

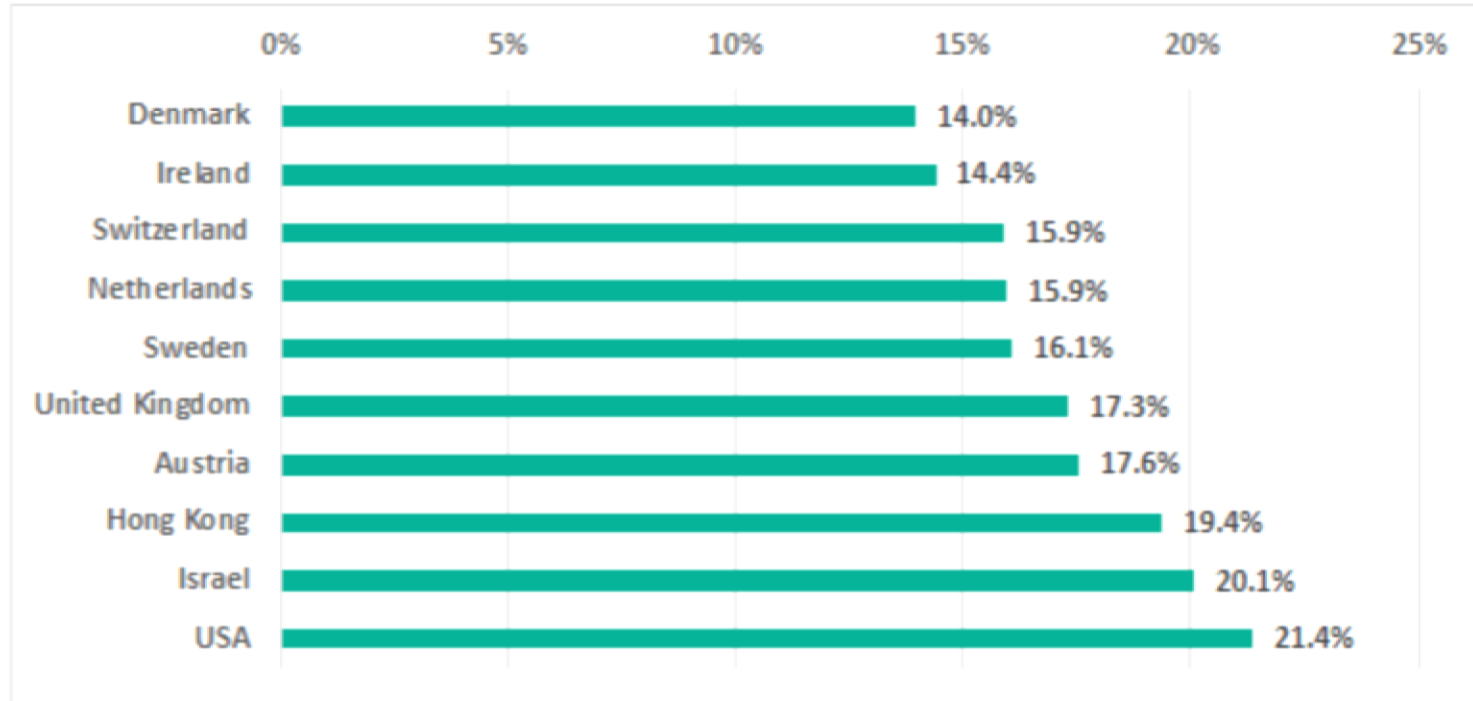
# Visibility als erster Schritt zu sicheren OT Netzwerken

November, 2018

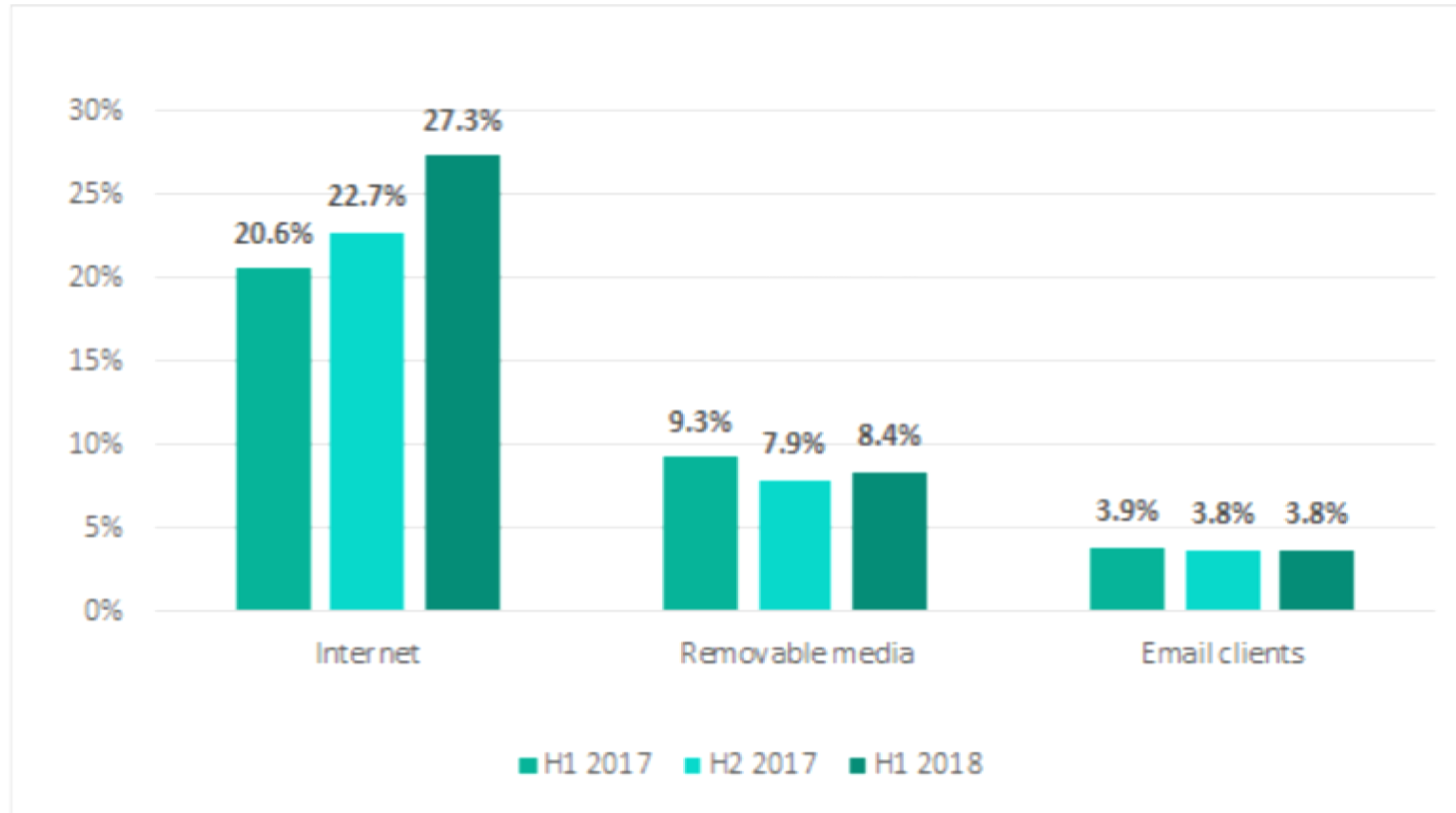
Markus Hirsch (mhirsch@fortinet.com)

# Good News...?

10 countries with the lowest percentages of ICS computers attacked, H1 2018



Main sources of threats blocked on ICS computers (percentage of computers attacked during half-year periods)





TOTAL RESULTS

73

TOP COUNTRIES



Austria 73

TOP CITIES

Vienna	7
Steyr	6
Telfs	3
Schorfing	3
Salzburg	2

TOP ORGANIZATIONS

Telekom Austria	35
LIWEST Kabelmedien GmbH	7
Salzburg AG	6
Hutchison Drei Austria GmbH	3
EEG Customers	3

178. [REDACTED]

Added on 2018-11-05 12:00:59 GMT

Austria

Details

ICS

```
Unit ID: 0
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)
```

```
Unit ID: 1
-- Slave ID Data: Illegal Function (Error)
-- Device Identification: Illegal Function (Error)
```

77 [REDACTED]

Added on 2018-11-01 15:08:32 GMT

Austria

Details

ICS

```
Unit ID: 0
-- Slave ID Data: LMB3.1.1 (0ab4ff4c4d42332e312e31)
```

```
Unit ID: 1
-- Slave ID Data: LMB3.1.1 (0ab4ff4c4d42332e312e31)
```

```
Unit ID: 2
-- Slave ID Data: LMB3.1.1 (0ab4ff4c4d42332e312e31)
```

```
Unit ID: 3
-- Slave ID Data: LMB3.1.1 (0ab4ff4c4d42332e312e31)
```

```
Unit ID: 4
-- Slave ID Data: ...
```

[REDACTED]

Added on 2018-11-02 19:01:35 GMT

Austria

Details

ICS


```
Unit ID: 1
-- Slave ID Data: ? (@13f00)
```

SHODAN  [Explore](#) [Downloads](#) [Reports](#) [Developer Pricing](#) [Enterprise Access](#) [Contact Us](#)

[Exploits](#) [Maps](#) [Share Search](#) [Download Results](#) [Create Report](#)

TOTAL RESULTS  
**27**

TOP COUNTRIES



Austria 27

TOP CITIES

Vienna 7  
Wiener Neustadt 2  
Graz 2  
Wienerberg 1  
Tarrenz 1

TOP SERVICES

SNMP 19  
Siemens S7 8

TOP ORGANIZATIONS

Telekom Austria 7  
T-Mobile Austria GmbH 6  
Hutchison Drei Austria GmbH 5  
H3G Customers 3  
nmc kommunikationstechnologie gmbh 1

TOP PRODUCTS

Compot 2

**195** [REDACTED]

Added on 2018-11-02 14:17:51 GMT

**Austria, Salzburg**

[Details](#)

[Decrypt](#)

Reserved for operating system:  
Serial number of memory card: SD 217C9210  
Location designation of a module:  
Manufacturer and profile of a CPU module:  
Module type: CPU 315-2 PN/DP  
PLC name: **SIMATIC 300(1)**  
Module: 6ES7 315-2EH14-0AB0 v.0.1  
Plant identification:  
OEM ID of a module:  
Module name:...

**178** [REDACTED]

Added on 2018-11-02 08:42:19 GMT

**Austria**

[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.0.2  
Basic Firmware: v.2.6.11  
Module name: CPU 313C  
Serial number of module: S C-A4V005672010  
Plant identification: Rollo&Pool  
Basic Hardware: 6ES...

**178** [REDACTED]

Added on 2018-10-31 20:17:08 GMT

**Austria, [REDACTED]**

[Details](#)

[ICS](#)

Copyright: Original Siemens Equipment  
PLC name: **SIMATIC 300(1)**  
Module type: CPU 314C-2 PN/DP  
Unknown (129): Boot Loader A  
Module: 6ES7 314-6EH04-0AB0 v.0.2  
Basic Firmware: v.3.3.6  
Module name: Zentrale\_CPU  
Serial number of module: S C-C4TX49092012  
Plant identification:  
Basic Hardware:...

https://www.shodan.io/



Kacy Zurkus News Writer

[Email Kacy](#) [Connect on LinkedIn](#)



According to a newly released survey conducted at **Black Hat 2018**, 50% of hackers said that Windows 8 and Windows 10 have been the easiest attack vectors to exploit this year.

**Thycotic** surveyed more than 300 hackers – nearly 70% of whom identified as white hats – to understand the hacker perspective with regard to vulnerabilities and attack vectors.




<https://www.infosecurity-magazine.com/news/hackers-say-windows-8-10-easiest>

# Pwned with '4 lines of code': Researchers warn SCADA systems are still hopelessly insecure

How Stuxnet, Shamoon, et al ran riot

By [John Leyden](#) 18 Jun 2018 at 09:43

66  SHARE ▼



**BSides London** Industrial control systems could be exposed not just to remote hackers, but to local attacks and physical manipulation as well.

[https://www.theregister.co.uk/2018/06/18/physically\\_hacking\\_scada\\_infosec/](https://www.theregister.co.uk/2018/06/18/physically_hacking_scada_infosec/)

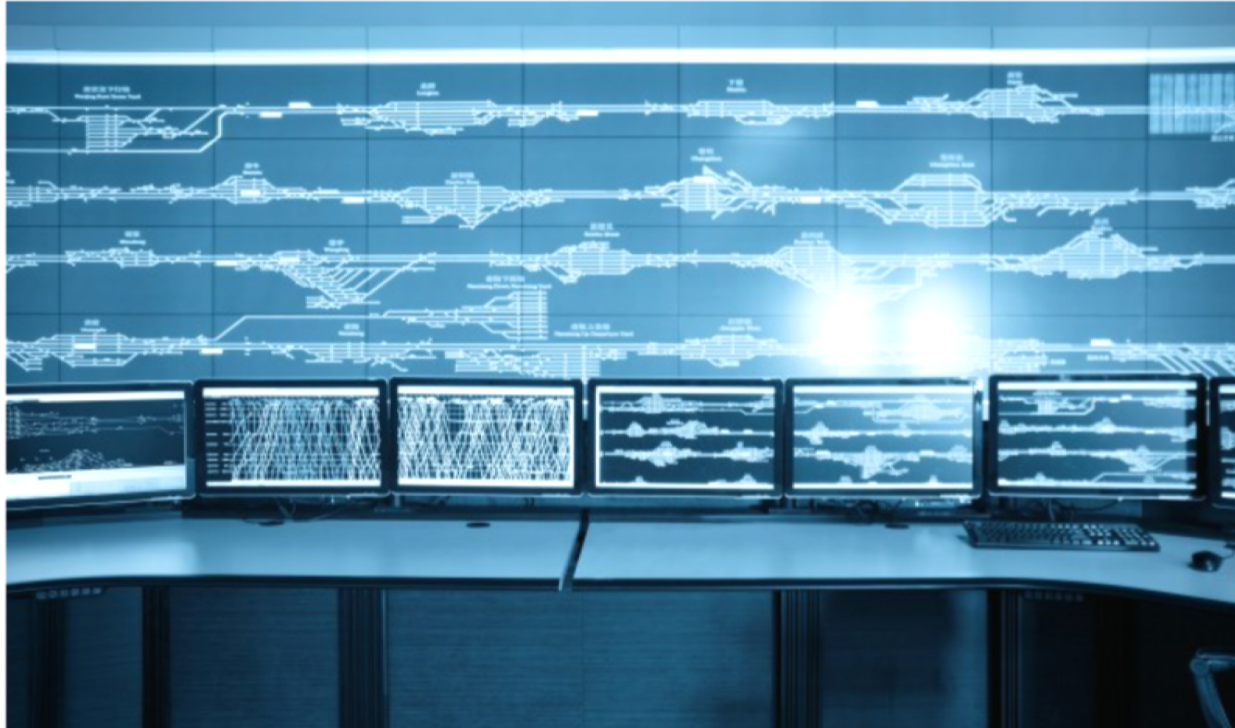
# Insecure SCADA Systems Blamed in Rash of Pipeline Data Network Attacks



Author:  
Lindsey O'Donnell  
April 4, 2018 / 10:12 am

2:30 minute read

Share this article:



After a cyberattack shut down numerous pipeline communication networks this week experts are stressing the importance of securing third-party systems in supervisory control and data acquisition (SCADA) environments.

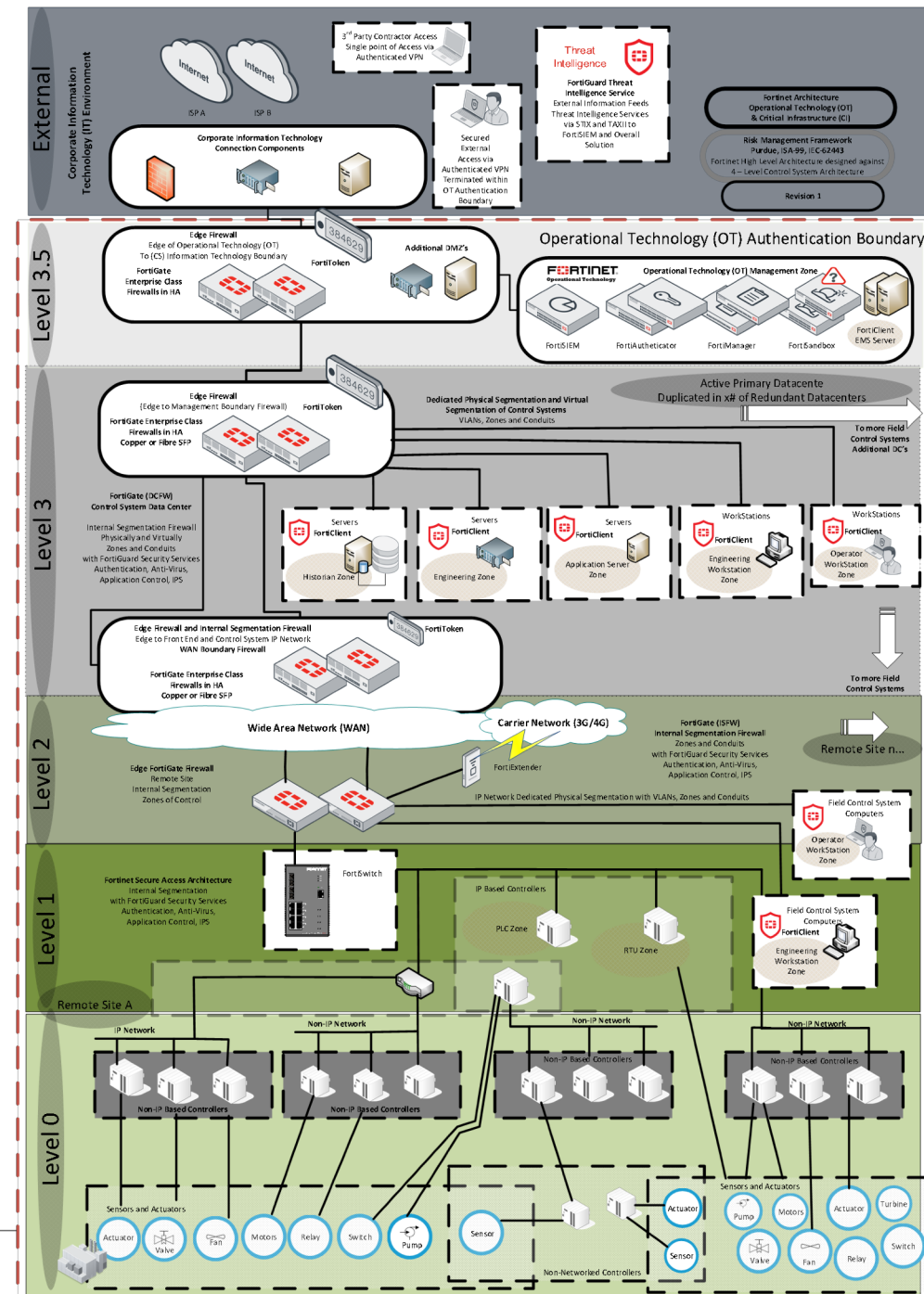
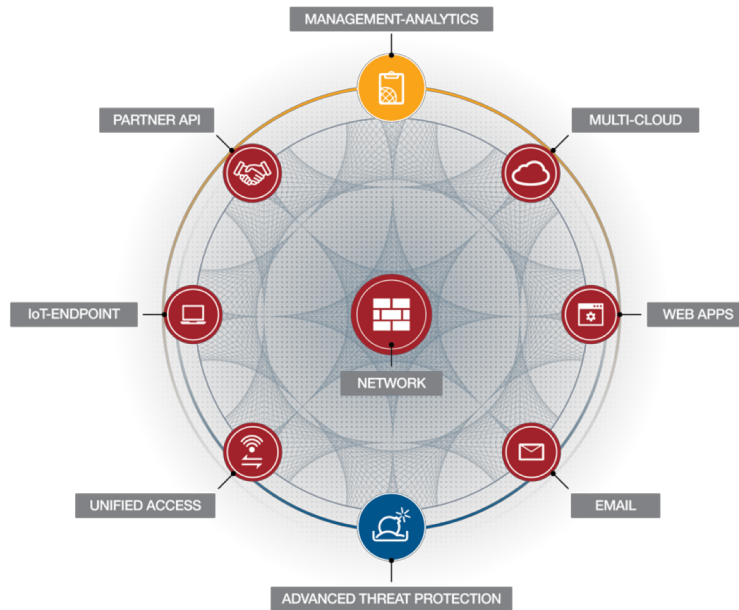
threat **post**

<https://threatpost.com/insecure-scada-systems-blamed-in-rash-of-pipeline-data-network-attacks/130952/>



# Purdue Model

- ISA-99, IEC-62443, RMF
- Effective Layered Security Model
- Aligns to Fortinet Fabric
- Logical Level Approach
- Focused on Business requirements



# Strukturierte Herangehensweise

---

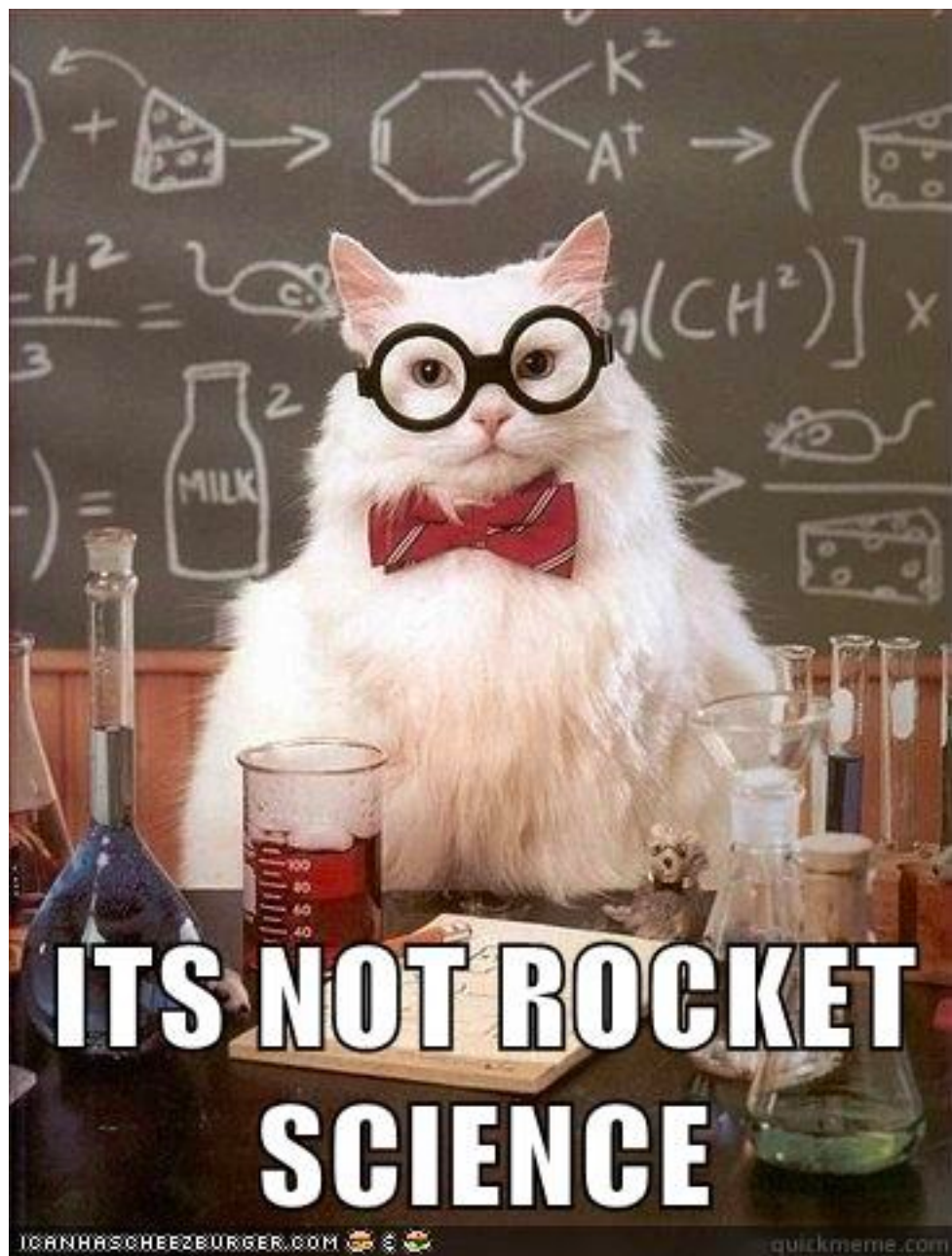
## Guide to Industrial Control Systems (ICS) Security

**Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS),  
and Other Control System Configurations such as Programmable Logic Controllers (PLC)**

---

Keith Stouffer  
Victoria Pillitteri  
Suzanne Lightman  
Marshall Abrams  
Adam Hahn

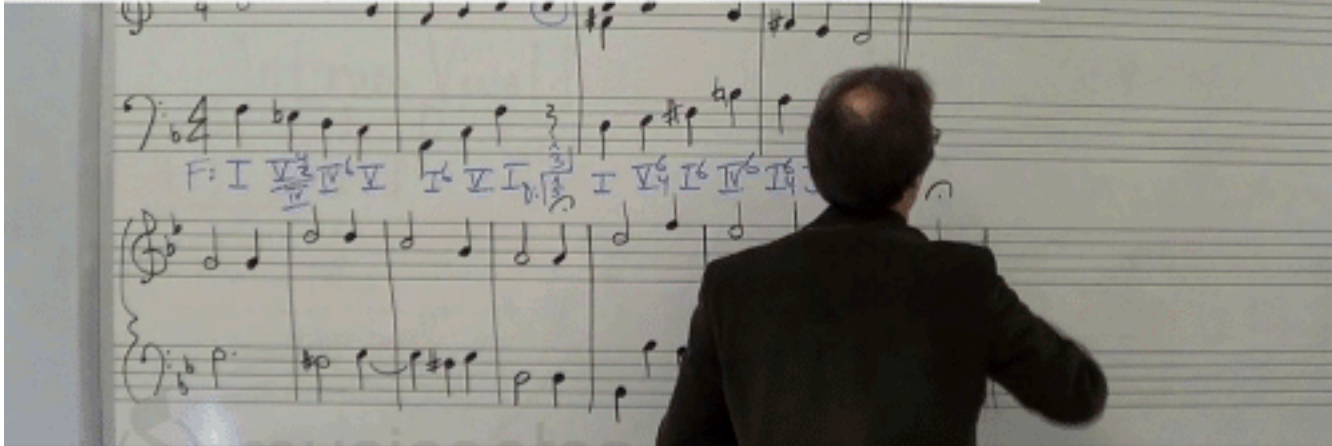
This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-82r2> T



# Strukturierte Herangehensweise

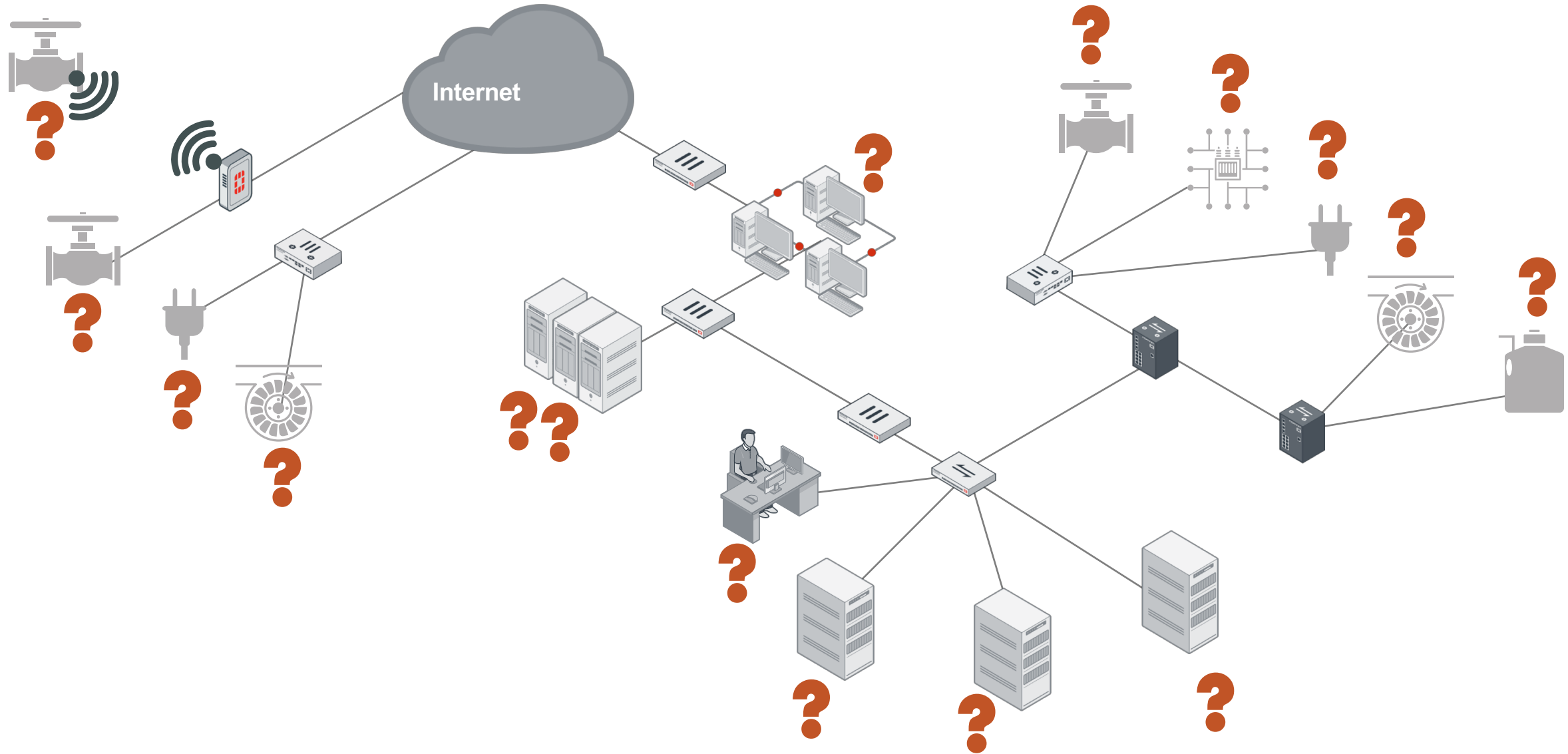
- 4.1 Business Case for Security
  - 4.1.4 Presenting the Business Case to Leadership
- 4.4 Define ICS-specific Security Policies and Procedures
- 4.5 Implement an ICS Security Risk Management Framework
  - 4.5.1 Categorize ICS Systems and Networks Assets
  - 4.5.2 Select ICS Security Controls
  - 4.5.3 Perform Risk Assessment
  - 4.5.4 Implement the Security Controls

Come on guys, it's not Rocket Science...

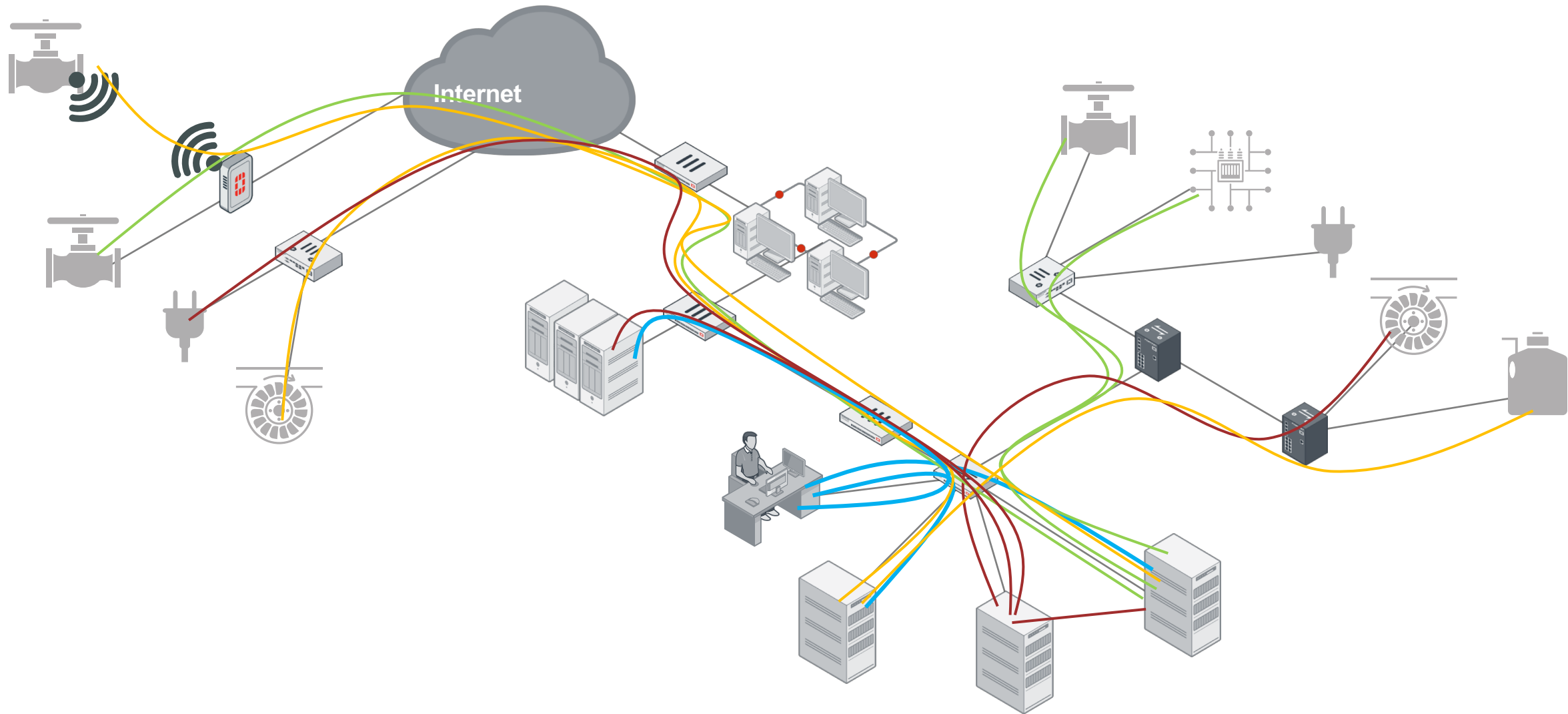


<https://me.me/i/come-on-guys-its-not-rocket-science-1-3-1016-7-5-dcb4d82b649b4a788cf1002db5be1478>

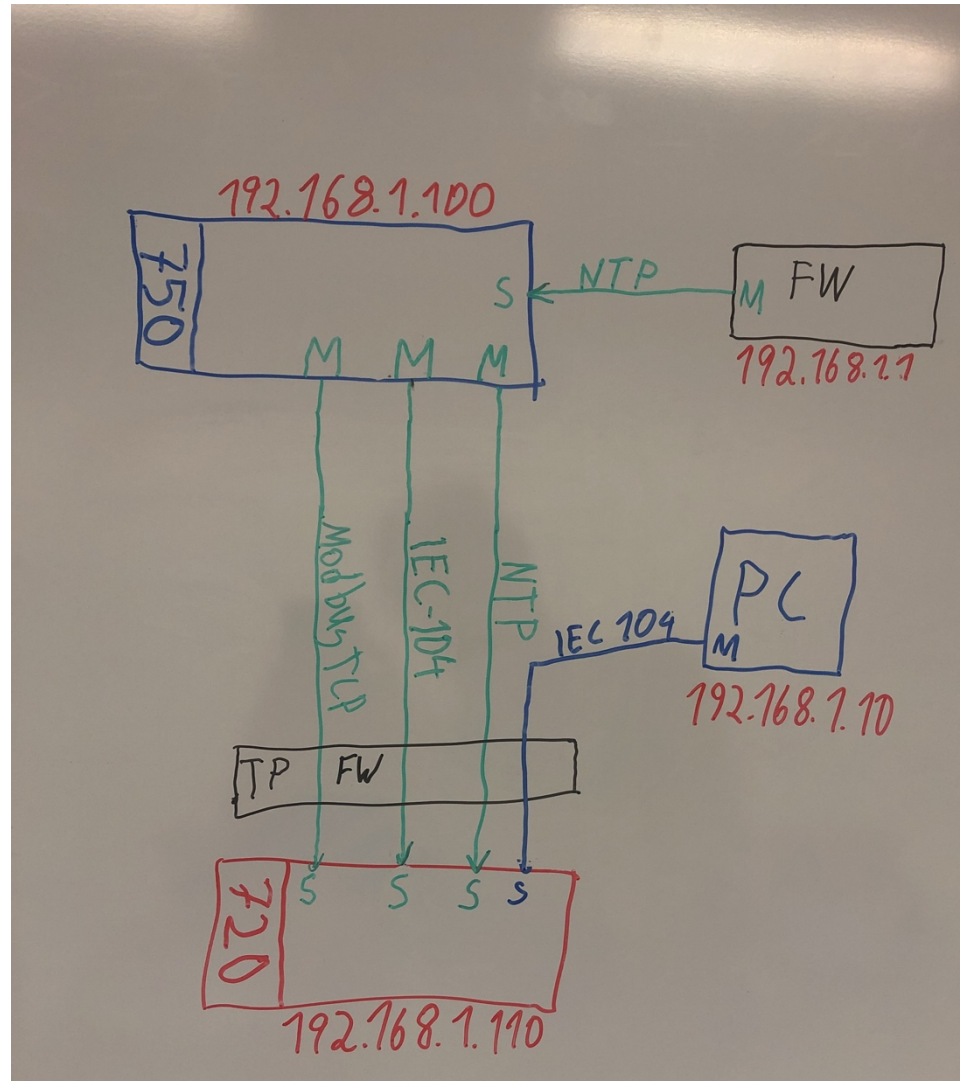
# Schritt 1: Finde alle Geräte



# Schritt 2: Erkenne die Kommunikationsbeziehungen



# Wie alles begann...





## OT Kommunikationsreport

### Modbus Kommunikation

#	srcip	dstip	num_conn
1	192.168.1.100	192.168.1.110	95131

### Modbus Kommunikationen mit Protokolldetails

#	srcip	dstip	
1	192.168.1.100	192.168.1.110	Modbus Modbus_Read.Input.Registers

### Modbus Kommunikationen pro Server mit Protokolldetails

#	dstip	app__agg__
1	192.168.1.110	Modbus Modbus_Read.Input.Registers

## IEC-140 Kommunikation

#	srcip	dstip	num_conn
1	10.0.1.1	10.0.2.1	183986
2	192.168.1.100	192.168.1.110	6440

## IEC-104 Kommunikation mit Protokolldetails

#	srcip	dstip	
1	10.0.1.1	10.0.2.1	IEC.60870.5.104_Control.Functions.STARTDT.ACT IEC.60870.5.104_Control.Functions.STARTDT.CON IEC.60870.5.104_Information.Transfer IEC.60870.5.104_Information.Transfer.C.CS.NA.1 IEC.60870.5.104_Information.Transfer.C.IC.NA.1 IEC.60870.5.104_Information.Transfer.M.EI.NA.1 IEC.60870.5.104_Information.Transfer.M.ME.NC.1 IEC.60870.5.104_Information.Transfer.M.ME.TF.1 IEC.60870.5.104_Information.Transfer.M.SP.NA.1 IEC.60870.5.104_Information.Transfer.M.SP.TB.1 IEC.60870.5.104_Information.Transfer.Process.Monitor IEC.60870.5.104_Information.Transfer.System.Information IEC.60870.5.104_Supervisory.Functions
2	192.168.1.100	192.168.1.110	IEC.60870.5.104_Control.Functions.STARTDT.ACT IEC.60870.5.104_Control.Functions.STARTDT.CON IEC.60870.5.104_Control.Functions.TESTFR.ACT IEC.60870.5.104_Control.Functions.TESTFR.CON IEC.60870.5.104_Information.Transfer IEC.60870.5.104_Information.Transfer.C.CS.NA.1 IEC.60870.5.104_Information.Transfer.M.SP.TB.1 IEC.60870.5.104_Information.Transfer.Process.Monitor IEC.60870.5.104_Information.Transfer.System.Information IEC.60870.5.104_Supervisory.Functions

## IEC-104 Kommunikationen pro Server mit Protokolldetails

#	dstip	app_agg_
1	10.0.2.1	IEC.60870.5.104_Control.Functions.STARTDT.ACT IEC.60870.5.104_Control.Functions.STARTDT.CON IEC.60870.5.104_Information.Transfer IEC.60870.5.104_Information.Transfer.C.CS.NA.1 IEC.60870.5.104_Information.Transfer.C.IC.NA.1 IEC.60870.5.104_Information.Transfer.M.EI.NA.1 IEC.60870.5.104_Information.Transfer.M.ME.NC.1 IEC.60870.5.104_Information.Transfer.M.ME.TF.1

## Alle Kommunikationen pro Server mit Protokolldetails

#	dstip	app__agg__
1	10.0.2.1	IEC.60870.5.104_Control.Functions.STARTDT.ACT IEC.60870.5.104_Control.Functions.STARTDT.CON IEC.60870.5.104_Information.Transfer IEC.60870.5.104_Information.Transfer.C.CS.NA.1 IEC.60870.5.104_Information.Transfer.C.IC.NA.1 IEC.60870.5.104_Information.Transfer.M.EI.NA.1 IEC.60870.5.104_Information.Transfer.M.ME.NC.1 IEC.60870.5.104_Information.Transfer.M.ME.TF.1 IEC.60870.5.104_Information.Transfer.M.SP.NA.1 IEC.60870.5.104_Information.Transfer.M.SP.TB.1 IEC.60870.5.104_Information.Transfer.Process.Monitor IEC.60870.5.104_Information.Transfer.System.Information IEC.60870.5.104_Supervisory.Functions
2	192.168.1.1	NTP Unknown Application
3	192.168.1.100	NTP SSL SSL_TLSv1.2 Unknown Application
4	192.168.1.110	IEC.60870.5.104_Control.Functions.STARTDT.ACT IEC.60870.5.104_Control.Functions.STARTDT.CON IEC.60870.5.104_Control.Functions.TESTFR.ACT IEC.60870.5.104_Control.Functions.TESTFR.CON IEC.60870.5.104_Information.Transfer IEC.60870.5.104_Information.Transfer.C.CS.NA.1 IEC.60870.5.104_Information.Transfer.M.SP.TB.1 IEC.60870.5.104_Information.Transfer.Process.Monitor IEC.60870.5.104_Information.Transfer.System.Information IEC.60870.5.104_Supervisory.Functions Modbus Modbus_Read.Input.Registers

## FortiGate Logs:

#	Source	Destination IP	Service	Application	Application Categ...	File Name
1	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
2	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
3	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
4	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
5	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
6	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
7	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
8	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
9	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
10	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02
11	192.168.1.1...	192.168.1.110	Modbus	Modbus_Read.Input.Registers	Industrial	01 90 00 02

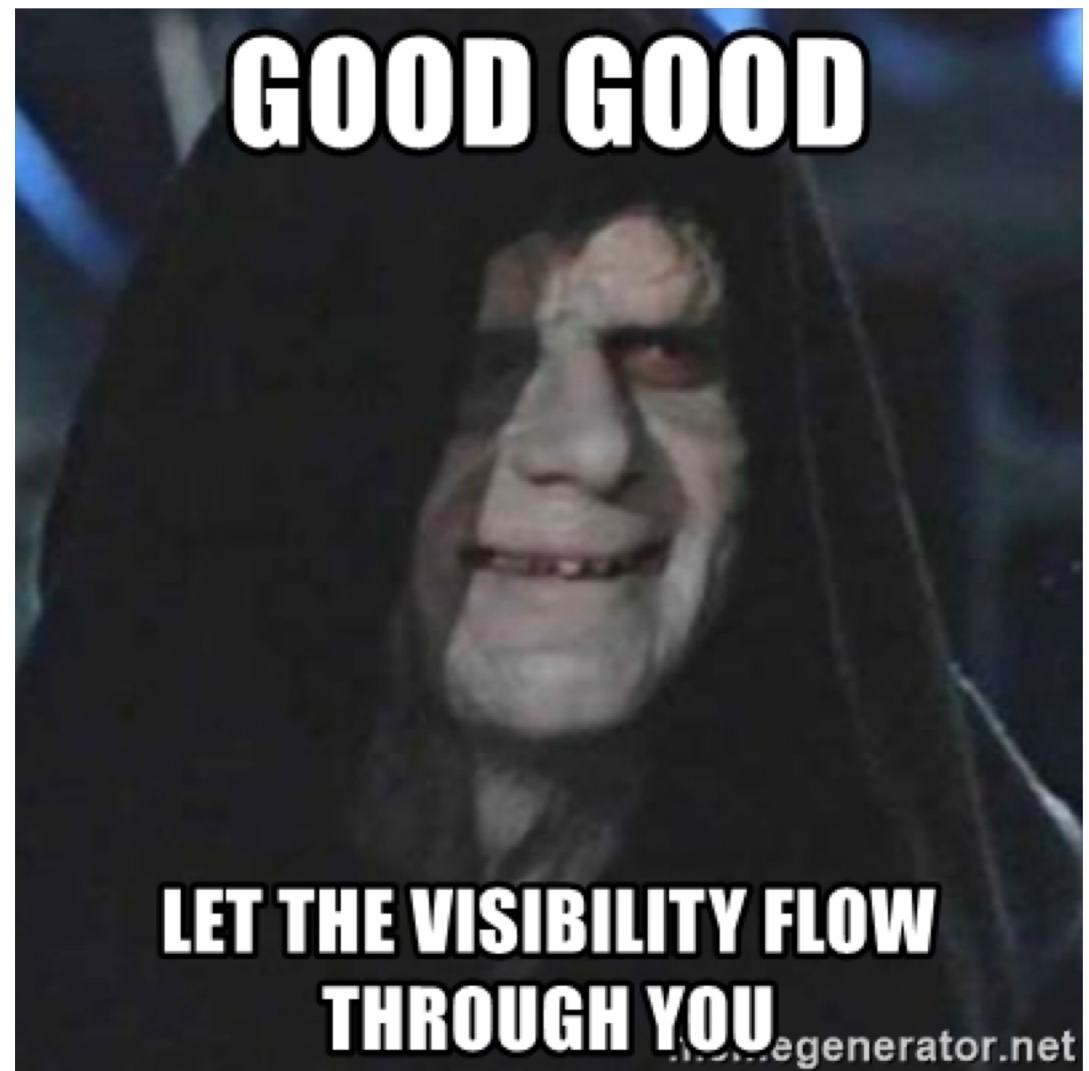
## Wireshark:

```

▶ Frame 2: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▶ Ethernet II, Src: Ids_01:60:00 (00:12:ad:01:60:00), Dst: Ids_01:5d:7a (00:12:ad:01:5d:7a)
▶ Internet Protocol Version 4, Src: 192.168.1.100, Dst: 192.168.1.110
▶ Transmission Control Protocol, Src Port: 57456, Dst Port: 502, Seq: 1, Ack: 1, Len: 12
▼ Modbus/TCP
  ▶ [Expert Info (Warning/Protocol): Cannot classify packet type. Try setting Modbus/TCP Port pr
    Transaction Identifier: 35717
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 1
▼ Modbus
  .000 0100 = Function Code: Read Input Registers (4)
0000 00 12 ad 01 5d 7a 00 12 ad 01 60 00 08 00 45 00 .....]z.....E.
0010 00 40 b7 8d 40 00 40 06 ff 07 c0 a8 01 64 c0 a8 @.@.@.....d.
0020 01 6e e0 70 01 f6 0d c9 46 71 c5 bf f3 ff 80 18 .n.p....Fq....
0030 01 12 52 dc 00 00 01 01 08 0a 00 bb 25 00 1f 7a .R.....#.z
0040 dc 10 8b 85 00 00 00 06 01 04 01 90 00 02 .....
  
```

## Rapid SCADA Modbus Parser <http://modbus.rapidscada.net/>

Part of Data Package	Description	Value
8B 85	Transaction identifier	0x8B85 (35717)
00 00	Protocol identifier	0 = MODBUS protocol
00 06	Length	0x0006 (6)
01	Unit identifier	0x01 (1)
04	Function code	0x04 (4) - Read Input Registers
01 90	Starting address	0x0191 (401)
00 02	Quantity	0x0002 (2)



The logo for FERTINET is displayed in a bold, white, sans-serif font. The letter 'F' is stylized with three horizontal bars. The letters 'E', 'R', 'T', 'I', 'N', and 'E' are solid. The final 'T' is also solid. A registered trademark symbol (®) is located to the right of the final 'E'. The background is a solid blue color with a complex, white, geometric pattern of overlapping lines and rectangles, creating a 3D architectural effect.

**FERTINET®**