Scada/ICS Security

some experiences from the field

Dieter Sarrazyn

dieter.sarrazyn@toreon.com

@dietersar

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

Introduction

Introduction

Why?

Business impact

Human safety

Environmental

Economical

Introduction

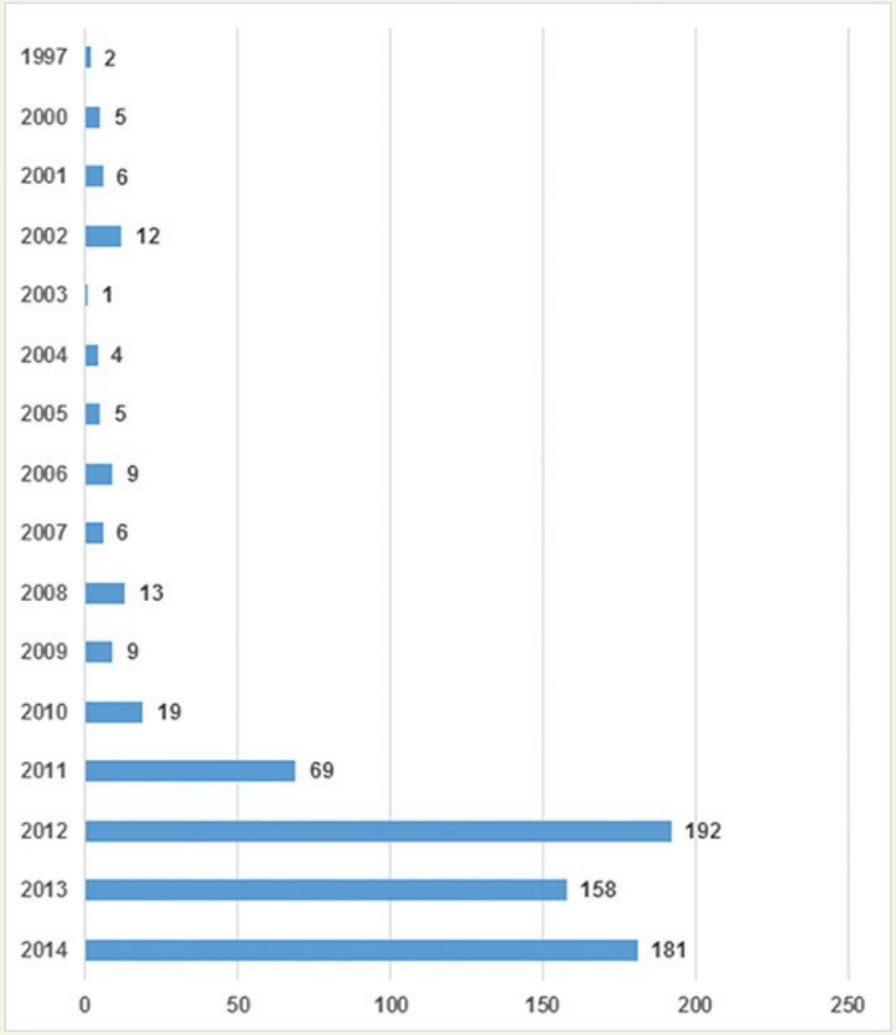
Business Trends

- Increased Industrial Control Systems connectivity (corporate networks, internet...)
- Increasing need for real-time business information
- Increasing need for faster operational response
- Further consolidation of small systems
- Security as a feature
- Further IT & OT integration

Introduction

Vulnerability Trends

- Aging infrastructure
- Transformation from proprietary, isolated systems to open architectures and standard technologies
- Decreasing end user knowledge and awareness due to the use of standard embedded systems platforms
- Increased research on ICS weaknesses and vulnerabilities
- Patch management is more difficult (lack of test environments, lacking support of vendors)



Source: http://blog.ptsecurity.com/2016/10/industrial-control-system-security-in.html

Introduction

Cyber Threats/Attack trends

Title	Year	Industry Type	Country	Brief
Page 1 of 9 pages **1** 2 3 > Last ›				
German Steel Mill Cyber Attack	2014	Metals	Germany	
Russian-Based Dragonfly Group Attacks Energy Industry	2014	Power and Utilities	United States	
Public utility compromised after brute-force hack attack, says Homeland Security	2014	Power and Utilities	United States	
After 'Godzilla Attack!' U.S. warns about traffic-sign hackers	2014	Transportation	United States	
U-2 spy plane caused widespread shutdown of U.S. flights: report	2014	Transportation	United States	
Virus shuts down county highway department network	2013	Transportation	United States	
Signal problems cause train delays	2013	Transportation	United States	
Computer Glitch Leads to Shutdown of Nuclear Reactor	2012	Power and Utilities	United States	
U. S. Power Plant Infected With Malware	2012	Power and Utilities	United States	

http://www.risidata.com/Database/event_date/desc

Introduction

Questions that you may receive

“Is this really an issue?”

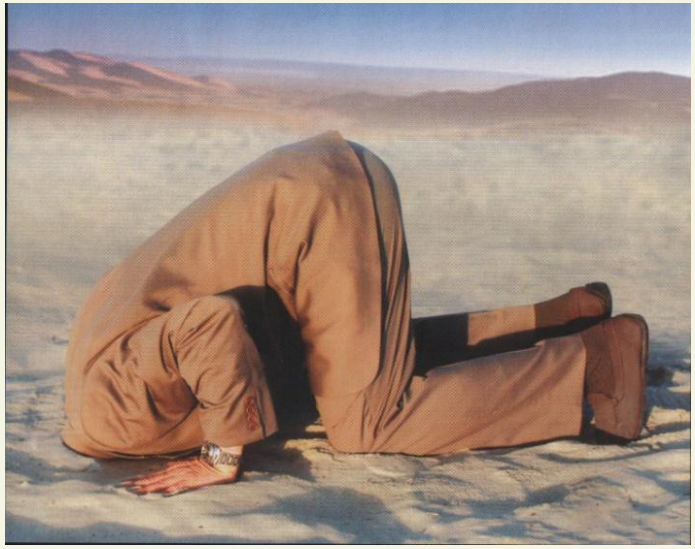
“We can change this in the next product upgrade.”

“Is this really worth the investment ?”

“What are the chances…. this has never happened before…”

“We aren’t connected to the internet”

…



SCADA Top 10

A top 10 of things heard/noticed/encountered in scada environments

Top 10

Nr. 10 – hardening fun

“Of course we can harden your systems…
just buy a new system”

“We tested the hardening in our test environment”

(but forgot to deploy it in production …)

Top 10

Nr. 9 – viri & malware

Suppliers don’t always deliver DCS systems virus free

(even base images contain malware sometimes ...)

USB sticks of supplier/vendor engineers are not always malware free ...

(and they use these with different customers...)

Top 10

Nr. 8 – no internet …

“We don’t need security, there is no connection with the internet”

(but vendor xyz is performing remote maintenance)

Top 10

Nr. 7 – desktop restrictions … really?

“Why aren’t we allowed to use the admin account to start that software/service?

It’s a restricted desktop”

Top 10

Nr. 6 – security through obscurity

“I know the security isn’t in order,

but nobody told me
you guys where coming”

(you referring to the ones testing security)

Top 10

Nr. 5 – port/vulnerability scanners ...

Automated scanners versus ICS/SCADA

(“fun” as attacker but certainly not a good combination...)

Top 10

Nr. 4 – network bridges ...

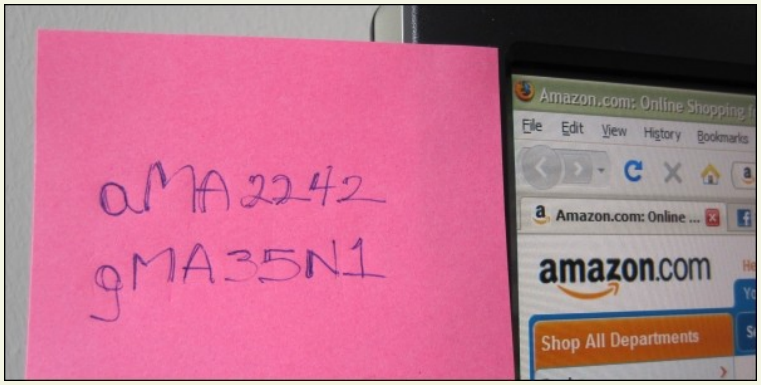
“we would like this system to have multiple interfaces connected to these different networks”

(question coming after firewalls came along ...

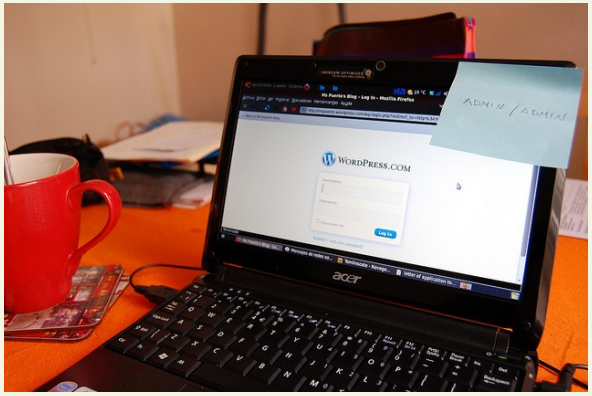
Zoning concept hasn’t sipped through yet ...)

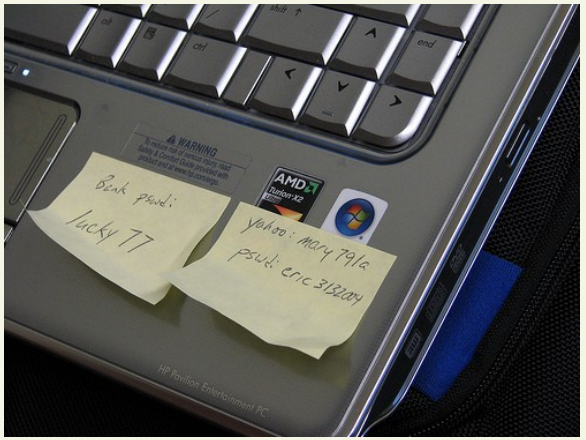
Top 10

Nr. 3 – passwords …



“Yes, we do password management”





Top 10

Nr. 2 – air gap …

“An air gap will solve all our problems”

Ok … but how do you transfer files/info to/from those systems? …

“uhm… by USB stick”

Top 10

Nr. 1 – not in objectives

“Security is not in my objectives …”

Standards (overview)

Industrial Security Standards

- NERC CIP – Electric
- CIDX / ACC – Chemicals
- ISA 99 (IEC-62443)
- NIST 800-82 Rev2
- AGA 12 – Natural Gas
- API – Oil & liquids
- IAEA NSS17 – Nuclear

- Cybersecurity framework for critical infrastructure systems

Industrial Security Standards

Compliancy to a standard <> security

it's just a start ...

(possible) Approach

How the security level can be increased & maintained.

How to create awareness.

Approach

Build a team

Approach

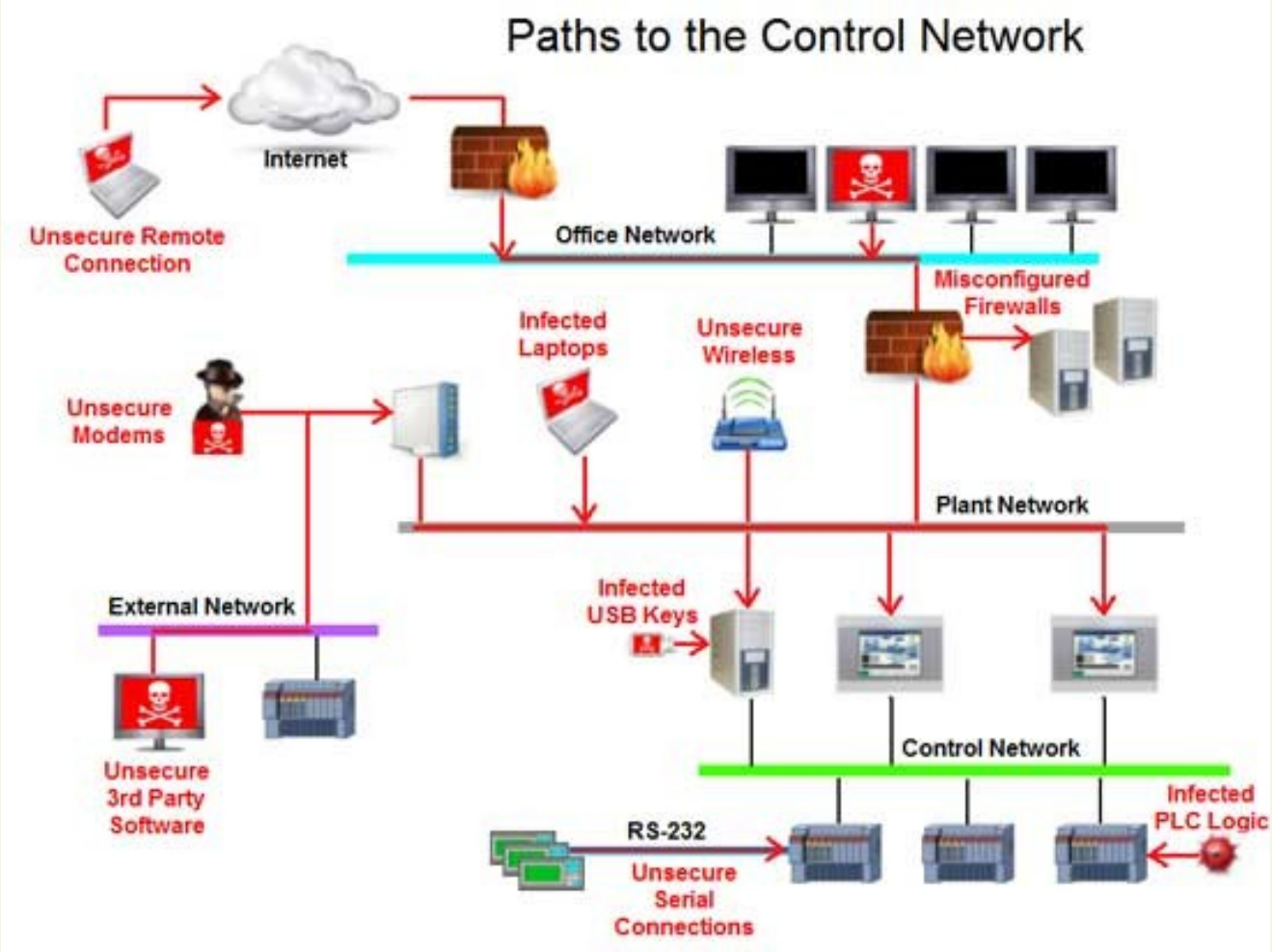
Inventory

Build a comprehensive inventory of the SCADA/ICS environment

- Find all network connections
  - Modem
  - Wifi
  - 3rd party partner connections
- Perform a physical walkthrough
  - Check for unprotected devices
  - Check for unlocked systems
  - Check for password indications
- Identify used Operating Systems
  - Include patch level
  - Include installed software

Approach

Inventory – access paths



Source: http://program-plc.blogspot.be/2016/09/easy-methods-to-remote-hmiscada-users.html

Approach

Verify security levels - how

- Penetration testing
- Perform Wifi walks/drives/…
- Perform physical walkthroughs
- FAT/SAT testing
- Other things to verify
    - Is hardening applied?
    - How are applications started? As Admin?
    - Communication between applications? Cleartext?
    - Can you “break out” of the “operator jail”?

Approach

Verify security levels - when

When to test?

- Initial baseline security test
- Every X months (to show improvements)
- Before implementation/deployment new product (FAT/SAT testing)

Unannounced “spot checks” (wifi, external links, physical walkthroughs…)

Approach

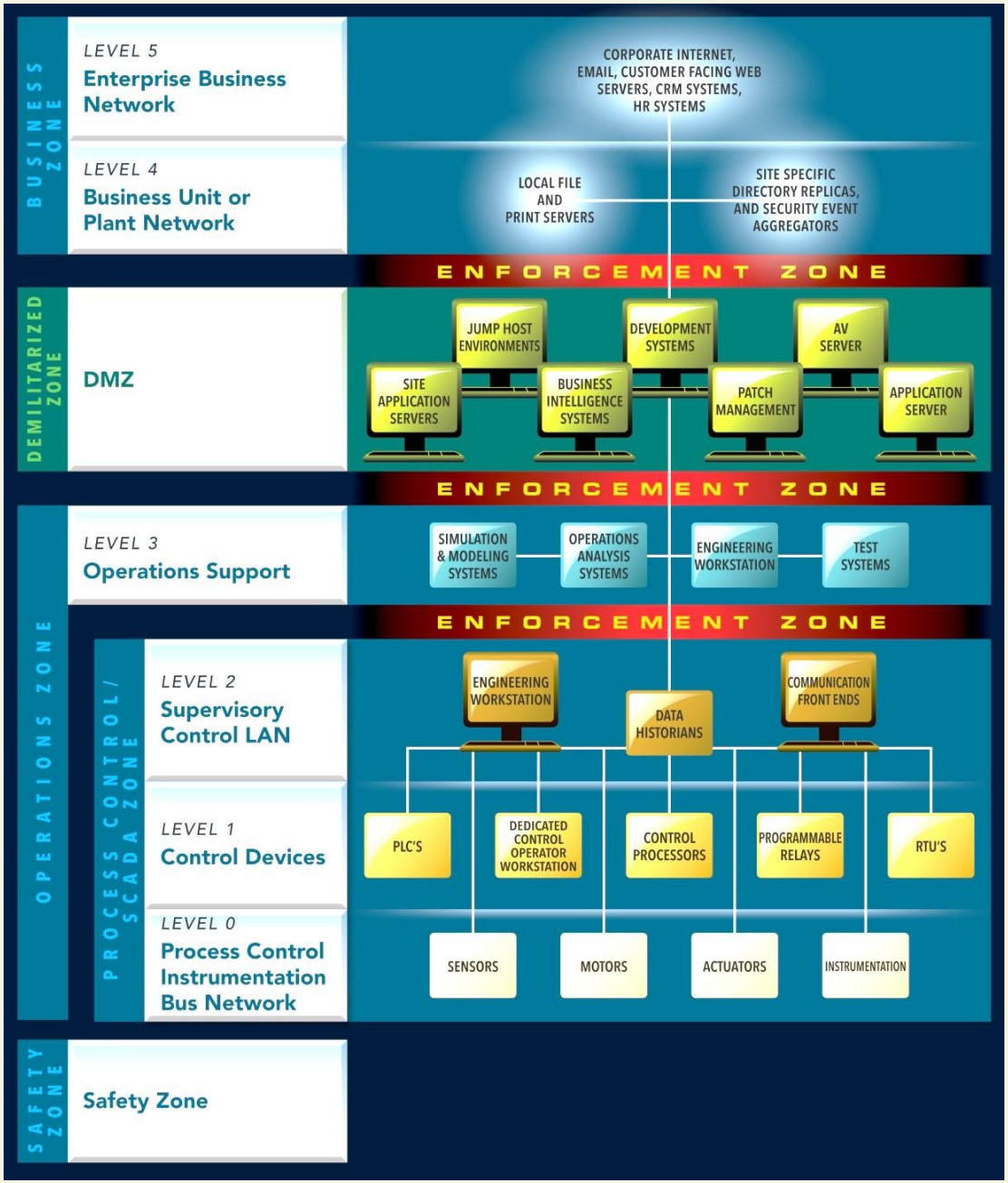
Verify Security levels - where

Where to test?
… safely ...

All testing ok

Take Care !!

“Forbidden zone”



Sources:
http://www.iebmedia.com/index.php?id=8460&parentid=74&themeid=255&showdetail=true
https://www.sans.org/industrial-control-systems/resources

Approach

Create awareness, get trust & buy-in

Most important rule => ***Talk to people***

- Vendors need to know what you are expecting
  - Takes time & effort

- Personnel (Management staff, I&C people …)
  - Raise awareness
  - Help them (also with non-scada related things)

Approach

SCADA/ICS Security governance

Security requirements for (SCADA) suppliers

- Should be mandatory for every new project being ordered
- Can be introduced gradually within existing environments
- (former) WIB document, now part of IEC 62443

Create necessary Security policies

- Incident Handling/Response
- Wifi & network usage
- Password management
- USB usage (stick/drive)
  - How to perform data transfer?
  - Antivirus checking before using/connecting it to systems

Approach

Network architecture changes

Get rid of all those (unprotected) DSL lines …

Implement a centralized remote maintenance system

- For internal personnel
- For external personnel

Have your process networks firewalled …

Approach

Network architecture changes

But first…

create a Zone concept

- Zone concept policy
- Define security levels
- Define an access matrix

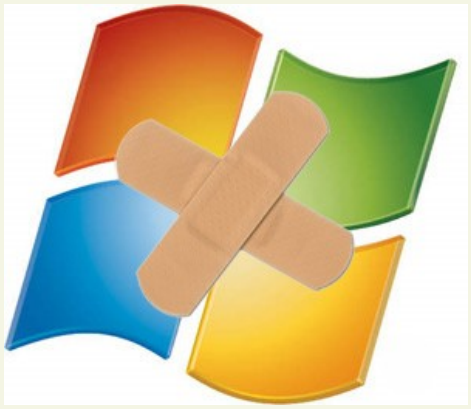
Approach

Network architecture changes – access matrix

TO \ FROM		1	2	3	4	5	6	internet
critical control systems - PLC's, RTU's, field devices ...	1	only in own zone. Constant check of active MAC addresses	x	x	x	x	x	x
critical monitoring and control systems - HMI level	2	logical diode (transport layer - TCP)	only in own zone. Check of MAC connected to gateway	only when urgent - ad hoc setup, after risk analysis	only when urgent - ad hoc setup, after risk analysis	only when urgent - ad hoc setup, after risk analysis	only when urgent - ad hoc setup, after risk analysis	only when urgent - ad hoc setup, after risk analysis
Process environment supporting systems	3	controlled by signal diode - only out, no in - possible after risk analysis	logical diode (transport layer - TCP)	V	possible, strong monitoring & authentication	possible on demand - ad hoc setup	possible on demand - ad hoc setup	possible on demand - ad hoc setup
trusted and controlled systems and servers, under ICT control	4	controlled by signal diode - only out, no in - possible after risk analysis	logical diode (transport layer - TCP) - possible after risk analysis	possible after risk analysis	V	monitoring and IDS, no firewalling	VPN	VPN
Users and unmanaged systems	5	x	x	possible after risk analysis	monitoring and IDS	V	x	VPN
guests, only internet access	6	x	x	x	x	possible for external dmz	V	VPN
internet	I	x	x	ad hoc, after risk analysis	limited to basic internet protocols, logging	limited to basic internet protocols, logging	limited to basic internet protocols, logging	V

Approach

System changes – patching & hardening



Operating systems
3rd party applications

Every x months

Operating systems
Network systems
Applications (e.g. OPC)

Approach

Monitoring

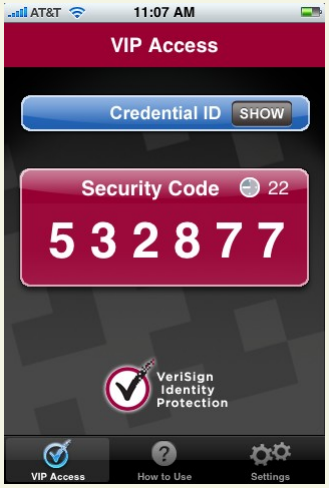
IDS / IPS functionality (make sure you don’t create a DOS)

Central Event monitoring & alerting => SIEM

System monitoring (HIDS/HIPS)

Approach

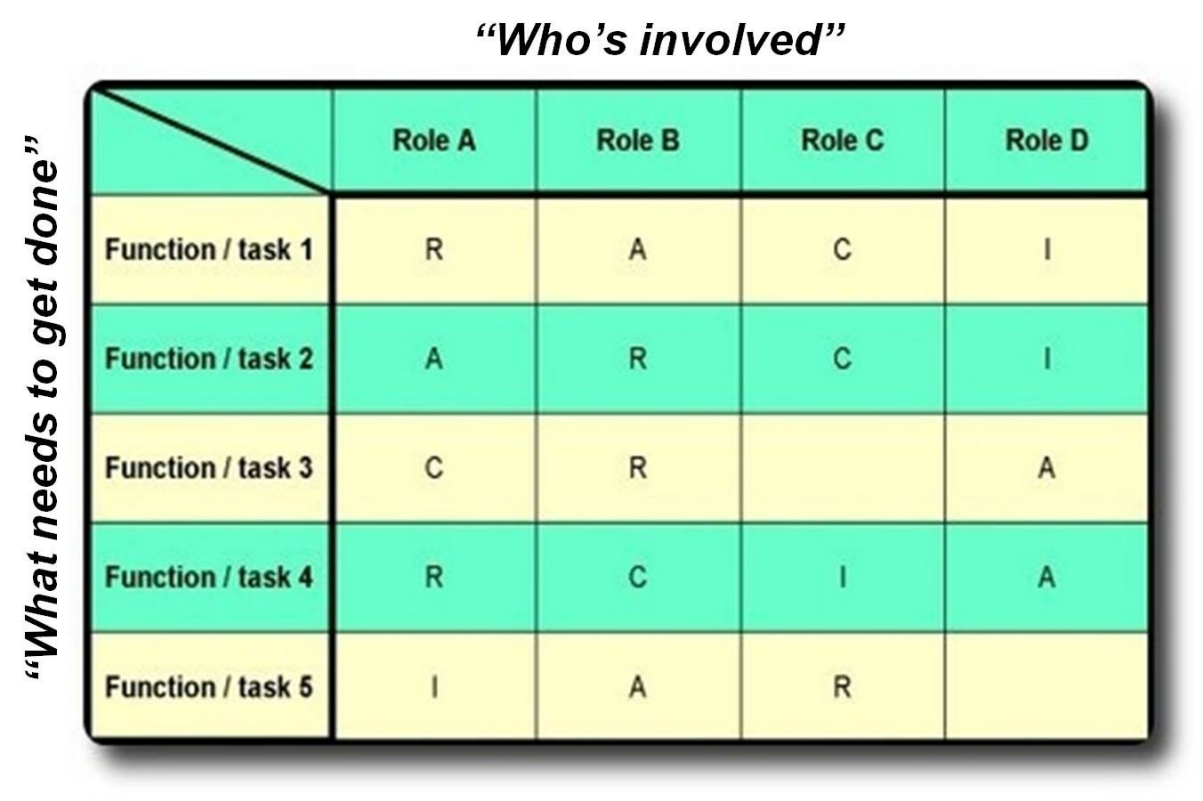
Authentication (logical & physical)



Combine several methods for more secure zones

Approach

Responsibilities – RACI matrix



	Role A	Role B	Role C	Role D
Function / task 1	R	A	C	I
Function / task 2	A	R	C	I
Function / task 3	C	R		A
Function / task 4	R	C	I	A
Function / task 5	I	A	R	

But most important:

Put security in the objectives/KPI's of people

Approach

Set realistic goals

Questions?

Dieter Sarrazyn (dieter.sarrazyn@toreon.com)

@dietersar

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