Security By Design

Industrial Systems Cyber Security in Mind

By *Shaker S. Hashlan*

المملكة العربية السعودية
وزارة المياه والكهرباء
MINISTRY OF WATER & ELECTRICITY

ارامكو السعودية
Saudi Aramco

Saudi Electricity Co.

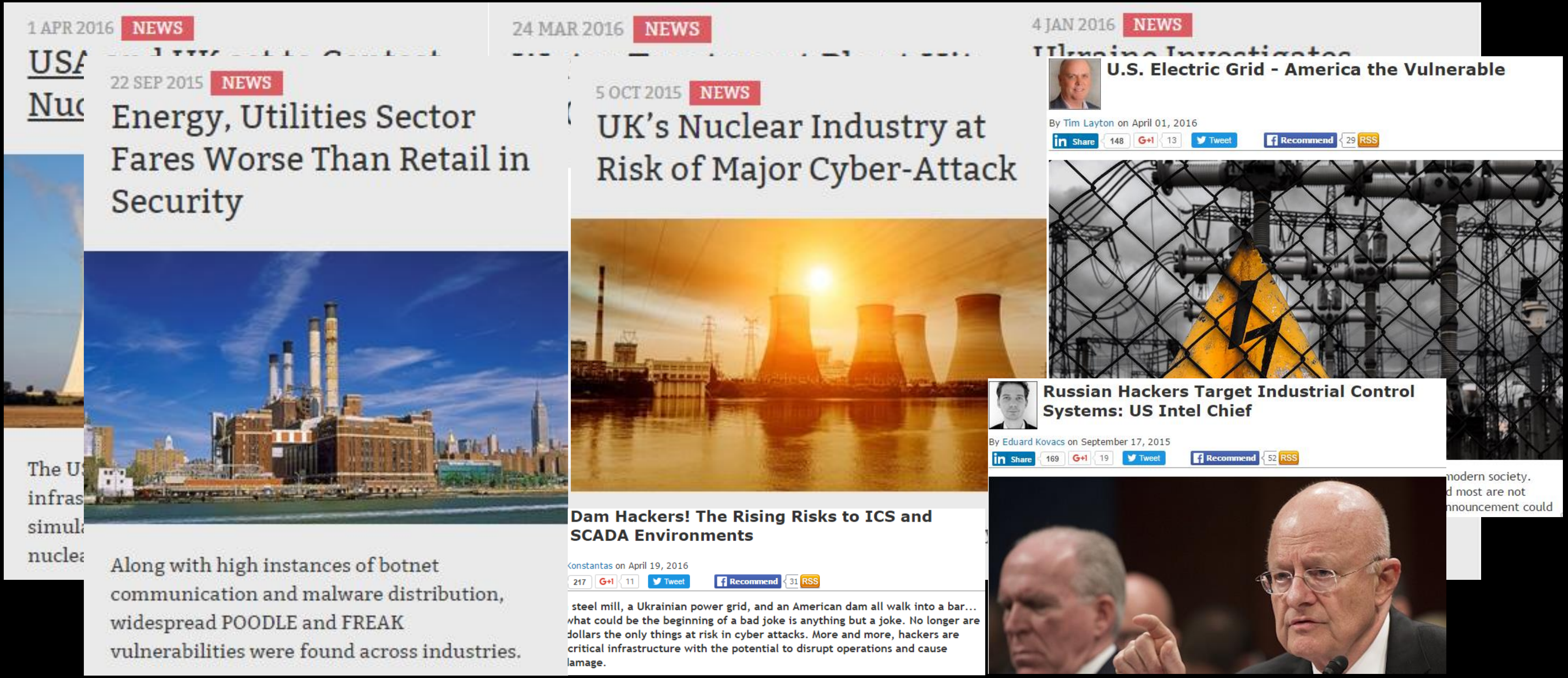
>60 Power Plant
>52 GW

الشركة السعودية للكهرباء
Saudi Electricity Company

Things to get out of this:.

- What is Cyber Security for Industrial Control System?
- Controls Systems and OT
- Cyber Threats to the Critical Infrastructure Control Systems
- Cyber Security Complaisance
- Critical infrastructure and Security Practices

ICS in The News



1 APR 2016 NEWS

USA

Nuc

The U
infras
simul
nuclea

24 MAR 2016 NEWS

4 JAN 2016 NEWS

22 SEP 2015 NEWS

Energy, Utilities Sector Fares Worse Than Retail in Security

Along with high instances of botnet communication and malware distribution, widespread POODLE and FREAK vulnerabilities were found across industries.

5 OCT 2015 NEWS

UK's Nuclear Industry at Risk of Major Cyber-Attack

Dam Hackers! The Rising Risks to ICS and SCADA Environments

Konstantas on April 19, 2016

217 G+1 11 Tweet Recommend 31 RSS

steel mill, a Ukrainian power grid, and an American dam all walk into a bar… what could be the beginning of a bad joke is anything but a joke. No longer are dollars the only things at risk in cyber attacks. More and more, hackers are critical infrastructure with the potential to disrupt operations and cause damage.

U.S. Electric Grid - America the Vulnerable

By Tim Layton on April 01, 2016

Share 148 G+1 13 Tweet Recommend 29 RSS

modern society.
d most are not
nnouncement could

Russian Hackers Target Industrial Control Systems: US Intel Chief

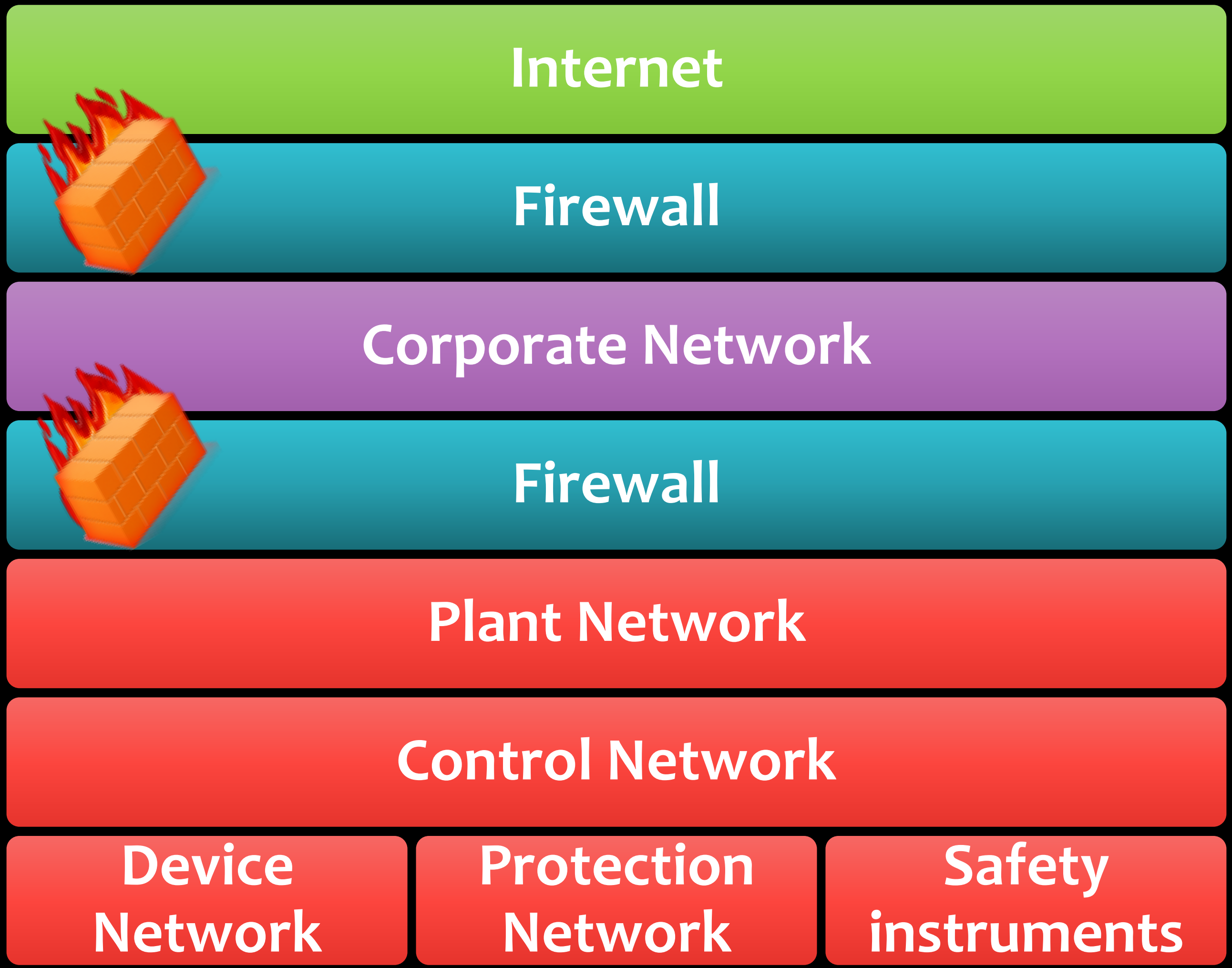
By Eduard Kovacs on September 17, 2015

Share 169 G+1 19 Tweet Recommend 52 RSS

What is it all about?

Controls System Security = Safety + Reliability:.

- Typical ICS Topology
- ICS security is a Mixture of cyber, Operational, and Industrial Protection practices that results in a secure system.



Internet

Firewall

Corporate Network

Firewall

Plant Network

Control Network

Device Network

Protection Network

Safety instruments

What is the worst that can happen:.

Security Basics:.

- You are never Perfectly Safe, You are never Perfectly Secure.
- All software can be compromised
- Security vs. Practicality
  - The only Secure computer is a Disconnected, Powered off one with armed guards on the door. What use is there for such computer, and even then it is not perfectly secure.

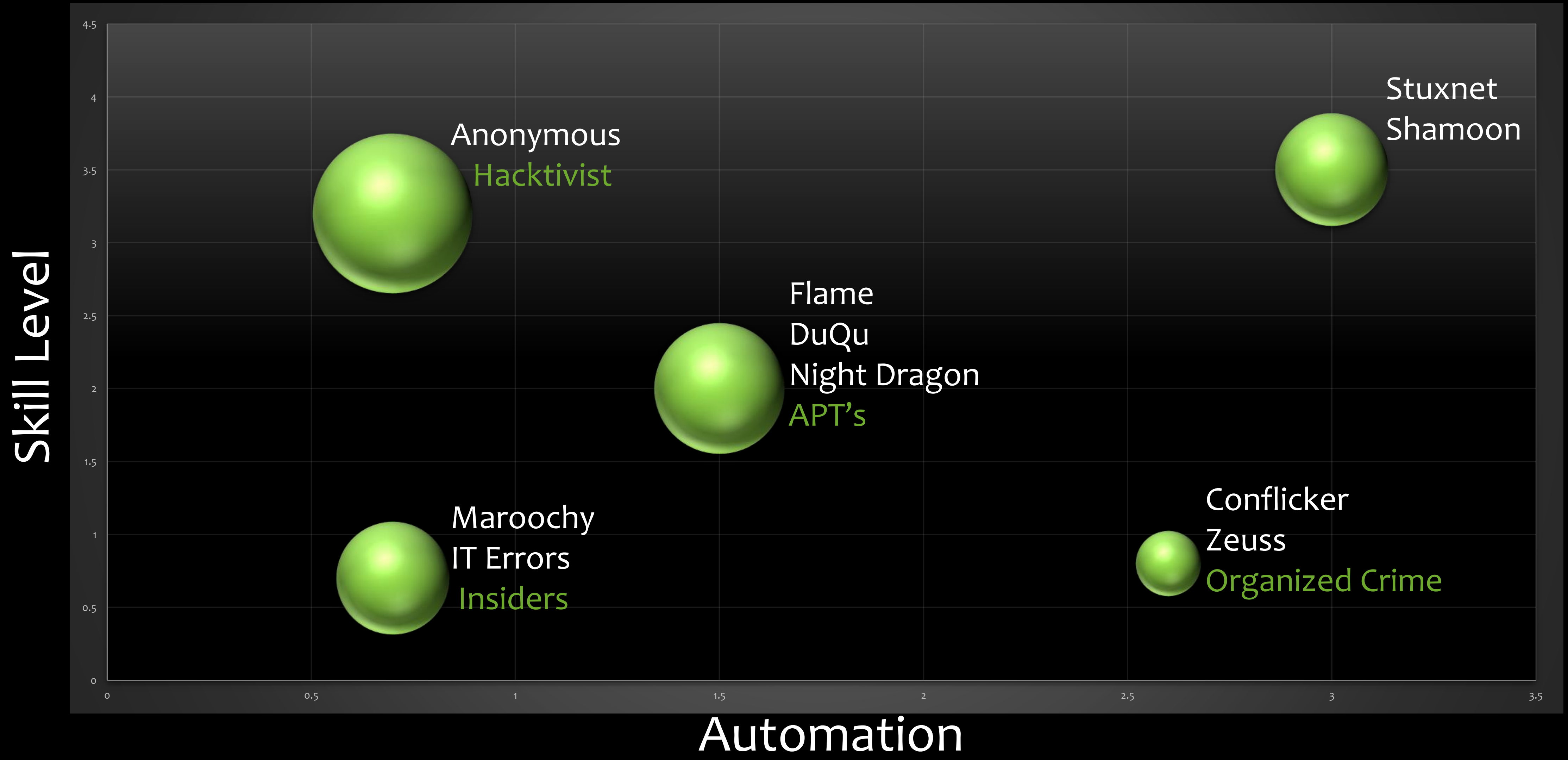
ICS Networks Drive and Risks:.

- Predictive maintenance,
- Inventory
- Just in Time Manufacturing,
- SAP/ERP Billing,
- Production Planning
- Centralized Support
- Etc…
- ICS must be connected to the corporate network that ultimately connects to the internet

Stuxnet:.

Created By:	????????
Targeted:	Critical Industrial and Infrastructure
Propagation Method:	Network Shared Folders, USB Mass Storage Drives
Estimated Casualties:	100,000 – 300,000 infected machines.
Resulting Effect:	Compromised Safety Systems

Threat Spectrum:.



Targeted Attacks:.

- Flame, DuQu, Night Dragon, Dragon Fly APT, Shamoon
- Trick users to provide info or provide a way of accessing the system
- Custom malware and RAT to create users or to escalate privileges.
- *ICS security Guidance does not address Targeted Attacks*

Safety, Reliability, Confidentiality:.

Attribute	Corporate IT	Control Systems
Scale	Large >100,000 devices	Small 100-500 devices
Priority	Confidentiality	Safety, Reliability
Objective	Data Theft	Sabotage
Exposure	Constant Exposure to the Internet	Exposed to Corporate IT
Equipment Lifecycle	3-5 Years	10-20 Years
Security Discipline	Speed / Aggressive Changes and stay ahead of the curve	Security is an aspect of Safety – Change control is important

ICS Engineering Culture

is Change Averse

Encryption:.

- All traffic is clear Text
- Protect your perimeter
- Once In, Concentrate on the Process

Nobody Really Uses Anti-Viruses:.

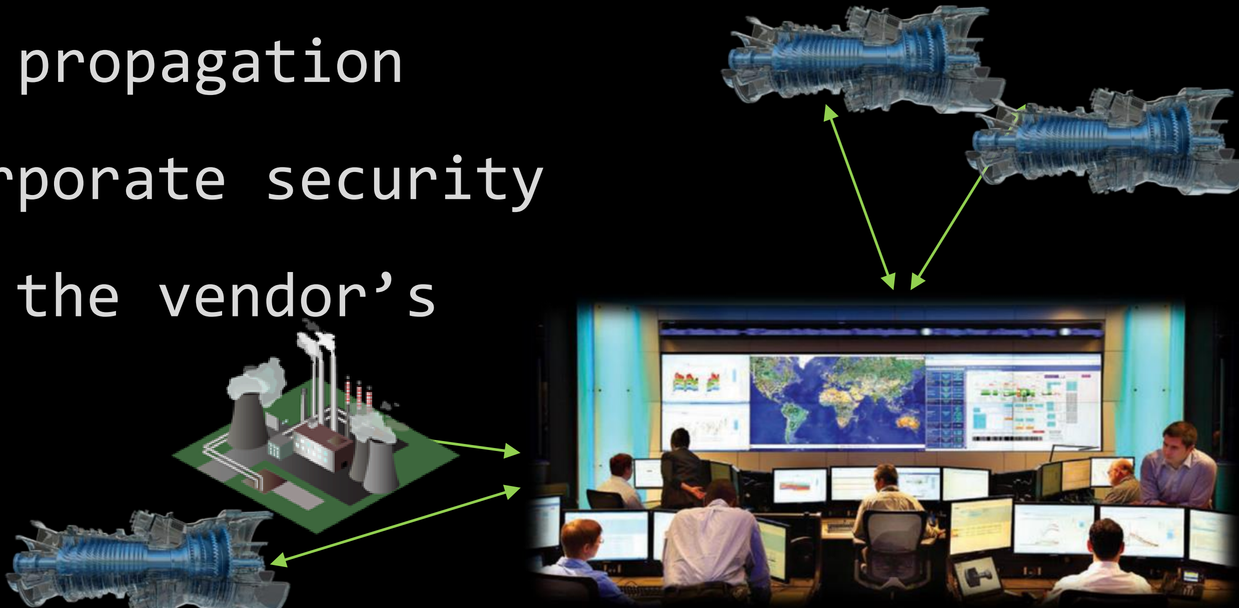
- Every signature update is a threat of “false positives” failure mistakenly diagnosing legitimate control system components as malware and quarantining them.
- Constant testing for safety of new signatures is costly
- ICS vendors estimate 90% of customers never update ICS signatures
- Corporate AV servers are attack channels into every ICS Host
- NERC-CIP and other standards mandate AV & signature updates but not frequency. Sites use very long frequency

Nobody Really Does Security Updates and Patches:.

- Updates are new Code. Is it safe?
- Constant testing for safety of new code is costly
- Corporate WSUS servers are attack vectors into most of the ICS systems
- Security update programs may be rolled out to plant-wide network
- Occasional spectacular failures effectively stall these programs at the ICS perimeter
- NERC-CIP & other standards mandate security update programs but not frequency sites use very long frequency.

Control Systems in the Claude

- Control vendors use it to monitor many costumer sites
- The system is configured to do the occasional remote access and control
- Exposed to attacks from the central site, customers or country
- Remote control attacks, viruses propagation
- Vendor connection bypass the Corporate security
- The systems security depends on the vendor’s implementation of security



> 100,000 Vulnerabilities

- Rough Potential vulnerabilities number calculation

50,000 * 2% * 10 * 3 * 5 * 0.75 = 112,500

- ICS security researchers confirm that they find 5-10 critical zero-day in the first few hours of examining every new ICS product
- ICS vendors are working on the problem, but it will be a long time before it is solved

Compliance vs Security:.

- Security is doing what you need to, in order to Protect your systems
- Compliance is doing what somebody told you to do, whether it is useful or not.
- Does it Matter to have Standards?

IEEE

IEC

NIST

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Is Security Handled in the Standards?

- No security
  - Complexity
  - Redundancy
  - Diversity

Application Control-WhiteListing:.

- Automatically maintain a list of all authorized executables and libraries
- Only allow recognized executables
- Zero days and early detection
- Include devices control capabilities
- In-memory protection
- Good fit for ICS
  - No Signature to update
  - Predictable execution cost

Physical Security:.

- Access Control
- Reduce risk of USB, CD/DVD R, Cell phone, networking, rogue laptops
- Entire ICS network must lie within physical security perimeter.
- Insider Threat

State of Practice:.

- **Leaders**: True Paranoia in dealing with ICS security
- **Misguided**: points of view between IT and ICS OT
- **Oblivious**: to the fact that “Air Gapped Systems” are NOT secure any more

Information Sharing:.

- Control Systems are complex, diverse, and control a huge number of IO’s
- Thinking like an Attacker, then how can these systems be attacked?
- Prompt sharing of information about attacks can prevent similar attacks
- Safe harbor laws to encourage information sharing
- This item will be more effective if attacks are detected promptly and have forensics teams and tools to analyze the attacks

CERT.sa
المركز الوطني الإرشادي لأمن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

verizon
2014 DATA BREACH INVESTIGATIONS REPORT

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

osvdb

Compensating Measures:.

- Enhance Safety Systems (from Safety to Reliability Risk) *
- Physical Security (if the system is within your facility)
- Device Control (Disable execution Removable Media)
- Anomaly based Intrusion detection (would it fit?)
- Whitelisting (NO Signatures)
- Device Firewalls (Less code, less to misconfigure, Simple)
- SIEM Solution (a SOC Technology) detection measure.
- Unidirectional Gateways
- Segregating the OT and the IT

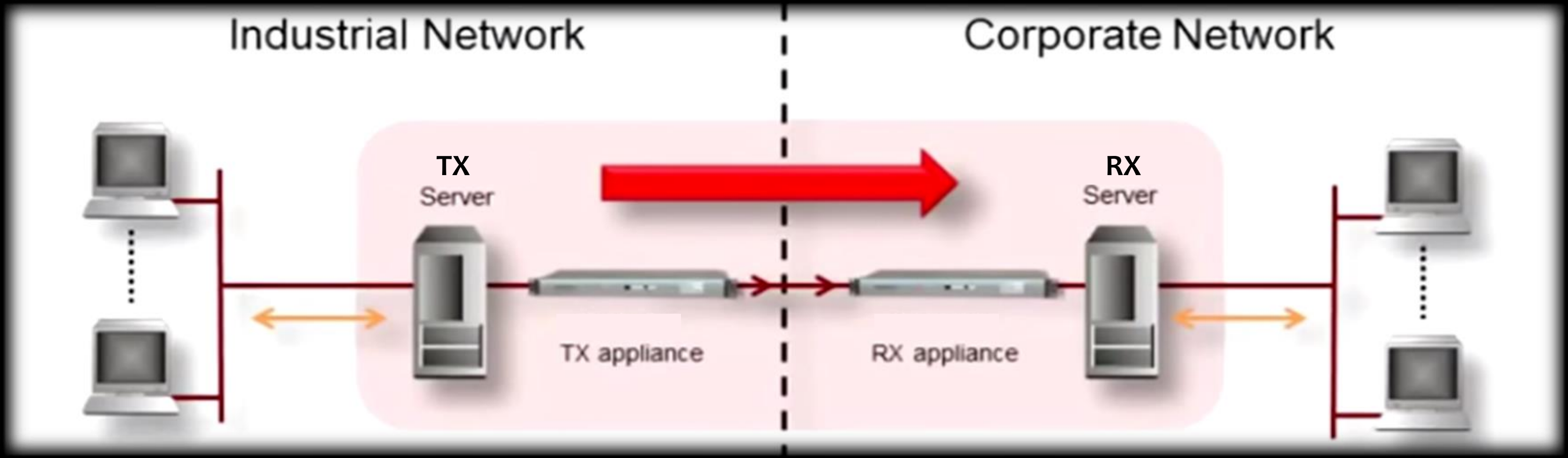
ICS Security :. *Final thoughts*

- Needs improvement
- Security = Safety + Reliability + ***Confidentiality + Integrity + Availability***
- ICS internals will Never be as secure as IT
- ICS perimeter security shall be improved constantly
- Communicating the Risk to management to invest in Cyber Security
- A lot of work is yet to be done

> Thank you for Your Time

Unidirectional Gateways

- Segregate the Operations Network (Plant’s Network)
- Unidirectional Gateways (or any containment technology) should be the only way out of the Plant’s Network.
- Limit Site to Site threats using firewalls.
- Provide Isolation yet maintained a Centralized management architecture



Simpler is Better:.

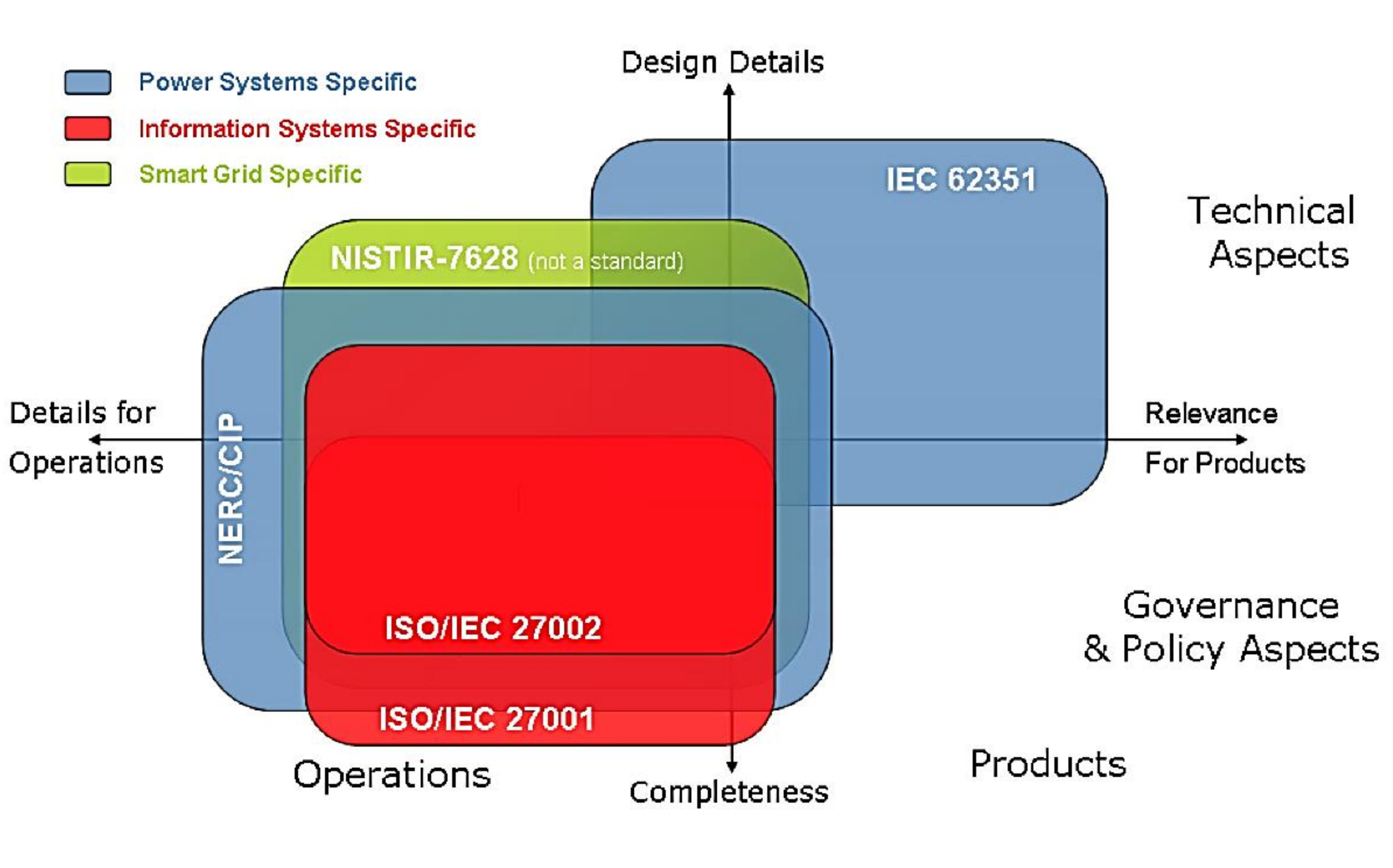
- Install Device Firewalls without the extra bells and whistles = fewer bugs to deal with.
- Implementing Anomaly-Based Network Intrusion Detection. Learns what is normal and what is not.
- The use of Statistics-based traffic flow analysis
- Adopt the SIEM (Security Information & Event Management) to obtain SOE, logs and visibility in to the environment and integrate it with cloud-based Threat Intelligence.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

IEC

ISO



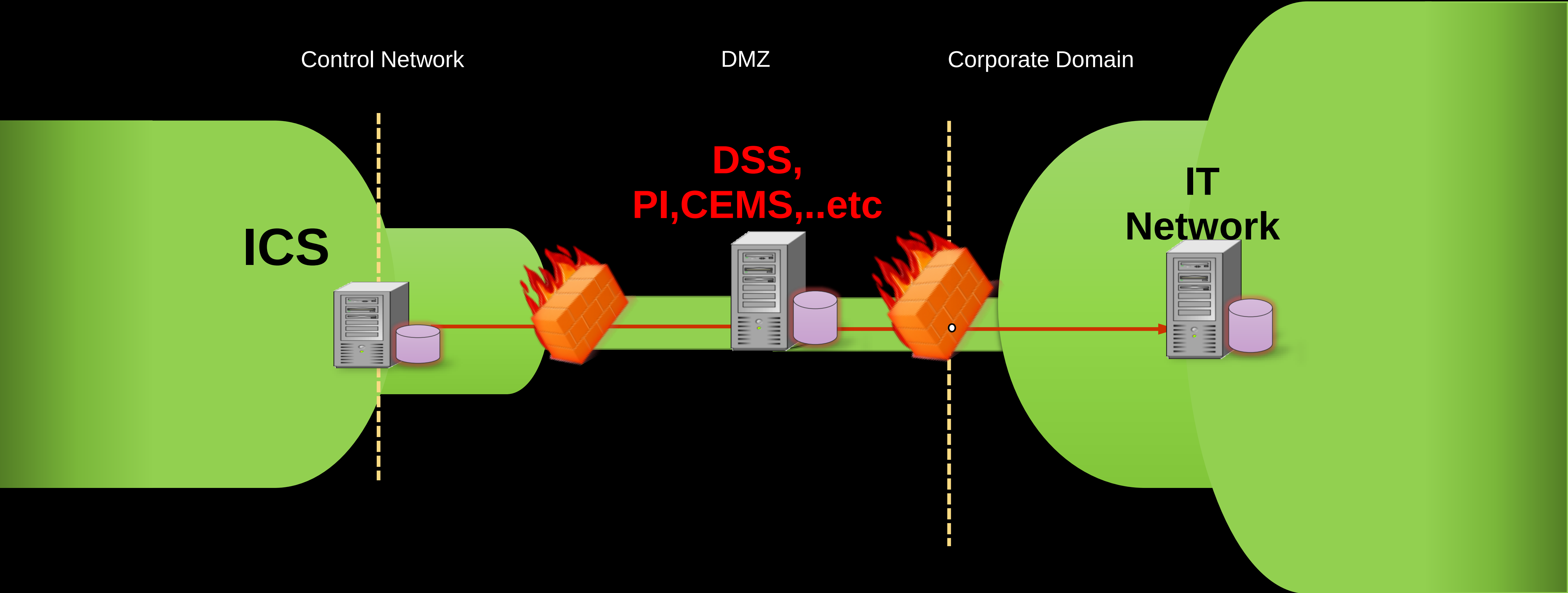
🟦 Power Systems Specific

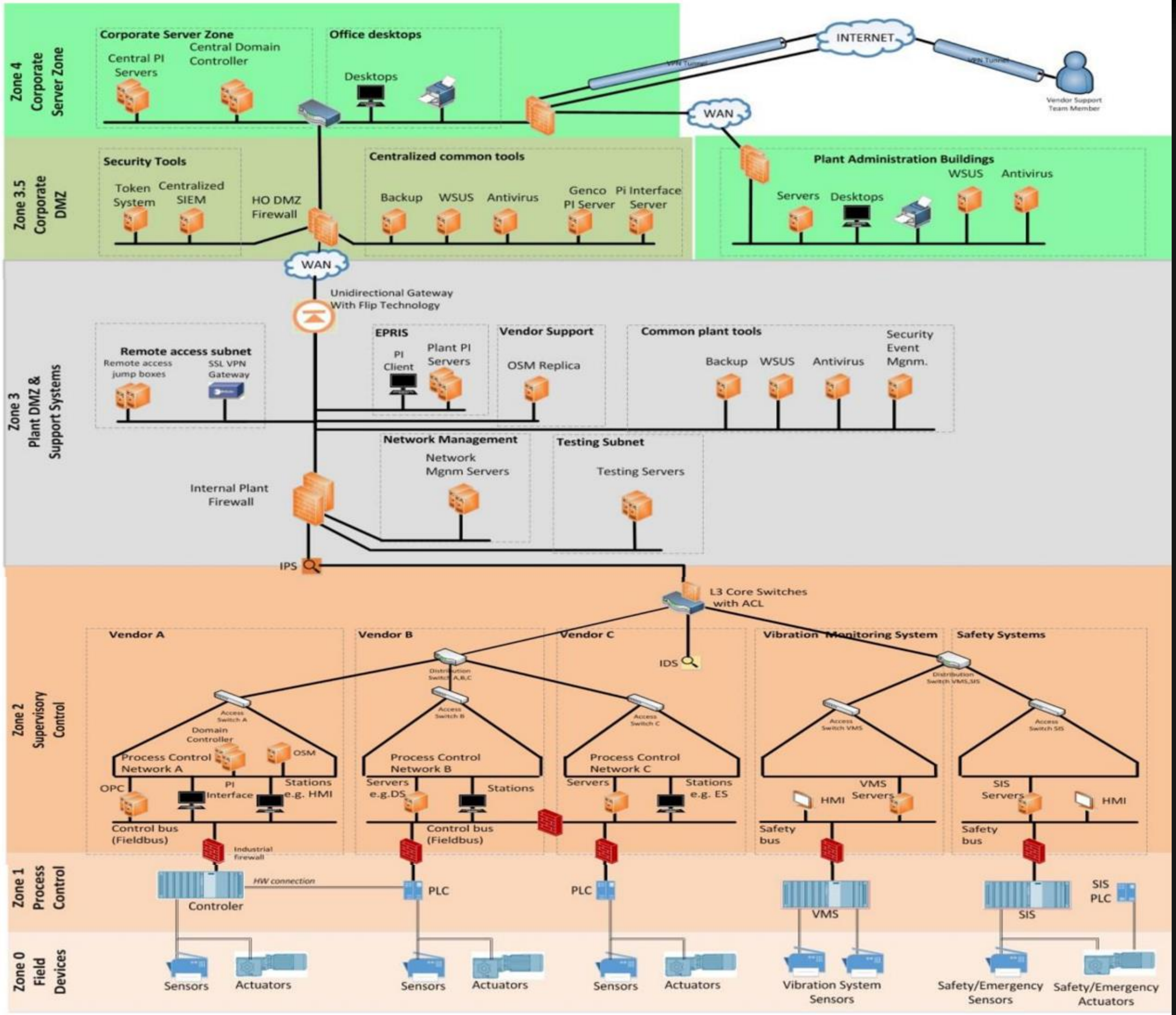
🟥 Information Systems Specific

🟩 Smart Grid Specific

Rules and Responsibilities:.

- Boarders of jurisdiction a Group with a set of responsibilities are to be initiated

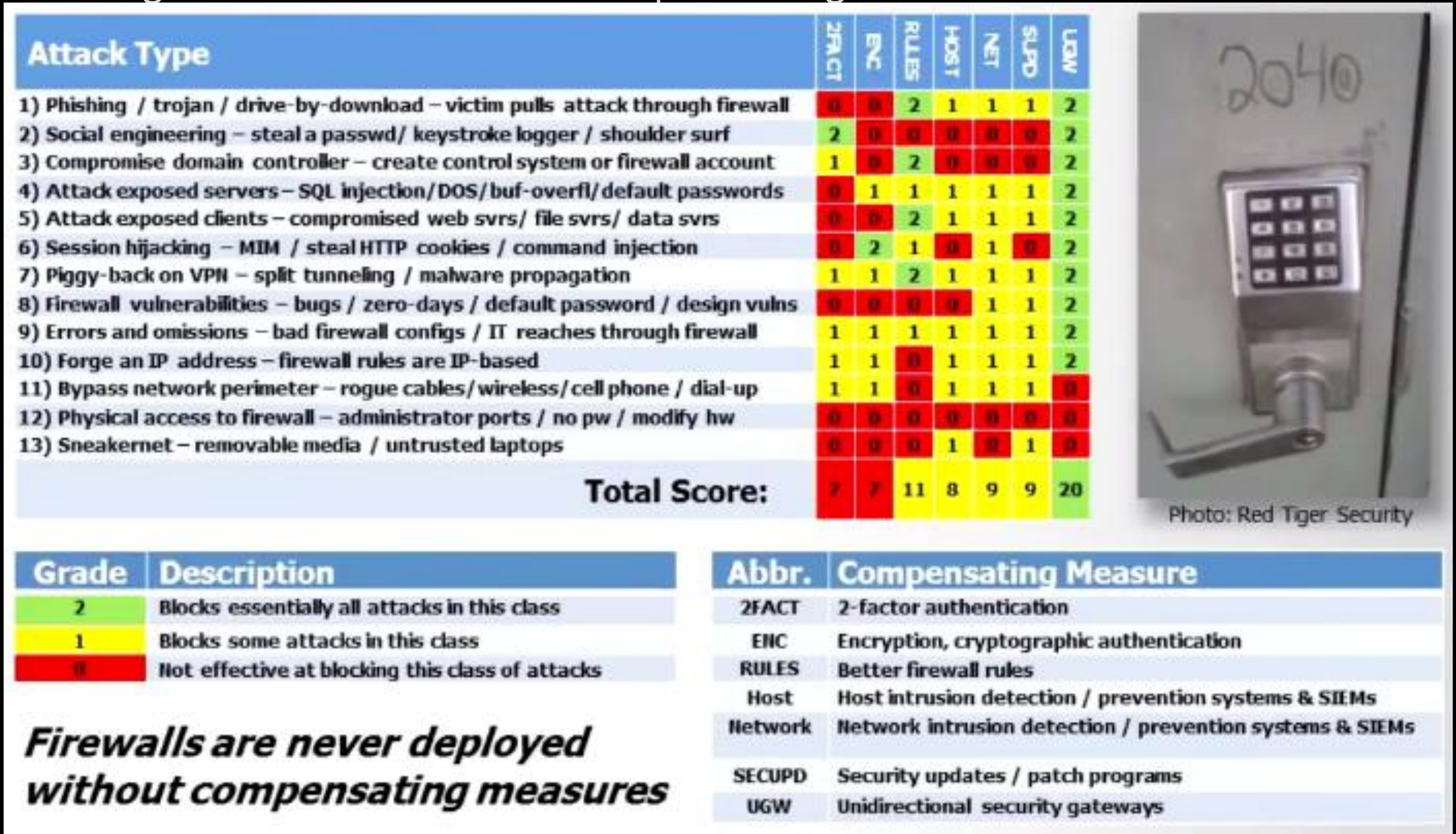




Proposed Network Architecure for SEC Generation Power Plants

13 Ways through a Firewall

- Firewall are almost always are deployed with one or a bunch of configuration mistakes or compensating measures



Attack Type	2FACT	ENC	RULES	HOST	NET	SUPD	UGW
1) Phishing / trojan / drive-by-download – victim pulls attack through firewall	0	0	2	1	1	1	2
2) Social engineering – steal a passwd/ keystroke logger / shoulder surf	2	0	0	0	0	0	2
3) Compromise domain controller – create control system or firewall account	1	0	2	0	0	0	2
4) Attack exposed servers – SQL injection/DOS/buf-overfl/default passwords	0	1	1	1	1	1	2
5) Attack exposed clients – compromised web svrs/ file svrs/ data svrs	0	0	2	1	1	1	2
6) Session hijacking – MIM / steal HTTP cookies / command injection	0	2	1	0	1	0	2
7) Piggy-back on VPN – split tunneling / malware propagation	1	1	2	1	1	1	2
8) Firewall vulnerabilities – bugs / zero-days / default password / design vulns	0	0	0	0	1	1	2
9) Errors and omissions – bad firewall configs / IT reaches through firewall	1	1	1	1	1	1	2
10) Forge an IP address – firewall rules are IP-based	1	1	0	1	1	1	2
11) Bypass network perimeter – rogue cables/wireless/cell phone / dial-up	1	1	0	1	1	1	0
12) Physical access to firewall – administrator ports / no pw / modify hw	0	0	0	0	0	0	0
13) Sneakernet – removable media / untrusted laptops	0	0	0	1	0	1	0
Total Score:	7	7	11	8	9	9	20

Photo: Red Tiger Security

Grade	Description
2	Blocks essentially all attacks in this class
1	Blocks some attacks in this class
0	Not effective at blocking this class of attacks

Firewalls are never deployed without compensating measures

Abbr.	Compensating Measure
2FACT	2-factor authentication
ENC	Encryption, cryptographic authentication
RULES	Better firewall rules
Host	Host intrusion detection / prevention systems & SIEMs
Network	Network intrusion detection / prevention systems & SIEMs
SECUPD	Security updates / patch programs
UGW	Unidirectional security gateways

Risk Analysis Approaches:.

- Types
  - Actuarial
  - Insurance style
  - Case based
- Lawyers are in charge of NERC-CIP