Equipment

Production Continuity

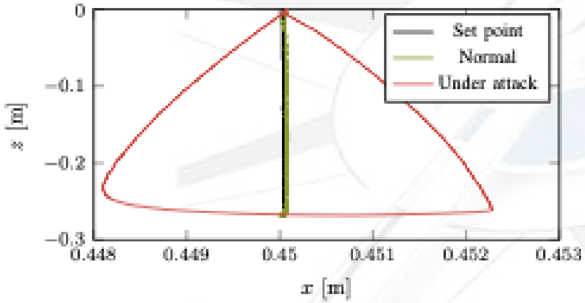
Production Plant
Halting
Ransomware

Production Outcome

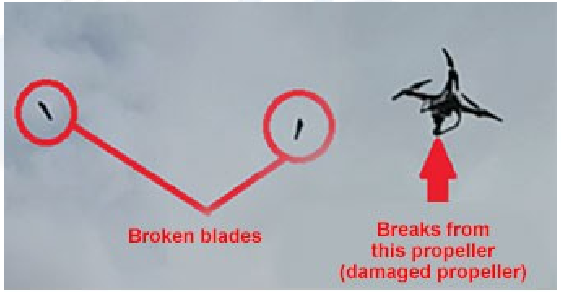
$$$
Indirect safety effects...

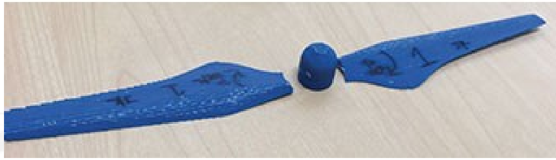
Intellectual Property (Confidentiality)

THREATS: CYBERPHYSICAL ATTACKS



Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, and Stefano Zanero. ***An Experimental Security Analysis of an Industrial Robot Controller***. 38th IEEE Symposium on Security and Privacy, San José, CA, June 2017.





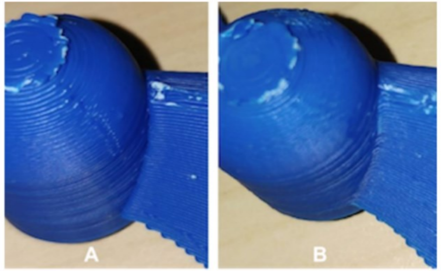
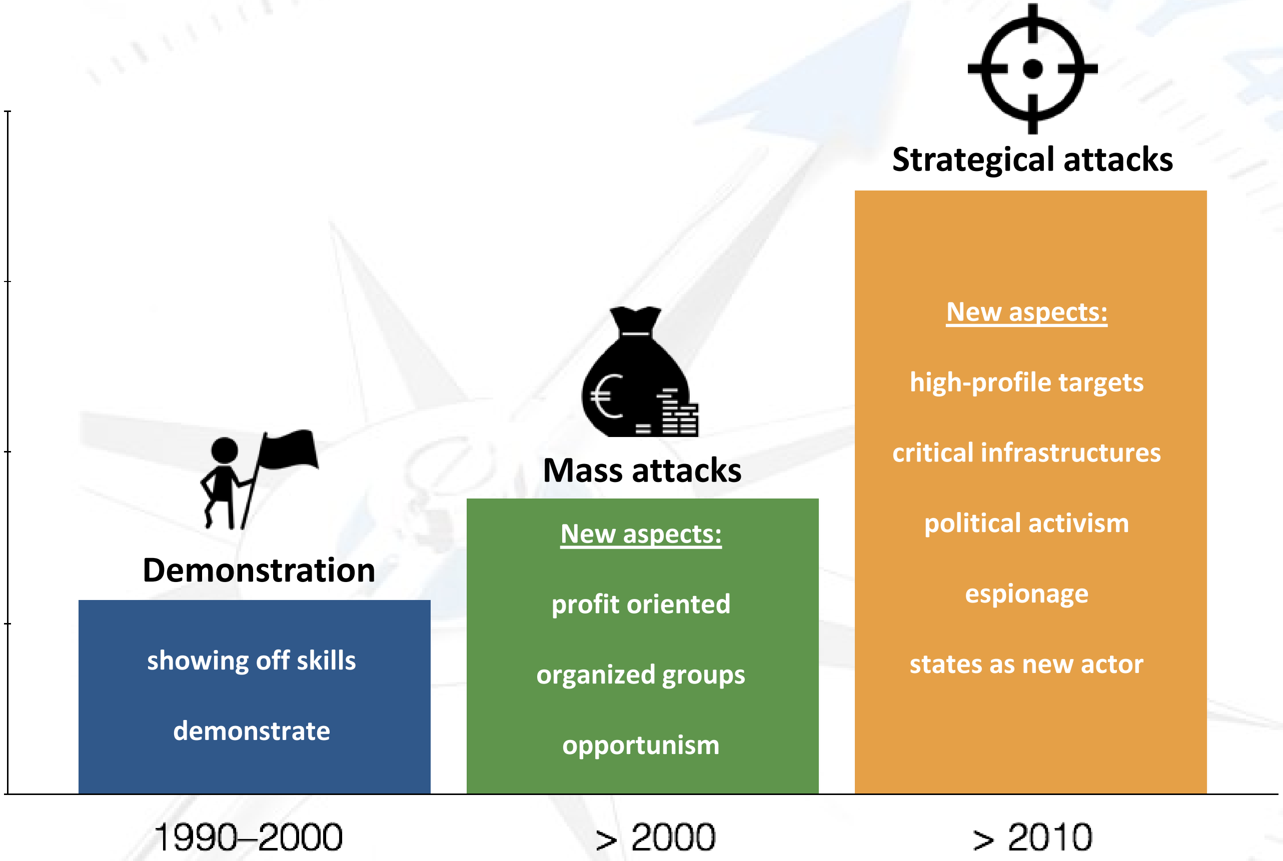


Figure 12. Two printed caps site-by-site. Cap A is *sabotaged* and Cap B is *benign*

S. Belikovetsky et al., **dr0wned-cyber-physical attack with additive manufacturing**, *WOOT 2017*

MALWARE (AND ITS EVOLUTION)



Demonstration

showing off skills

demonstrate

1990–2000

Mass attacks

New aspects:

profit oriented

organized groups

opportunism

> 2000

Strategical attacks

New aspects:

high-profile targets

critical infrastructures

political activism

espionage

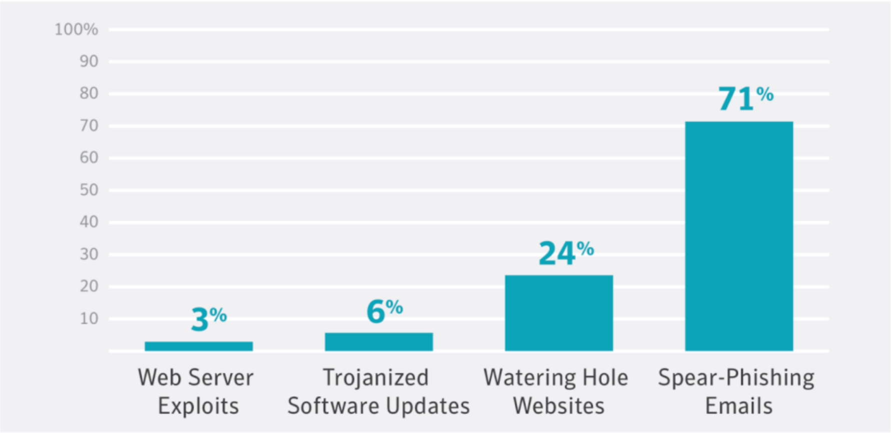
states as new actor

> 2010

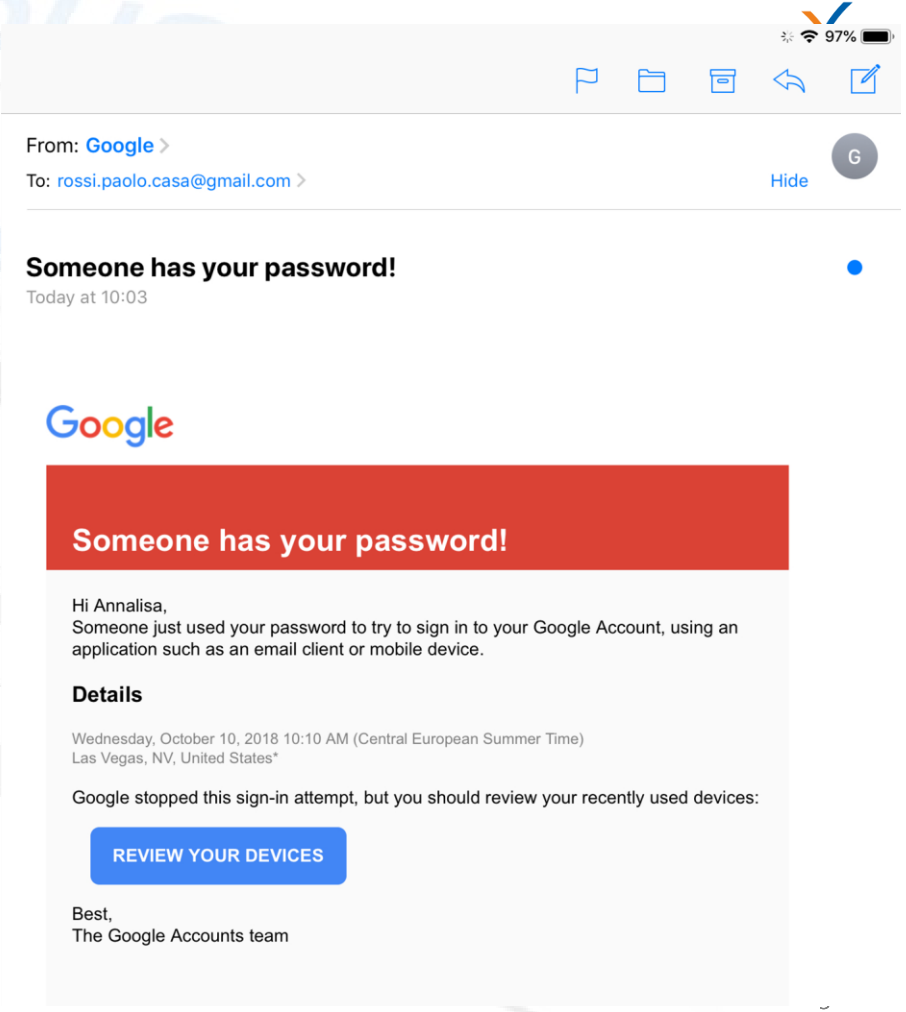
(SPEAR)PHISHING

Targeted attack infection vectors

Known infection vectors used by targeted attack groups. Spear phishing is by far the most popular.



2018 Symantec Internet Security Threat Report



From: Google
To: rossi.paolo.casa@gmail.com

Someone has your password!
Today at 10:03

Google

Someone has your password!

Hi Annalisa,
Someone just used your password to try to sign in to your Google Account, using an application such as an email client or mobile device.

Details

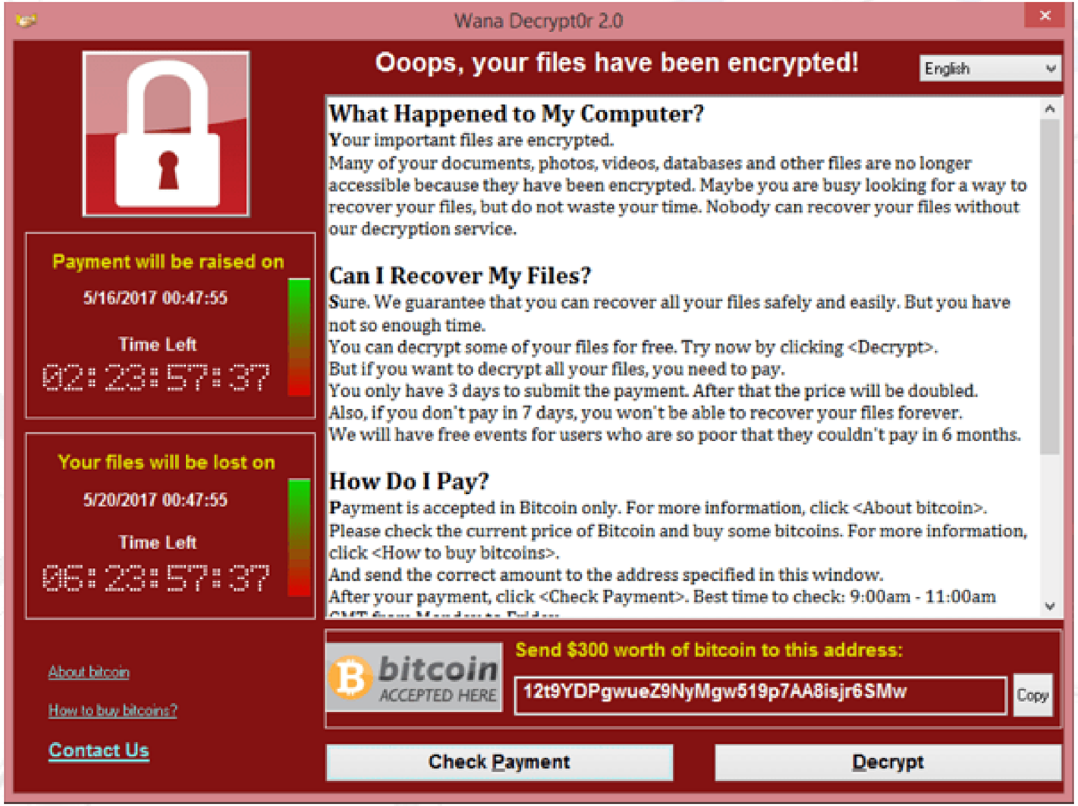
Wednesday, October 10, 2018 10:10 AM (Central European Summer Time)
Las Vegas, NV, United States*

Google stopped this sign-in attempt, but you should review your recently used devices:

REVIEW YOUR DEVICES

Best,
The Google Accounts team

RANSOMWARE (MASS ATTACKS)



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

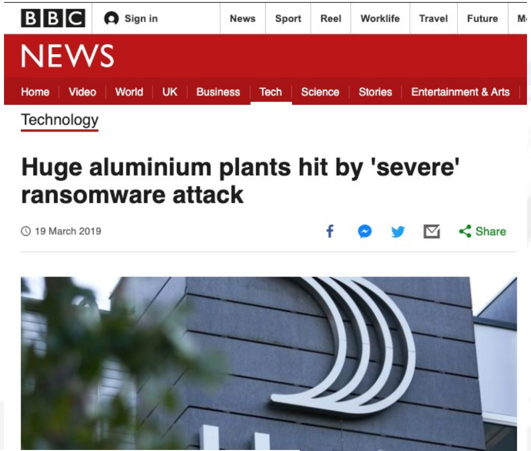
How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

RANSOMWARE (MASS ATTACKS)



Technology

Huge aluminium plants hit by 'severe' ransomware attack

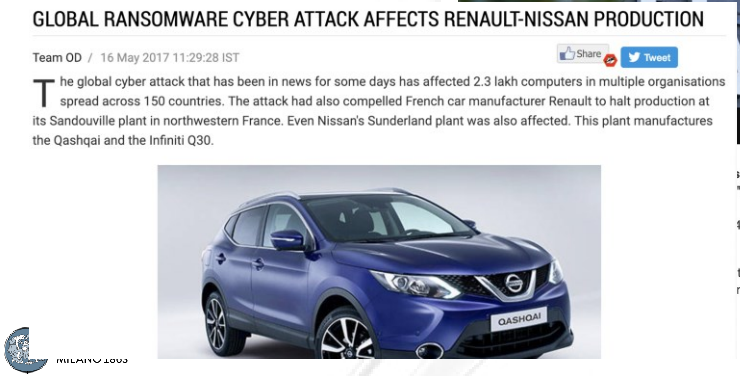
19 March 2019

GETTY IMAGES

s has switched to manual
"severe" ransomware attack.

40 countries, says the attack

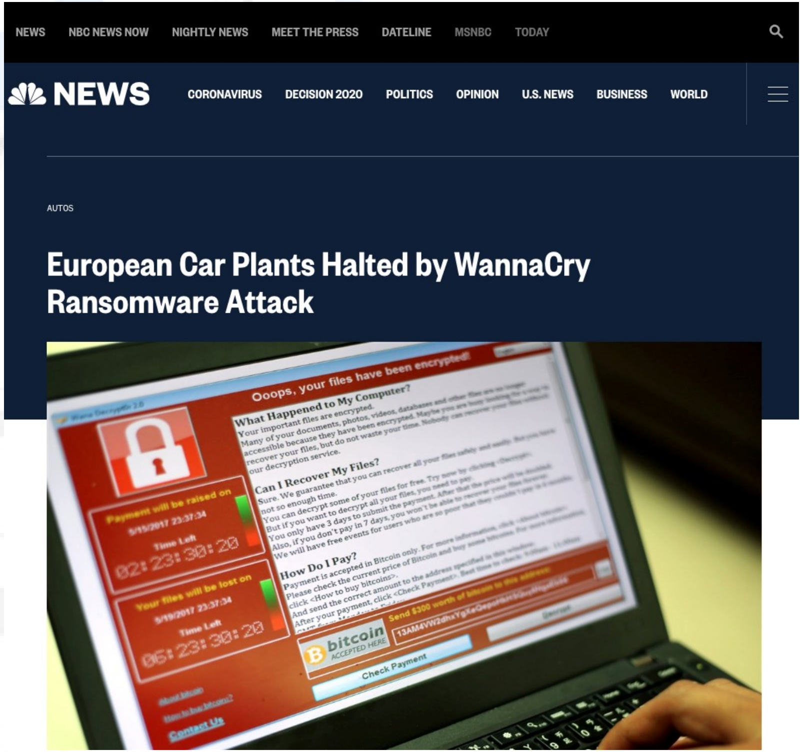
to halt production though other
normally.



GLOBAL RANSOMWARE CYBER ATTACK AFFECTS RENAULT-NISSAN PRODUCTION

Team OD / 16 May 2017 11:29:28 IST

The global cyber attack that has been in news for some days has affected 2.3 lakh computers in multiple organisations spread across 150 countries. The attack had also compelled French car manufacturer Renault to halt production at its Sandouville plant in northwestern France. Even Nissan's Sunderland plant was also affected. This plant manufactures the Qashqai and the Infiniti Q30.



AUTOS

European Car Plants Halted by WannaCry Ransomware Attack

TARGETED AND STRATEGICAL ATTACKS

2010
Stuxnet

2011
Duqu

2012
Flamer

2014
German
Mill Factory

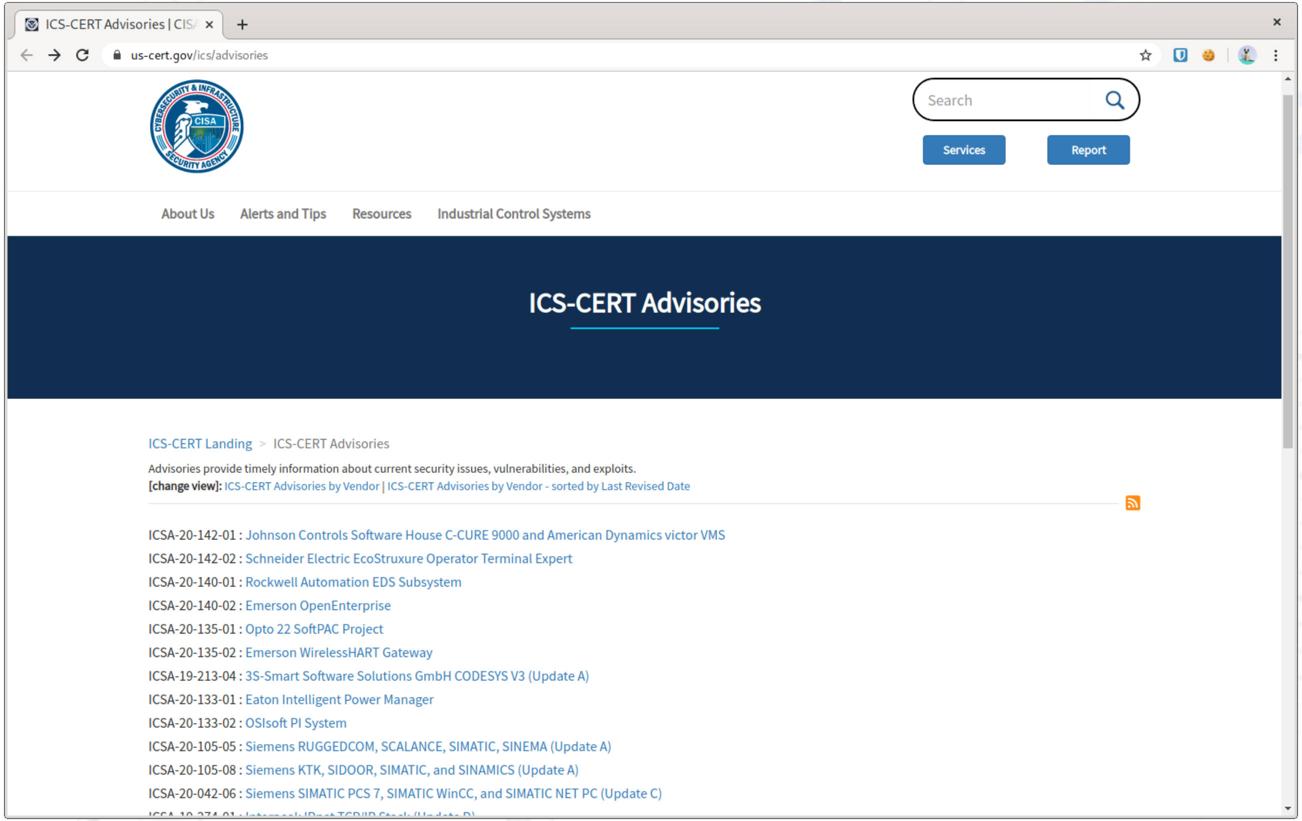
2015
Ukrainian
Power grid

2017
Triton

High profile (i.e., state) actors: reverse engineer proprietary protocols, bypass air-gaps, …

Stuxnet and Triton don’t focus on manufacturing (but… plenty of high-profile manufacturing plants)

VULNERABILITIES


ICS-CERT Advisories | CIS/
us-cert.gov/ics/advisories
Search
Services
Report
About Us
Alerts and Tips
Resources
Industrial Control Systems

ICS-CERT Advisories

ICS-CERT Landing > ICS-CERT Advisories

Advisories provide timely information about current security issues, vulnerabilities, and exploits.
[change view]: ICS-CERT Advisories by Vendor | ICS-CERT Advisories by Vendor - sorted by Last Revised Date

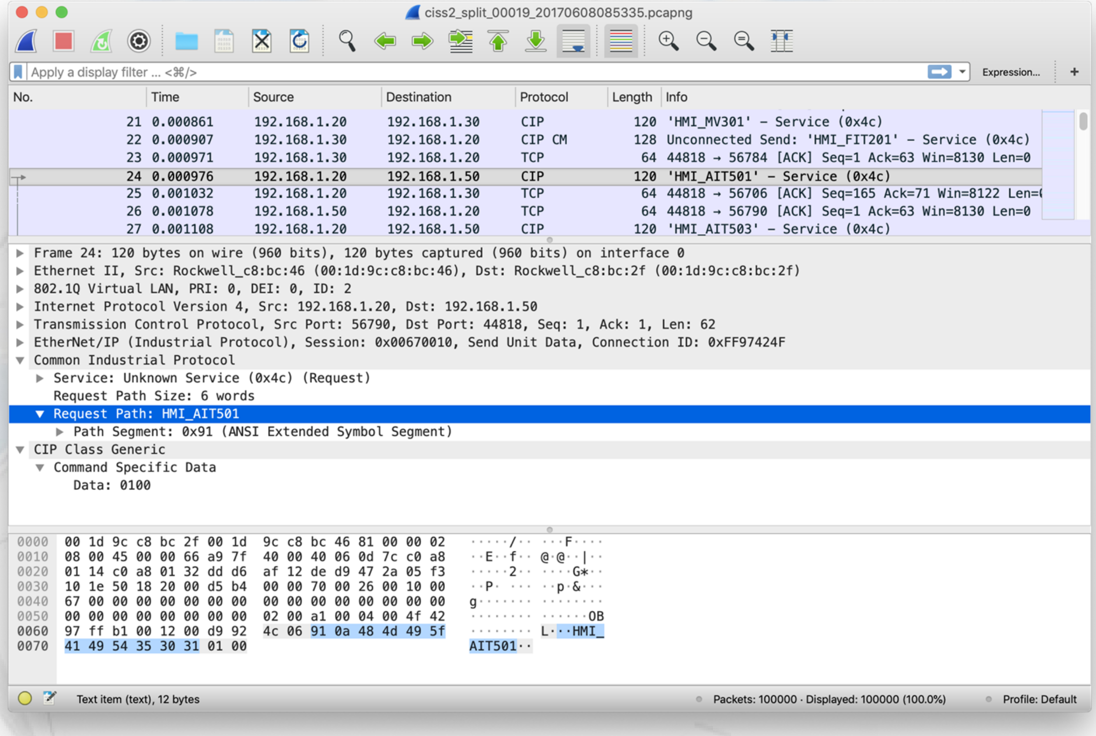
ICSA-20-142-01 : Johnson Controls Software House C-CURE 9000 and American Dynamics victor VMS
ICSA-20-142-02 : Schneider Electric EcoStruxure Operator Terminal Expert
ICSA-20-140-01 : Rockwell Automation EDS Subsystem
ICSA-20-140-02 : Emerson OpenEnterprise
ICSA-20-135-01 : Opto 22 SoftPAC Project
ICSA-20-135-02 : Emerson WirelessHART Gateway
ICSA-19-213-04 : 3S-Smart Software Solutions GmbH CODESYS V3 (Update A)
ICSA-20-133-01 : Eaton Intelligent Power Manager
ICSA-20-133-02 : OSIsoft PI System
ICSA-20-105-05 : Siemens RUGGEDCOM, SCALANCE, SIMATIC, SINEMA (Update A)
ICSA-20-105-08 : Siemens KTK, SIDOOR, SIMATIC, and SINAMICS (Update A)
ICSA-20-042-06 : Siemens SIMATIC PCS 7, SIMATIC WinCC, and SIMATIC NET PC (Update C)
ICSA-19-274-01 : Interpeak IPnet TCP/IP Stack (Update D)

VULNERABILITIES (AND THEIR IMPACT): IT vs OT

- Originally **disconnected** systems
  - Security as an afterthought
- **Production-critical** systems
  - Difficult to **update**
  - Long **service life** (decades - forever days)
  - Not managed by **corporate IT**
- Often, **safety-critical** systems
  - Influence the environment
  - Live security testing is, er…, difficult!

INDUSTRIAL PROTOCOLS

- No authentication
- No encryption
- Things are (slowly) changing
  - CIP security
  - Since 2018 (Allen Bradley)



ciss2_split_00019_20170608085335.pcapng

```
No.      Time      Source        Destination   Protocol  Length Info
      21 0.000861  192.168.1.20  192.168.1.30  CIP          120 'HMI_MV301' – Service (0x4c)
      22 0.000907  192.168.1.30  192.168.1.20  CIP CM       128 Unconnected Send: 'HMI_FIT201' – Service (0x4c)
      23 0.000971  192.168.1.30  192.168.1.20  TCP           64 44818 → 56784 [ACK] Seq=1 Ack=63 Win=8130 Len=0
      24 0.000976  192.168.1.20  192.168.1.50  CIP          120 'HMI_AIT501' – Service (0x4c)
      25 0.001032  192.168.1.20  192.168.1.30  TCP           64 44818 → 56706 [ACK] Seq=165 Ack=71 Win=8122 Len=(
      26 0.001078  192.168.1.50  192.168.1.20  TCP           64 44818 → 56790 [ACK] Seq=1 Ack=63 Win=8130 Len=0
      27 0.001108  192.168.1.20  192.168.1.50  CIP          120 'HMI_AIT503' – Service (0x4c)
```

```
▶ Frame 24: 120 bytes on wire (960 bits), 120 bytes captured (960 bits) on interface 0
▶ Ethernet II, Src: Rockwell_c8:bc:46 (00:1d:9c:c8:bc:46), Dst: Rockwell_c8:bc:2f (00:1d:9c:c8:bc:2f)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2
▶ Internet Protocol Version 4, Src: 192.168.1.20, Dst: 192.168.1.50
▶ Transmission Control Protocol, Src Port: 56790, Dst Port: 44818, Seq: 1, Ack: 1, Len: 62
▶ EtherNet/IP (Industrial Protocol), Session: 0x00670010, Send Unit Data, Connection ID: 0xFF97424F
▼ Common Industrial Protocol
  ▶ Service: Unknown Service (0x4c) (Request)
    Request Path Size: 6 words
  ▼ Request Path: HMI_AIT501
    ▶ Path Segment: 0x91 (ANSI Extended Symbol Segment)
▼ CIP Class Generic
  ▼ Command Specific Data
      Data: 0100
```

```
0000  00 1d 9c c8 bc 2f 00 1d  9c c8 bc 46 81 00 00 02   ·····/·· ···F····
0010  08 00 45 00 00 66 a9 7f  40 00 40 06 0d 7c c0 a8   ··E··f·· @·@··|··
0020  01 14 c0 a8 01 32 dd d6  af 12 de d9 47 2a 05 f3   ·····2·· ····G*··
0030  10 1e 50 18 20 00 d5 b4  00 00 70 00 26 00 10 00   ··P· ··· ··p·&···
0040  67 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   g······· ········
0050  00 00 00 00 00 00 00 00  02 00 a1 00 04 00 4f 42   ········ ······OB
0060  97 ff b1 00 12 00 d9 92  4c 06 91 0a 48 4d 49 5f   ········ L···HMI_
0070  41 49 54 35 30 31 01 00                            AIT501··
```

Text item (text), 12 bytes

Packets: 100000 · Displayed: 100000 (100.0%)

Profile: Default

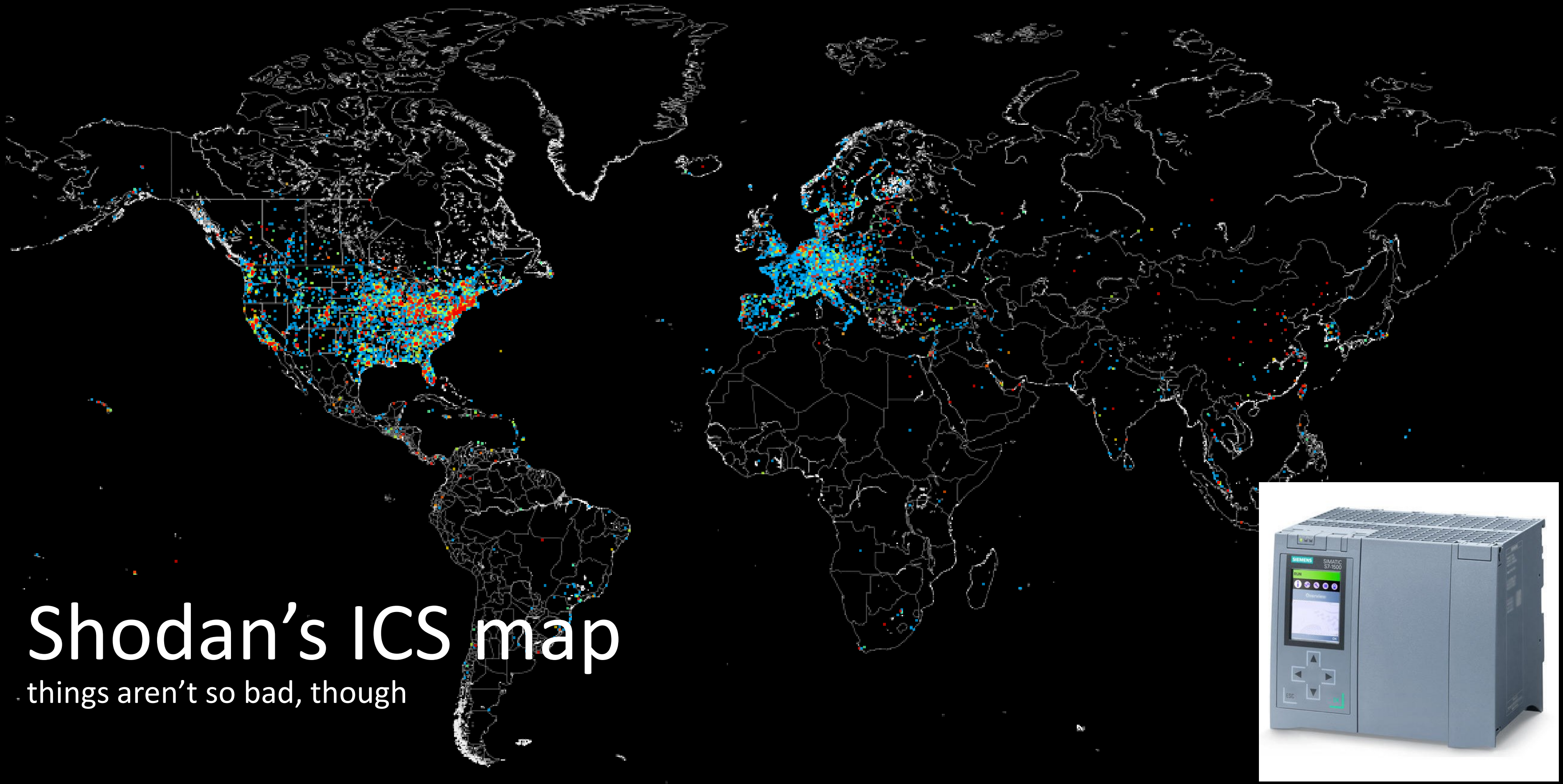
ATTACK SURFACE: WAIT, ISN'T THERE AN AIRGAP?

What Reviewer 4 thinks (and they aren't alone):

"The threat model seems too strong in practice. All attacks are possible for the attacker within the same network. Many ICSs on the other hand are located within air-gapped network."

…WRONG!

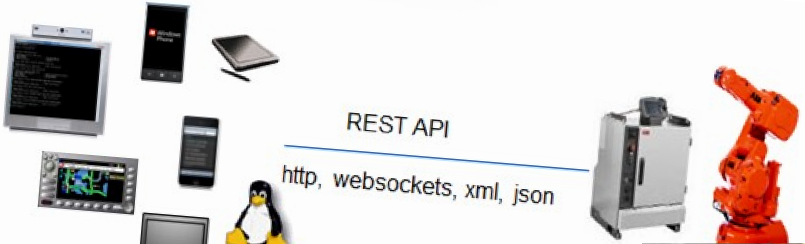
SHODAN



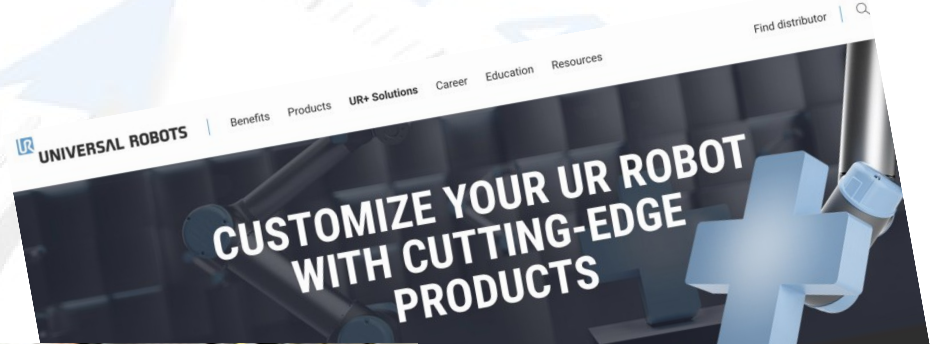
Shodan's ICS map

things aren't so bad, though

ROBOTICS: AN INTERCONNECTED ECOSYSTEM



source: http://developercenter.robotstudio.com



CUSTOMIZE YOUR UR ROBOT WITH CUTTING-EDGE PRODUCTS

ts+ Certified

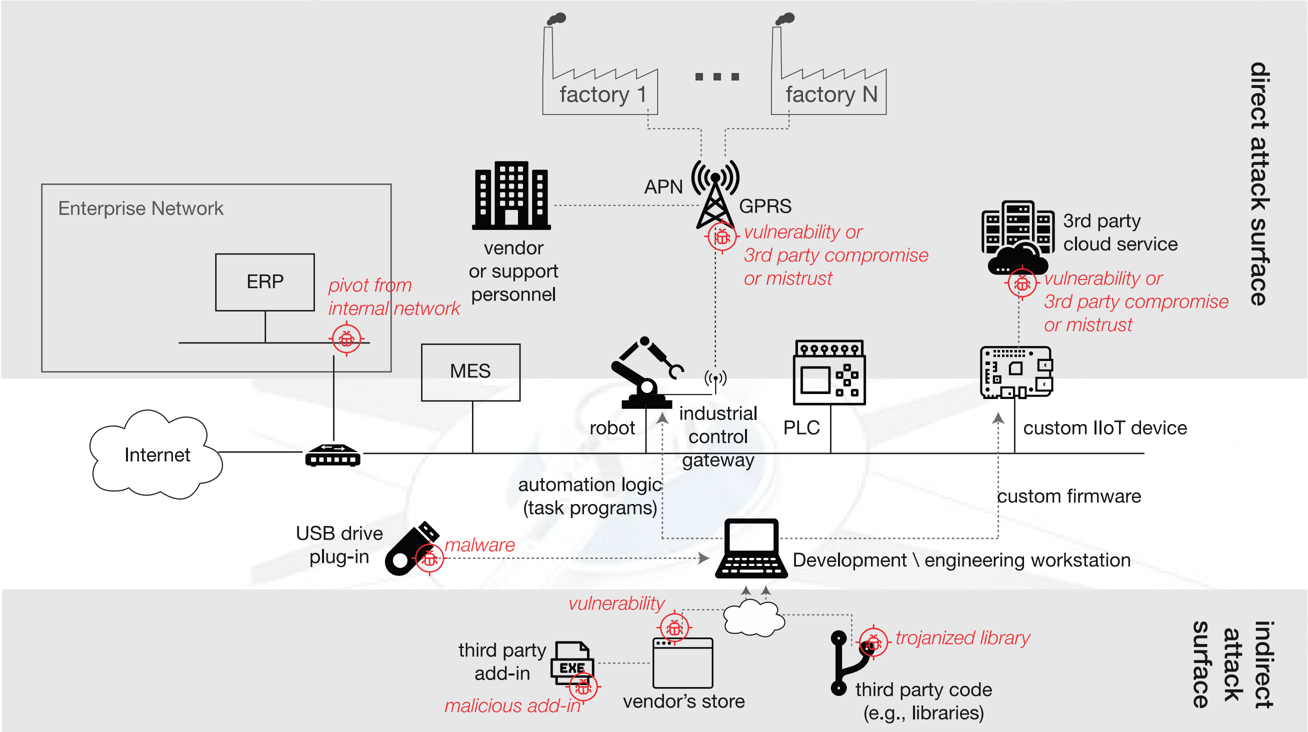
One-stop solutions

Direct support from developers

source: https://universal-robots.com/plus

source: abb.com

MANUFACTURING SYSTEM – ATTACK SURFACE


factory 1
...
factory N
direct attack surface
APN
GPRS
vulnerability or 3rd party compromise or mistrust
vendor or support personnel
3rd party cloud service
vulnerability or 3rd party compromise or mistrust
Enterprise Network
ERP
pivot from internal network
MES
robot
industrial control gateway
PLC
custom IIoT device
Internet
automation logic (task programs)
custom firmware
USB drive plug-in
malware
Development \ engineering workstation
vulnerability
trojanized library
third party add-in
EXE
malicious add-in
vendor's store
third party code (e.g., libraries)
indirect attack surface

Brand	Exposed Devices	No Authentication
Belden	956	
Eurotech	160	
eWON	6,219	1,160
Digi	1,200	
InHand	883	
Moxa	12,222	2,300
NetModule	886	135
Robustel	4,491	
Sierra Wireless	50,341	220
Virtual Access	209	
Welotec	25	
Westermo	6,081	1,200
TOTAL	83,673	5,105

F. Maggi and M. Pogliani, ***Attacks on Smart Manufacturing Systems A Forward-looking Security Analysis***, Trend Micro Whitepaper, 2020
F. Maggi, D. Quarta, M. Pogliani, M. Polino, A. M. Zanchettin, S. Zanero, ***Rogue Robots: Testing the Limits of an Industrial Robot's Security***, Trend Micro Whitepaper, 2017

Risk = assets x threats x vulnerabilities

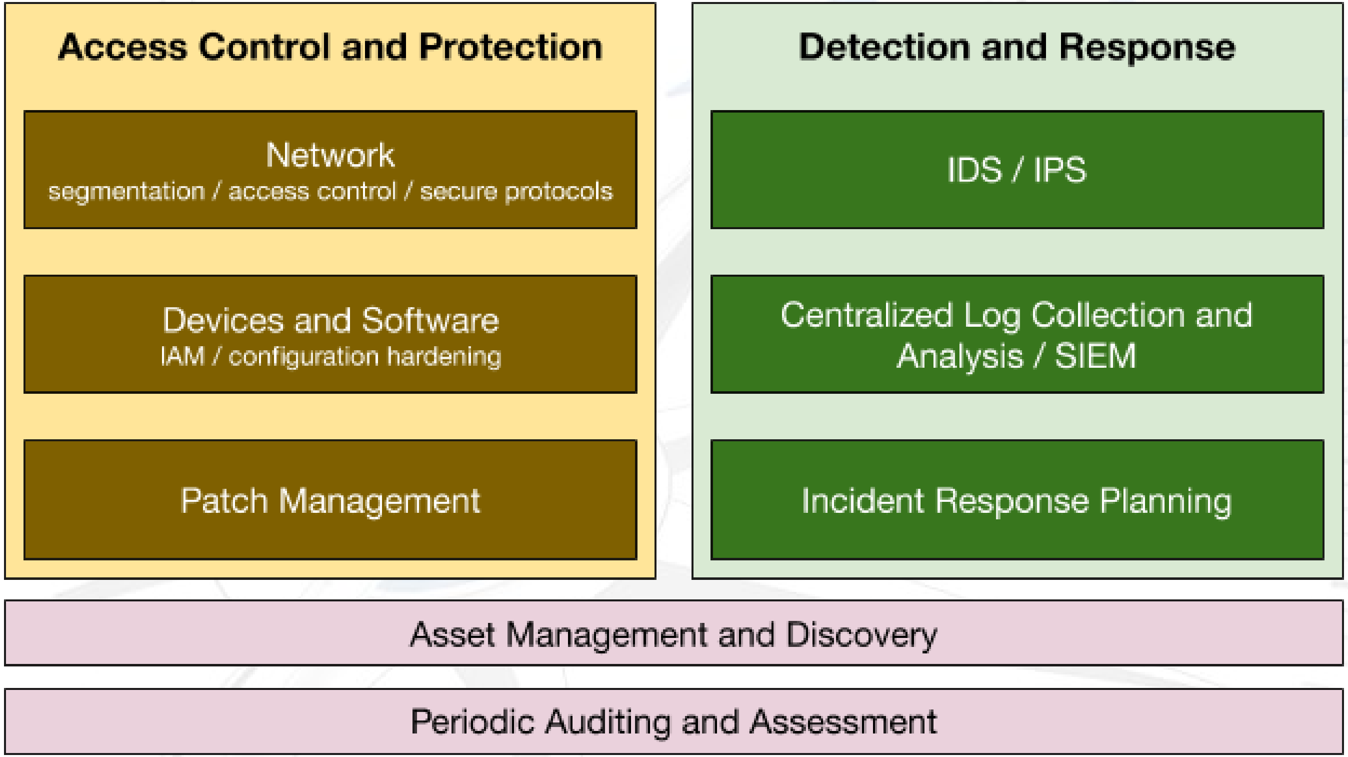
✓ ✓ ✓

Considering security-related risk is fundamental for Industry 4.0 projects

Technical Controls

Policy and Procedures

BASIC SECURITY CONTROLS



Access Control and Protection

Network
segmentation / access control / secure protocols

Devices and Software
IAM / configuration hardening

Patch Management

Detection and Response

IDS / IPS

Centralized Log Collection and Analysis / SIEM

Incident Response Planning

Asset Management and Discovery

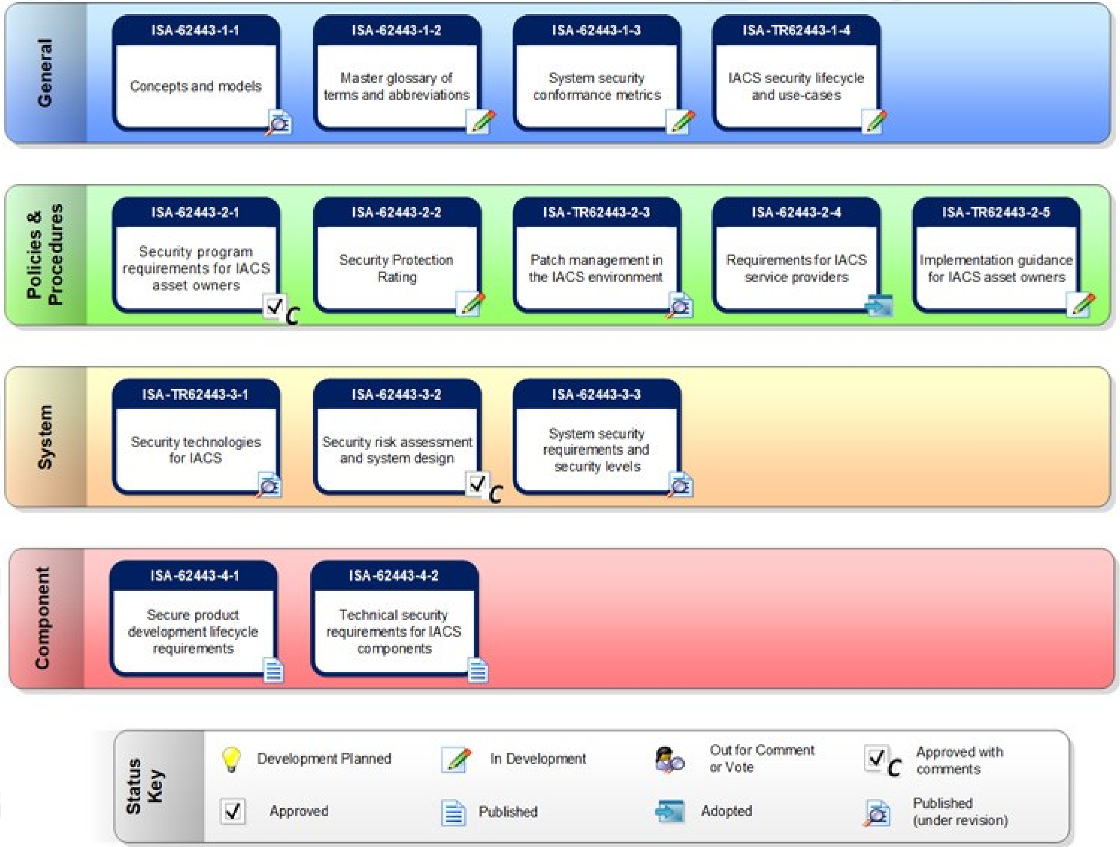
Periodic Auditing and Assessment

S. Zanero, M. Pogliani et al., ***Il tema della Security per l'Industria 4.0***, Osservatori Politecnico di Milano, 2019

CYBERSECURITY STANDARDS

- **Standards** are now explicitly **considering security features**
  - Example: **ISA/IEC 62443-4-2-2018**
  - *Security for Industrial Automation and Control Systems: Technical Security Requirements for IACS Components*
- Another example:
  - **ISO/TR 22100-4:2018** - *Safety of machinery [...]: Guidance to machinery manufacturers for consideration of related IT-security*
  - December 2018

IEC 62443: OVERVIEW



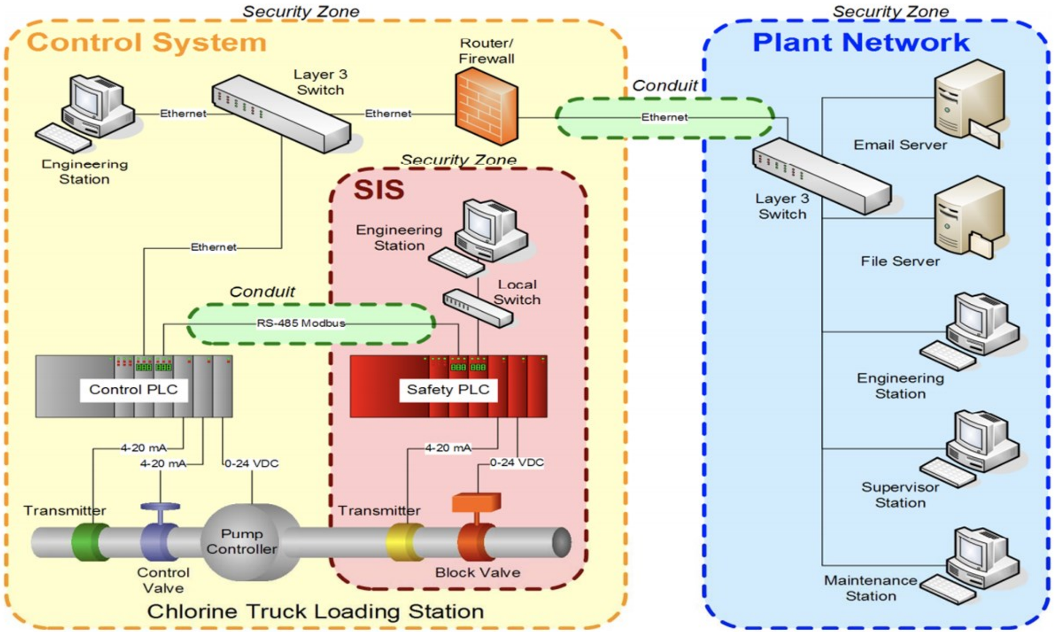
General	ISA-62443-1-1 Concepts and models	ISA-62443-1-2 Master glossary of terms and abbreviations	ISA-62443-1-3 System security conformance metrics	ISA-TR62443-1-4 IACS security lifecycle and use-cases	
Policies & Procedures	ISA-62443-2-1 Security program requirements for IACS asset owners ✓C	ISA-62443-2-2 Security Protection Rating	ISA-TR62443-2-3 Patch management in the IACS environment	ISA-62443-2-4 Requirements for IACS service providers	ISA-TR62443-2-5 Implementation guidance for IACS asset owners
System	ISA-TR62443-3-1 Security technologies for IACS	ISA-62443-3-2 Security risk assessment and system design ✓C	ISA-62443-3-3 System security requirements and security levels		
Component	ISA-62443-4-1 Secure product development lifecycle requirements	ISA-62443-4-2 Technical security requirements for IACS components			

Status Key

- Development Planned
- In Development
- Out for Comment or Vote
- ✓C Approved with comments
- ✓ Approved
- Published
- Adopted
- Published (under revision)

IEC 62443: ZONES AND CONDUITS

Décomposition en zones et conduits



http://www.kbintelligence.com/Medias/PDF/ISA_Doha_hauet.pdf

IEC 62443: SECURITY LEVELS

SL0	No requirement		
SL1	Eavesdropping or casual exposure		
SL2	Active attack	Generic skills	Low resources and motivation
SL3	Active attack	IACS skills	Moderate resources and motivation
SL4	Active attack	IACS skills	Extended resources and high motivation

IEC 62443: FOUNDATIONAL REQUIREMENTS

1. *Identification and authentication control (IAC)*
2. *Use control (UC)*
3. *System integrity (SI)*
4. *Data confidentiality (DC)*
5. *Restricted data flow (RDF)*
6. *Timely response to events (TRE)*
7. *Resource availability (RA)*

IEC 62443: SECURITY REQUIREMENTS (EXAMPLE)

		SL1	SL2	SL3	SL4
FR1	**Identification and authentication control**				
SR1.1	**Human user identification and authentication**	**X**	**X**	**X**	**X**
RE1	Unique identification and authentication		X	X	X
RE2	Multifactor authentication for untrusted networks			X	X
RE3	Multifactor authentication for all networks				X
SR1.2	**Software process and devide identification and authentication**		**X**	**X**	**X**
RE1	Unique identification and authentication			X	X
SR1.3	**Account management**	**X**	**X**	**X**	**X**
RE1	Unified account management			X	X
SR1.4	Identifier management	X	X	X	X
SR1.5	**Authentication management**	**X**	**X**	**X**	**X**
RE1	Hardware security for software process identity credentials			X	X
SR1.6	**Wireless access management**	**X**	**X**	**X**	**X**
RE1	Unique identification and authentication		X	X	X
SR1.7	**Strength of password-based authentication**	**X**	**X**	**X**	**X**
RE1	Password generation and lifetime restrictions for human users			X	X

CONCLUSIONS

Industrial cyber-physical systems are not isolated or air-gapped anymore.

- **Threats**: from casual "mass" attacks to very sophisticated targeted attacks.
- **Assets**: safety, production continuity, production outcome, IP
- **Vulnerabilities**:
  - Security of ***devices*** and ***protocols*** used in Industry 4.0 is not (yet) on par with IT standards
  - Patching problem
- Properly **managing "OT" security** is fundamental to maintain business requirements
  - Technical controls, standards, governance

ANIE FEDERAZIONE CONFINDUSTRIA

QUESTIONS?

marcello.pogliani@polimi.it

Organizzato da ANIE SERVIZI INTEGRATI