The tools dogma

SANS ICS APAC 2020

Dieter Sarrazyn

https://secudea.be

Image: ©nokblacksheep - stock.adobe.com

“Dogma“ ?

An authoritative principle, belief or statement of opinion, especially one considered to be absolutely true “we have a firewall …”

“we are safe from attacks from the Internet”

Do you have dual home systems bypassing the firewall(s) ??

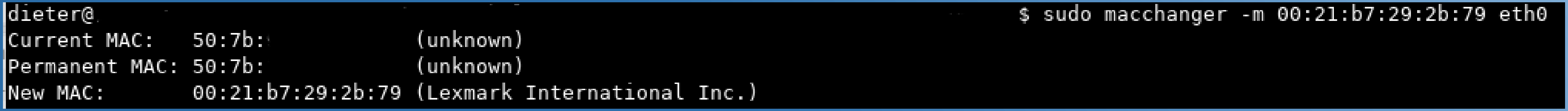
“with .1x nobody can access our (sensitive) network”

- Console ports left logged in
- Inadequate physical access to network devices

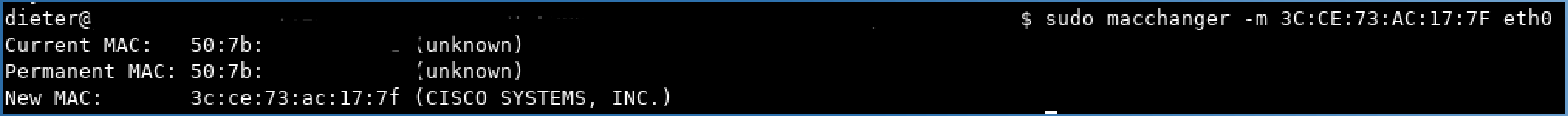
802.1x is just network authentication

“with .1x nobody can access our (sensitive) network”

- What about MAC address bypasses
  - “macchanger”



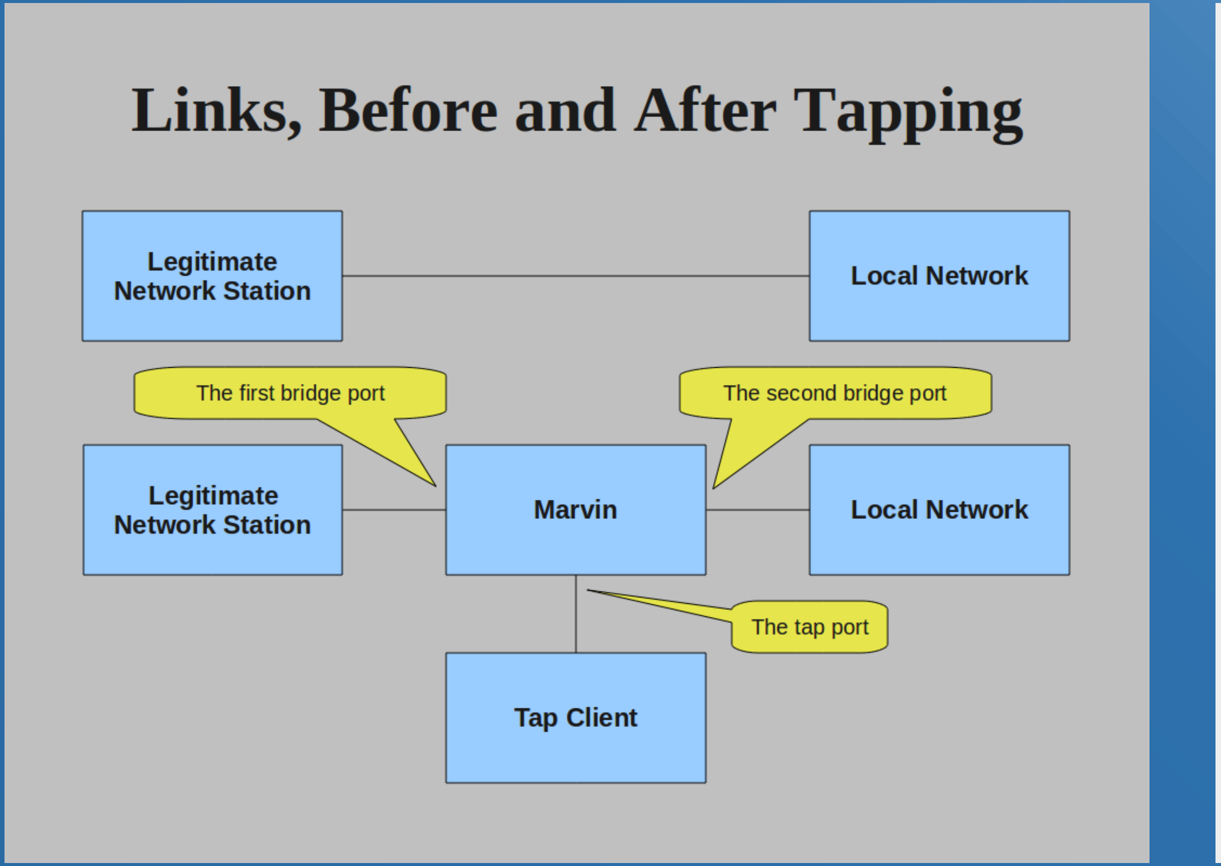
```
dieter@[redacted] $ sudo macchanger -m 00:21:b7:29:2b:79 eth0
Current MAC:   50:7b:[redacted] (unknown)
Permanent MAC: 50:7b:[redacted] (unknown)
New MAC:       00:21:b7:29:2b:79 (Lexmark International Inc.)
```

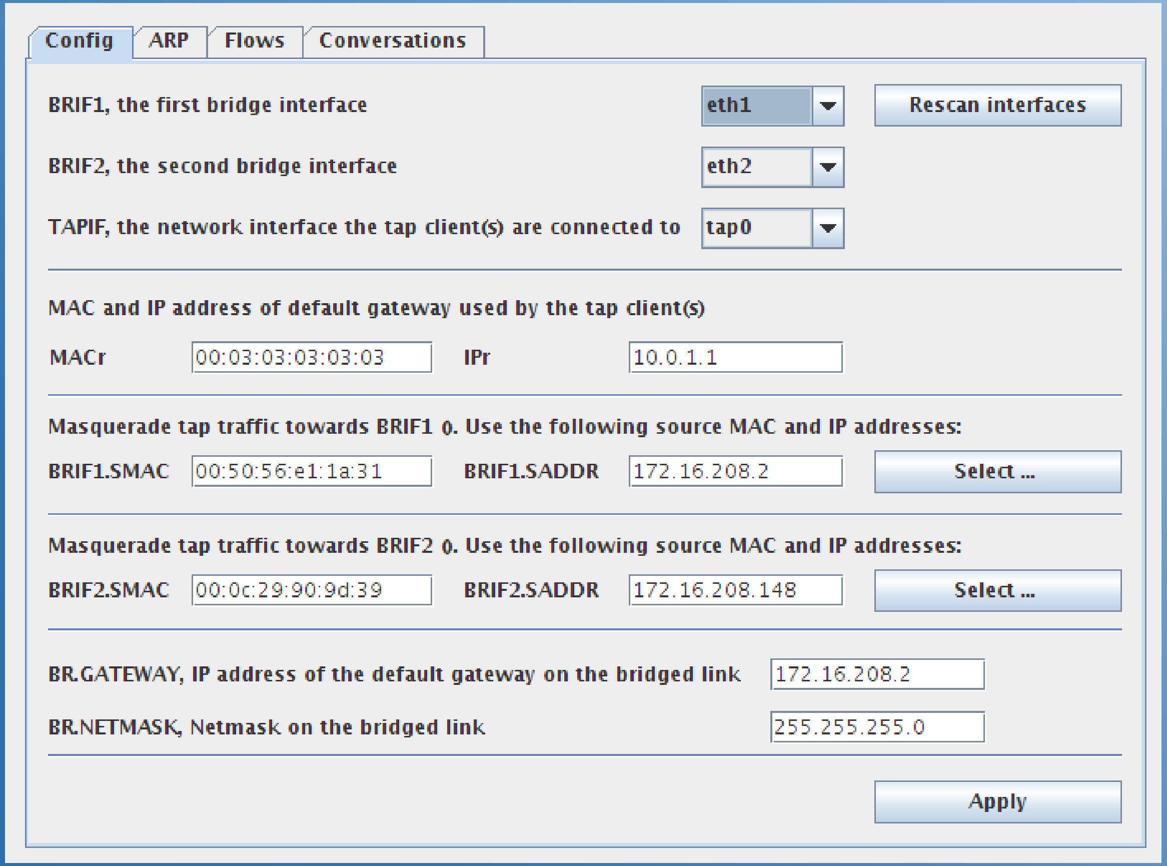


```
dieter@[redacted] $ sudo macchanger -m 3C:CE:73:AC:17:7F eth0
Current MAC:   50:7b:[redacted] (unknown)
Permanent MAC: 50:7b:[redacted] (unknown)
New MAC:       3c:ce:73:ac:17:7f (CISCO SYSTEMS, INC.)
```

“with .1x nobody can access our (sensitive) network”

- Enter Gremwell Marvin …





BRIF1, the first bridge interface: eth1

BRIF2, the second bridge interface: eth2

TAPIF, the network interface the tap client(s) are connected to: tap0

MAC and IP address of default gateway used by the tap client(s)

MACr: 00:03:03:03:03:03 IPr: 10.0.1.1

Masquerade tap traffic towards BRIF1 (). Use the following source MAC and IP addresses:

BRIF1.SMAC: 00:50:56:e1:1a:31 BRIF1.SADDR: 172.16.208.2

Masquerade tap traffic towards BRIF2 (). Use the following source MAC and IP addresses:

BRIF2.SMAC: 00:0c:29:90:9d:39 BRIF2.SADDR: 172.16.208.148

BR.GATEWAY, IP address of the default gateway on the bridged link: 172.16.208.2

BR.NETMASK, Netmask on the bridged link: 255.255.255.0

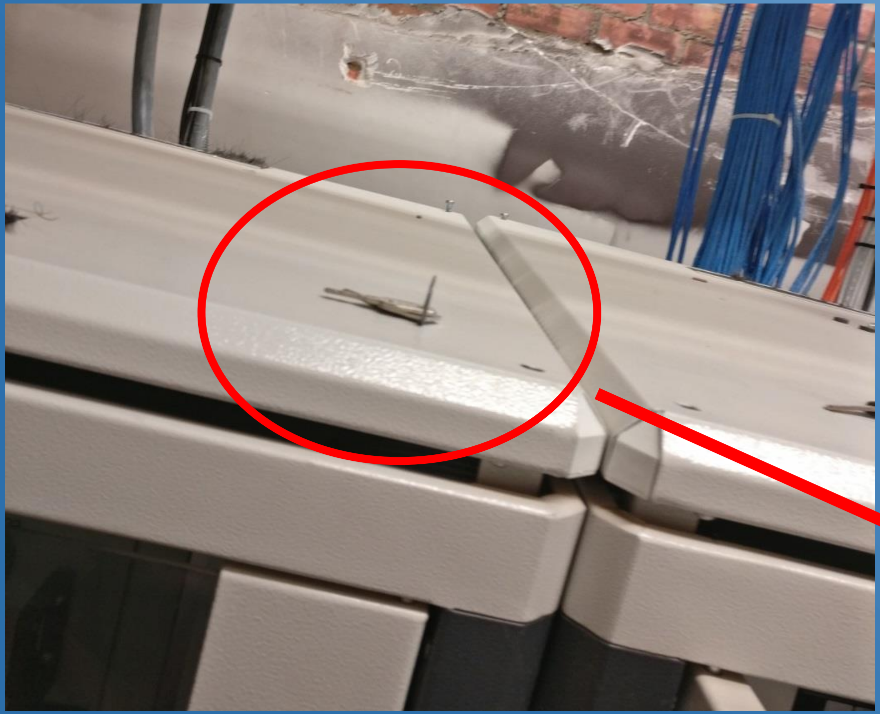
“we have a siem that monitors everything …”

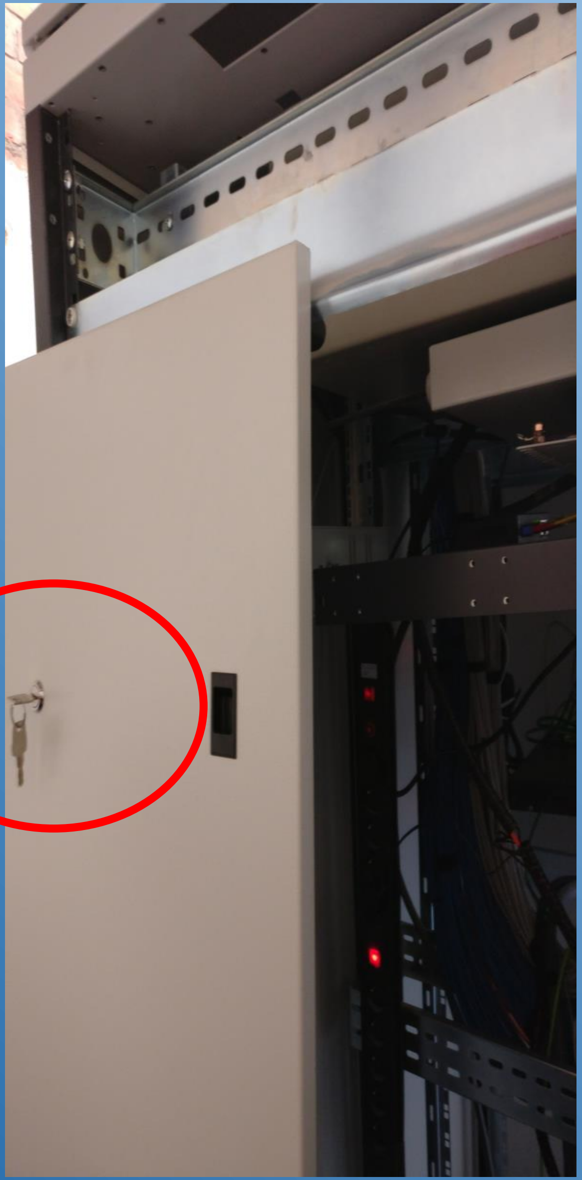
- Logs … lots of logs … lots of lots of …
- Nobody monitoring the thing
- Cloud siem ?

“with our solution, you will have the best visibility in your ICS network”

- Too much false positives
- Too much false negatives
- Missing (proven) malware detections
- Not interpreting ICS/SCADA traffic properly – skipping learning processes

“Nobody
can open
this door”





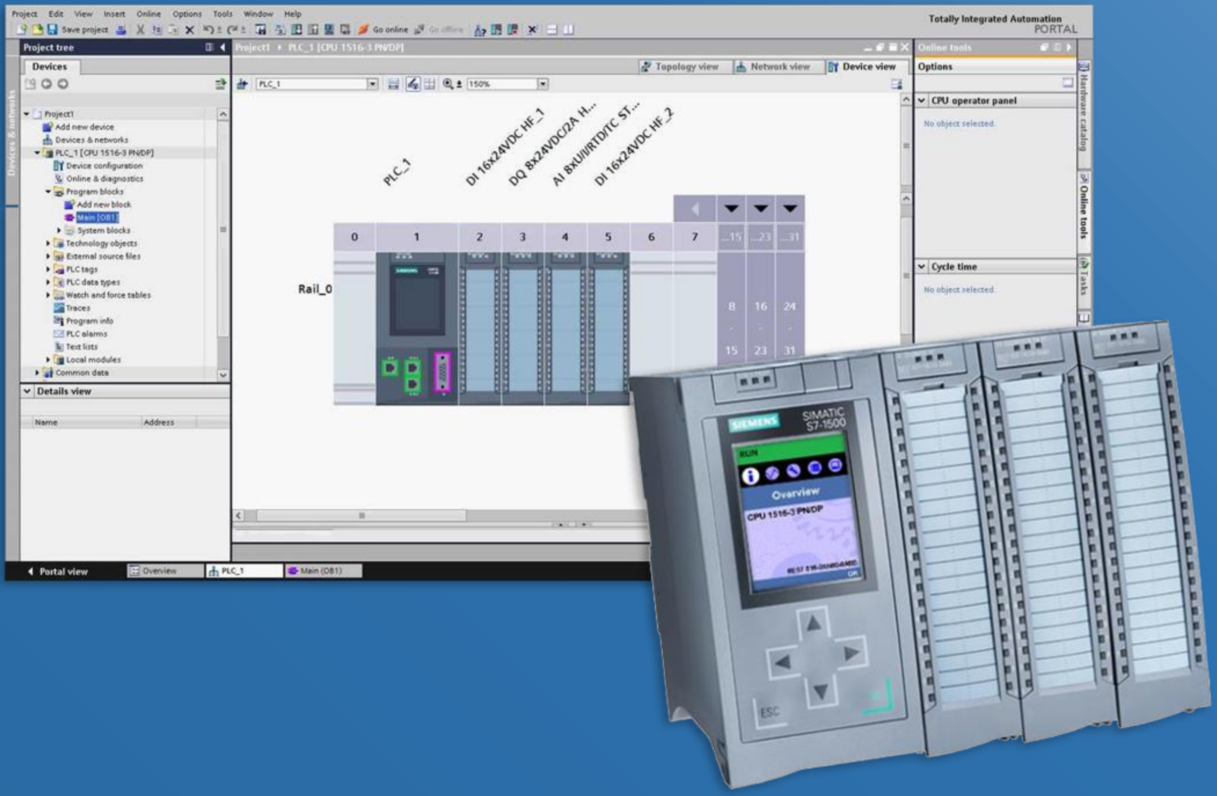
“forgotten” rack key’s
“unlocked” server rooms
“mismounted” physical security

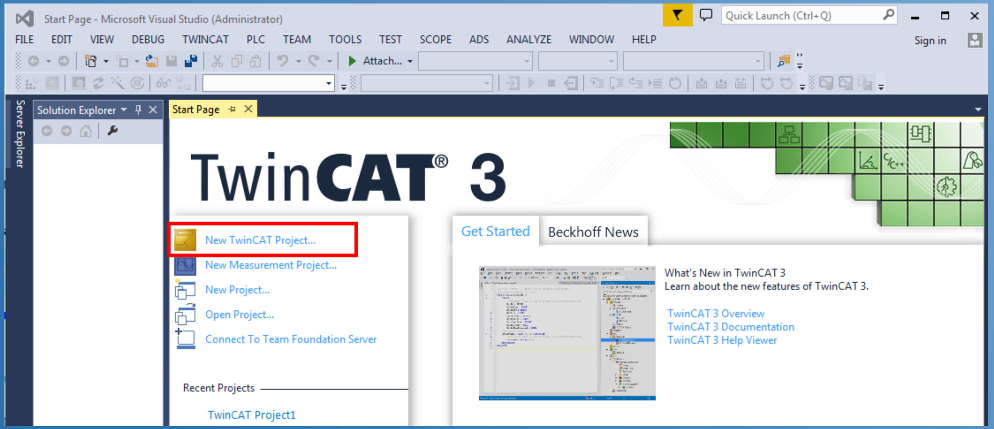
The tools dogma issue

- Tools are often sold as being the holy grail
- Often give a false sense of security
- Often have shortcomings
- Not always fit for your own environment
- “Patching solves everything”

The tools dogma issue

- Often specific to certain ICS/SCADA brands, often weak security



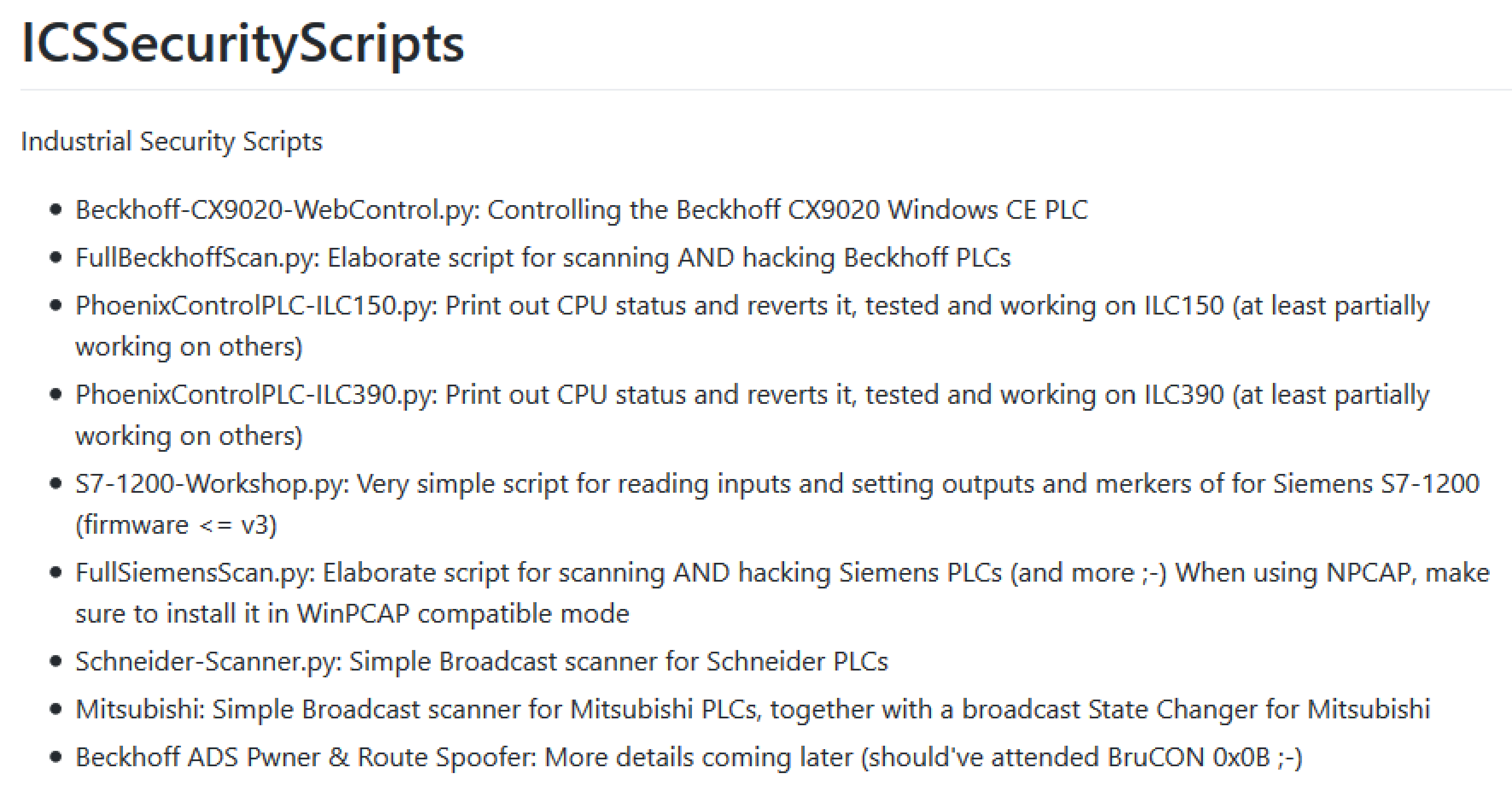


What's New in TwinCAT 3
Learn about the new features of TwinCAT 3.

Engineering tools … Security often an option or weak

The tools dogma issue

- Often specific to certain ICS/SCADA brands, often weak security



ICSSecurityScripts

Industrial Security Scripts

- Beckhoff-CX9020-WebControl.py: Controlling the Beckhoff CX9020 Windows CE PLC
- FullBeckhoffScan.py: Elaborate script for scanning AND hacking Beckhoff PLCs
- PhoenixControlPLC-ILC150.py: Print out CPU status and reverts it, tested and working on ILC150 (at least partially working on others)
- PhoenixControlPLC-ILC390.py: Print out CPU status and reverts it, tested and working on ILC390 (at least partially working on others)
- S7-1200-Workshop.py: Very simple script for reading inputs and setting outputs and merkers of for Siemens S7-1200 (firmware <= v3)
- FullSiemensScan.py: Elaborate script for scanning AND hacking Siemens PLCs (and more ;-) When using NPCAP, make sure to install it in WinPCAP compatible mode
- Schneider-Scanner.py: Simple Broadcast scanner for Schneider PLCs
- Mitsubishi: Simple Broadcast scanner for Mitsubishi PLCs, together with a broadcast State Changer for Mitsubishi
- Beckhoff ADS Pwner & Route Spoofer: More details coming later (should've attended BruCON 0x0B ;-)

https://github.com/tijldeneut/ICSSecurityScripts

The tools dogma demystified

- There is no such thing as a security tool swiss army knife

- Never put your trust in a single tool/solution

- Only relying on tools will fail… tools are part of the equation
  - Logical
  - Physical
  - Human

How to deal with this dogma?

Question everything…

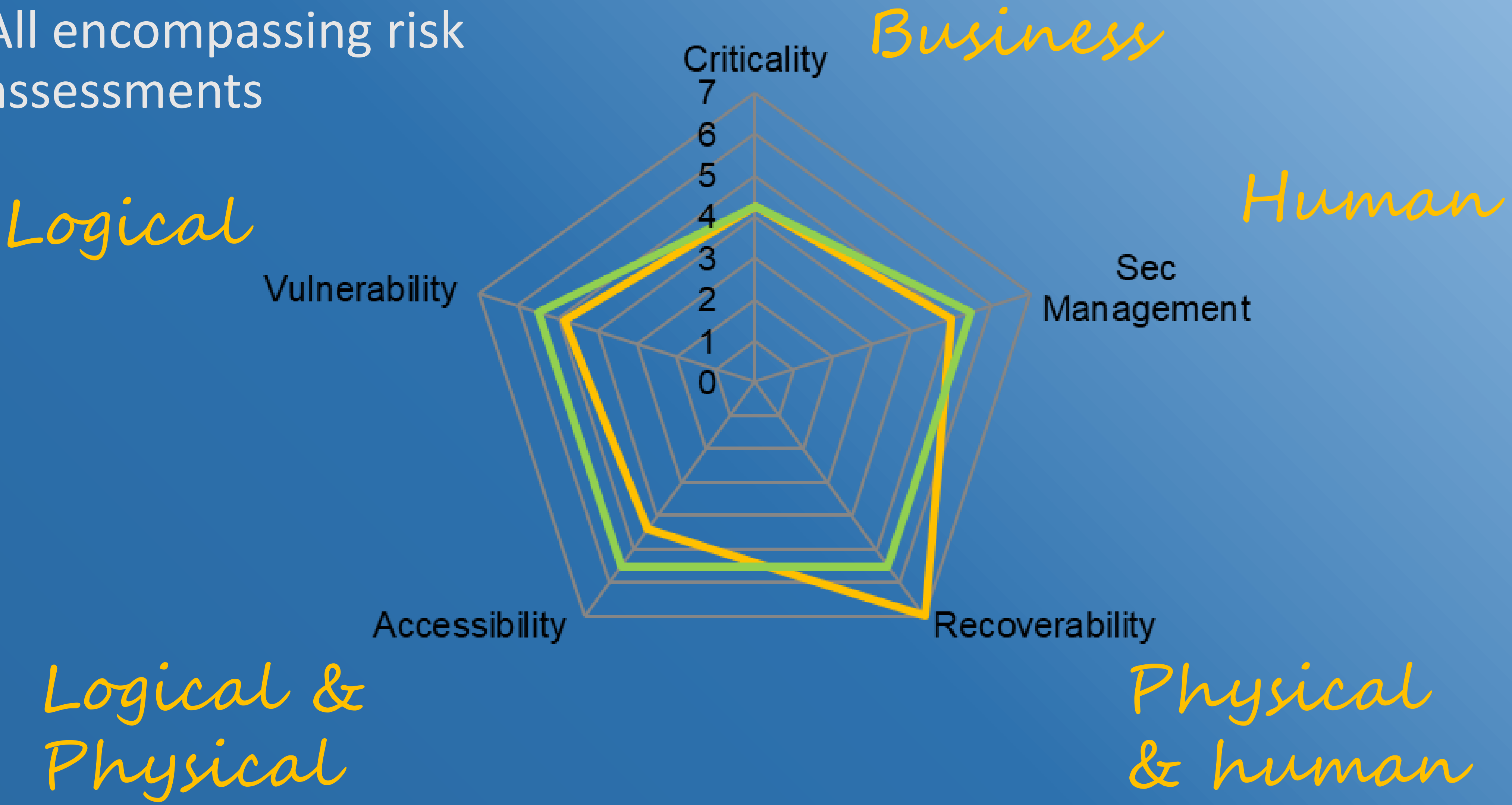
Test everything…

Question everything again …

Test everything again …

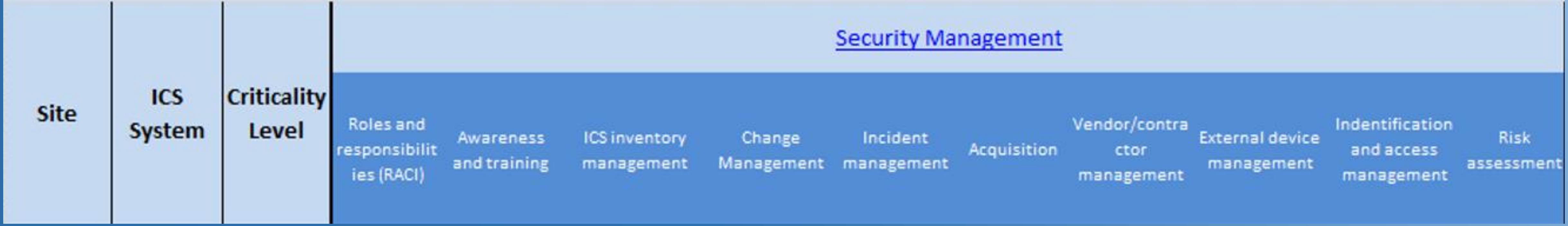
How to deal with this dogma?

- All encompassing risk assessments

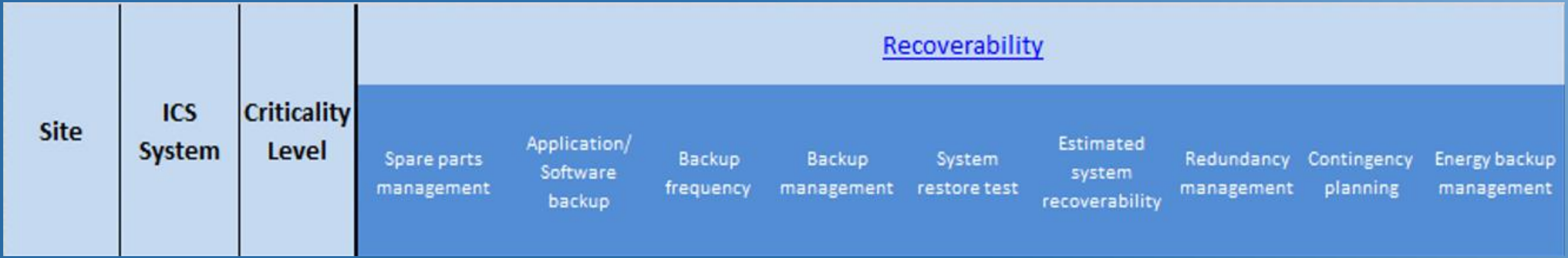


How to deal with this dogma?

- All encompassing risk assessments



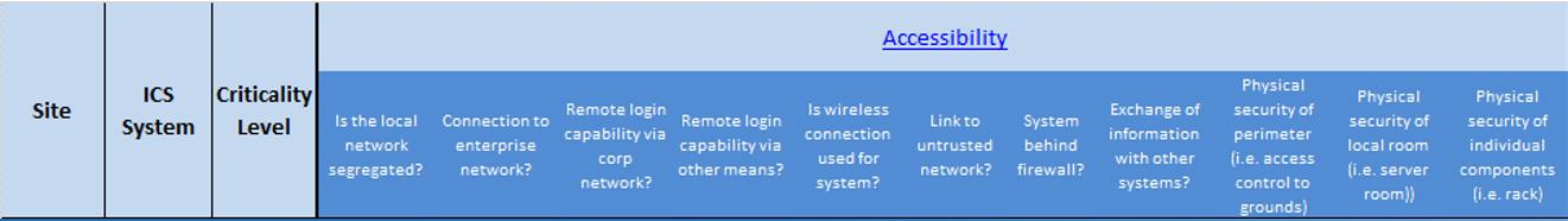
Site	ICS System	Criticality Level	Security Management									
			Roles and responsibilities (RACI)	Awareness and training	ICS inventory management	Change Management	Incident management	Acquisition	Vendor/contractor management	External device management	Indentification and access management	Risk assessment



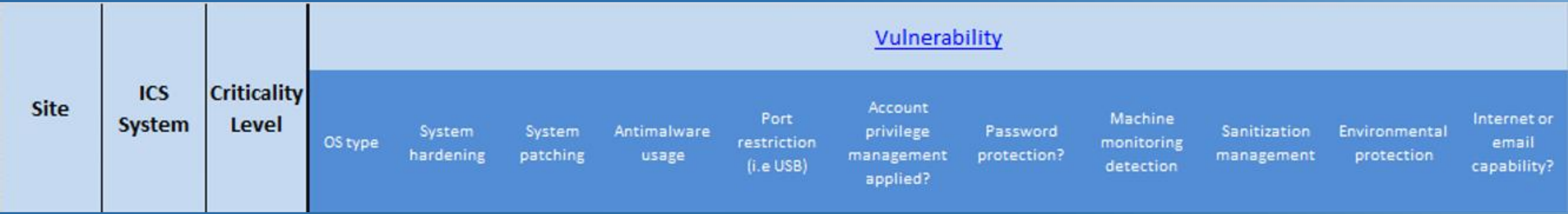
Site	ICS System	Criticality Level	Recoverability								
			Spare parts management	Application/ Software backup	Backup frequency	Backup management	System restore test	Estimated system recoverability	Redundancy management	Contingency planning	Energy backup management

How to deal with this dogma?

- All encompassing risk assessments



Site	ICS System	Criticality Level	Accessibility										
			Is the local network segregated?	Connection to enterprise network?	Remote login capability via corp network?	Remote login capability via other means?	Is wireless connection used for system?	Link to untrusted network?	System behind firewall?	Exchange of information with other systems?	Physical security of perimeter (i.e. access control to grounds)	Physical security of local room (i.e. server room))	Physical security of individual components (i.e. rack)

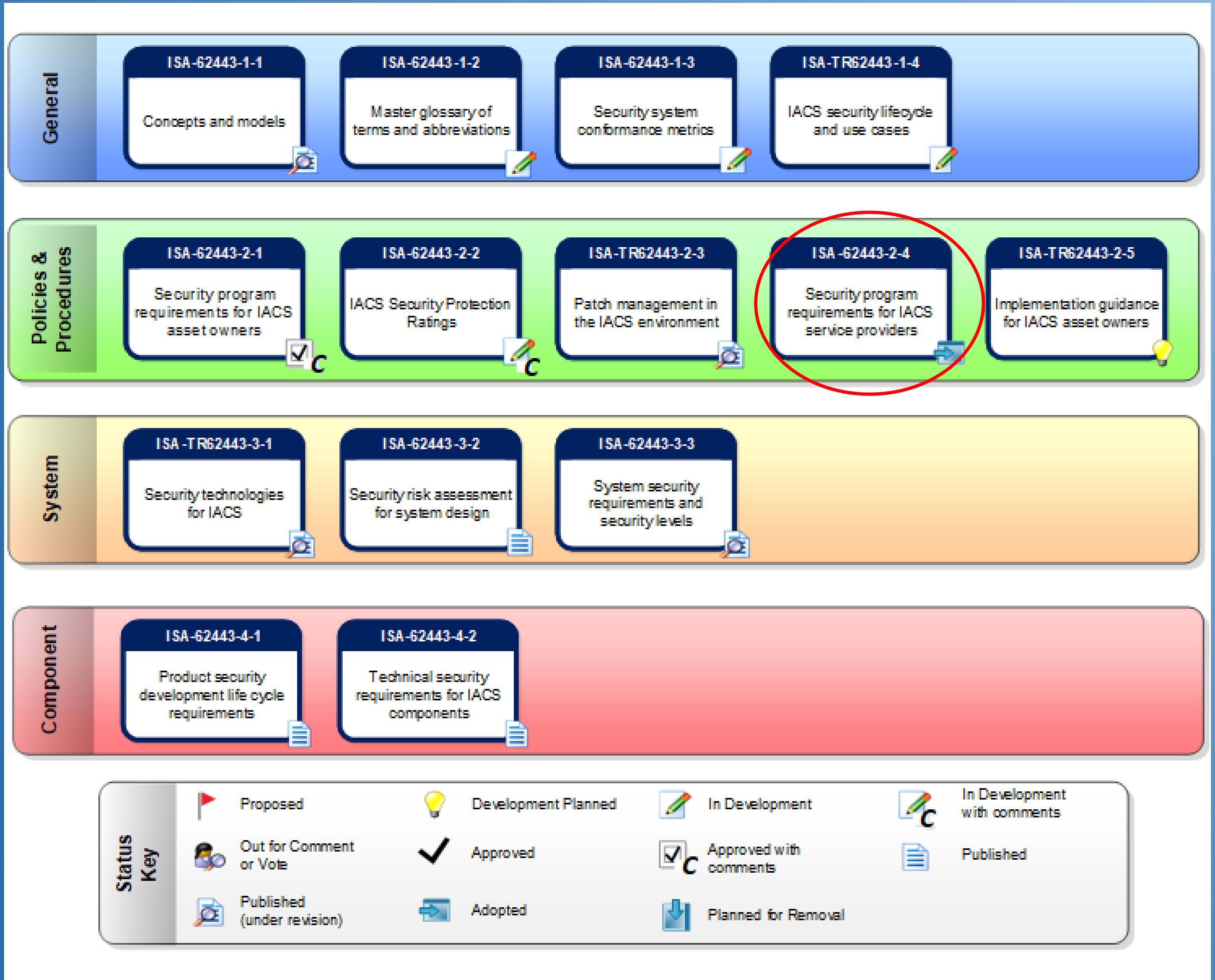


Site	ICS System	Criticality Level	Vulnerability										
			OS type	System hardening	System patching	Antimalware usage	Port restriction (i.e USB)	Account privilege management applied?	Password protection?	Machine monitoring detection	Sanitization management	Environmental protection	Internet or email capability?

How to deal with this dogma

Security Requirements

- Set
- Challenge Vendor(s)
- Verify claims
- Test claims



General

ISA-62443-1-1 Concepts and models

ISA-62443-1-2 Master glossary of terms and abbreviations

ISA-62443-1-3 Security system 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

ISA-62443-2-2 IACS Security Protection Ratings

ISA-TR62443-2-3 Patch management in the IACS environment

ISA-62443-2-4 Security program 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 for system design

ISA-62443-3-3 System security requirements and security levels

Component

ISA-62443-4-1 Product security development life cycle requirements

ISA-62443-4-2 Technical security requirements for IACS components

Status Key

Proposed

Development Planned

In Development

In Development with comments

Out for Comment or Vote

Approved

Approved with comments

Published

Published (under revision)

Adopted

Planned for Removal

How to deal with this dogma

- Security Testing Strategy

- Regular testing on existing environment (while keeping safety in mind)
- Security FAT/SAT on ALL new/upgraded equipment
- Have your “own” testing equipment or adversary emulation

Always include logical, human & physical

Play the “what if…” game …

How to deal with this dogma

- Security Testing Strategy

Some will say “never in live environments”

Why not … ? Just make sure you don’t trip anything …

During FAT/SAT testing

Do “Full Monty” tests …
… include active scanning

During ~~revisions~~

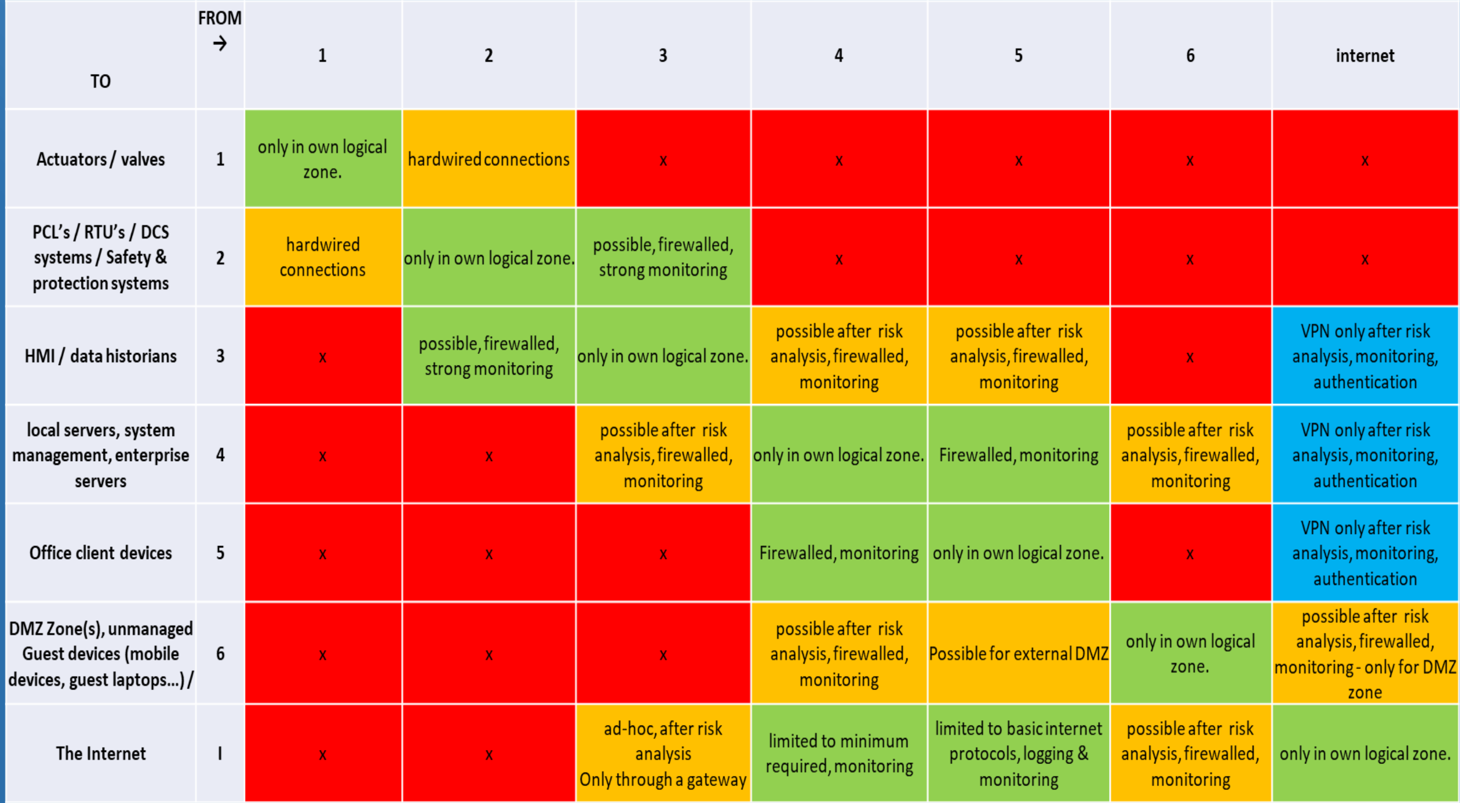
General meetings

All doors open …
Nobody to be seen …
(often) passwords all over the place …
Systems unlocked …

How to deal with this dogma

- Mitigating measures

- Network segmentation & zoning
- Hardening & Patching
- Physical security
  - Including presence monitoring



TO	FROM →	1	2	3	4	5	6	internet
Actuators / valves	1	only in own logical zone.	hardwired connections	x	x	x	x	x
PCL's / RTU's / DCS systems / Safety & protection systems	2	hardwired connections	only in own logical zone.	possible, firewalled, strong monitoring	x	x	x	x
HMI / data historians	3	x	possible, firewalled, strong monitoring	only in own logical zone.	possible after risk analysis, firewalled, monitoring	possible after risk analysis, firewalled, monitoring	x	VPN only after risk analysis, monitoring, authentication
local servers, system management, enterprise servers	4	x	x	possible after risk analysis, firewalled, monitoring	only in own logical zone.	Firewalled, monitoring	possible after risk analysis, firewalled, monitoring	VPN only after risk analysis, monitoring, authentication
Office client devices	5	x	x	x	Firewalled, monitoring	only in own logical zone.	x	VPN only after risk analysis, monitoring, authentication
DMZ Zone(s), unmanaged Guest devices (mobile devices, guest laptops…) /	6	x	x	x	possible after risk analysis, firewalled, monitoring	Possible for external DMZ	only in own logical zone.	possible after risk analysis, firewalled, monitoring - only for DMZ zone
The Internet	I	x	x	ad-hoc, after risk analysis Only through a gateway	limited to minimum required, monitoring	limited to basic internet protocols, logging & monitoring	possible after risk analysis, firewalled, monitoring	only in own logical zone.

How to deal with this dogma

- Mitigating measures

- (network) monitoring
  - Know what is going on in your environment
  - Do not rely on only 1 tool/product though

How to deal with this dogma

- Work with your vendor

~~Do NOT~~ trust your supplier/integrator *but verify*

As vendor/integrator

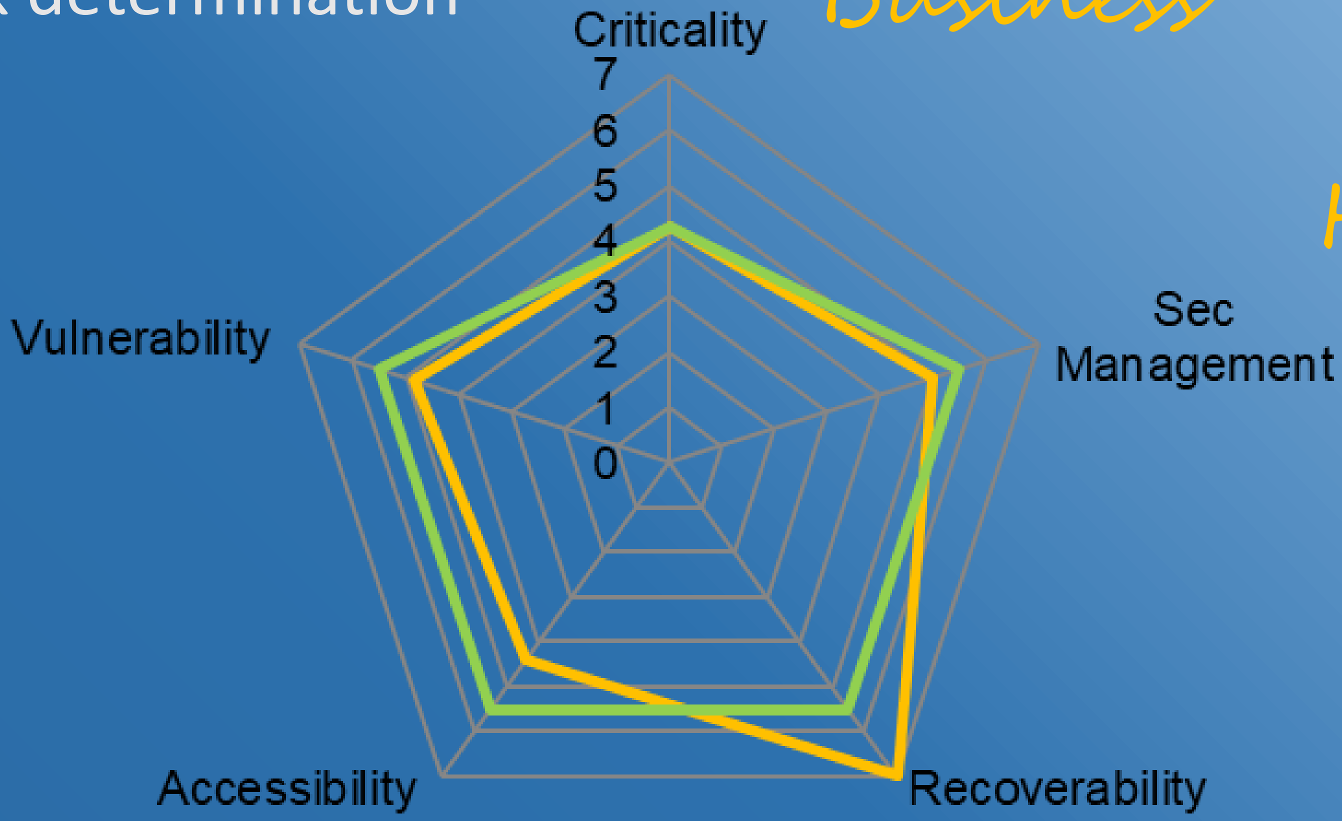
⇒ be ready to prove your solution security (without hiding things)

⇒ IEC62443 helps

Security is no longer a feature …

How to deal with this dogma?

- Residual risk determination



Business

Human

Logical

Logical & Physical

Physical & human

How to deal with this dogma?

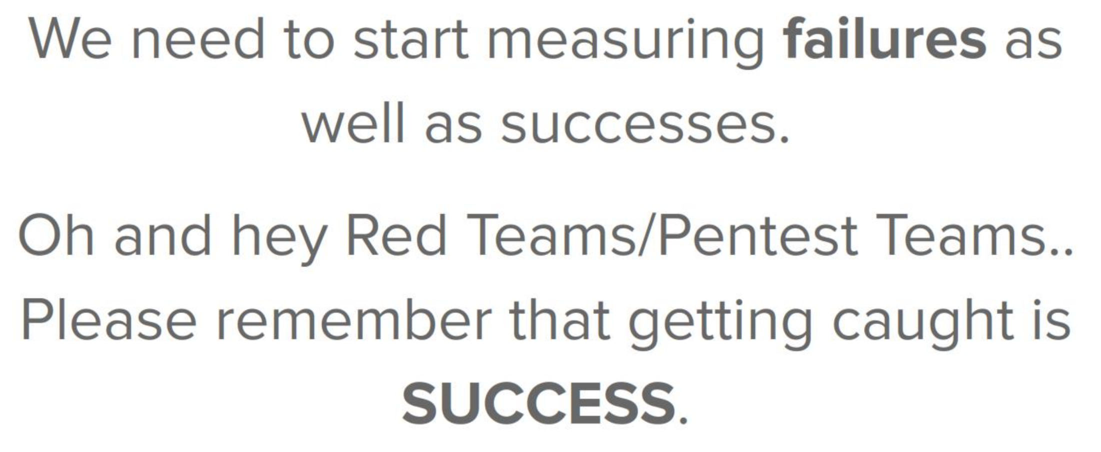
- People / Staff

- Whatever tools you use, people using/operating them are key
- > 1.5 FTE to operate cybersecurity solutions
- < 0.5 FTE = 0 FTE …

Human

Start looking at the bigger picture …

But also … Back to basics …



We need to start measuring **failures** as well as successes.

Oh and hey Red Teams/Pentest Teams.. Please remember that getting caught is **SUCCESS**.

@mubix, BruCon 2019

Dieter Sarrazyn

@dietersar

https://www.linkedin.com/in/dietersarrazyn/

https://secudea.be