# How Cybersecurity or the Lack of Impact Functional Safety

By David Ong
Founder/CEO, Excel Marco Industrial Systems Pte Ltd
Founder/CEO, Attila Cybertech Pte Ltd

Safety Case
Symposium 2018
Singapore

# Disclaimer

This disclaimer informs readers that the views, thoughts, and opinions expressed in this presentation belong solely to the presenter, and not necessarily to the presenter's employer, organization, committee or other group or individual.

# Biography

**David Ong,**

Entrepreneur and Founder of Excel Marco Group, a successful Industrial Automation Integrator and Attila Cybertech, a Operational Technology (OT) cyber security firm. With over 25 years of professional experience and is widely recognized as an active professional in process automation safety industries.

# Evolution of Safety PLC

- Relay based Interlocking Panel
- Solid-state Safety System
- PLC with redundant Processor, Fail-safe design
- Third party certified Safety PLC: FS, DMR, QMR, TMR

Siemens

Schneider Electric

Mitsubishi Electric

Allen Bradley

ABB

# Standards

***Functional Safety***

- DIN V VDE 0801
- DIN V 19250
- ISA SP84
- IEC 61508/61511

***Cybersecurity***

- ISO/IEC 27000 (Information Security)
- ISA/IEC 62443 (Industrial Security)
- NIST 800-53 Appendix
- NIST 800-82

61508-life.jpg

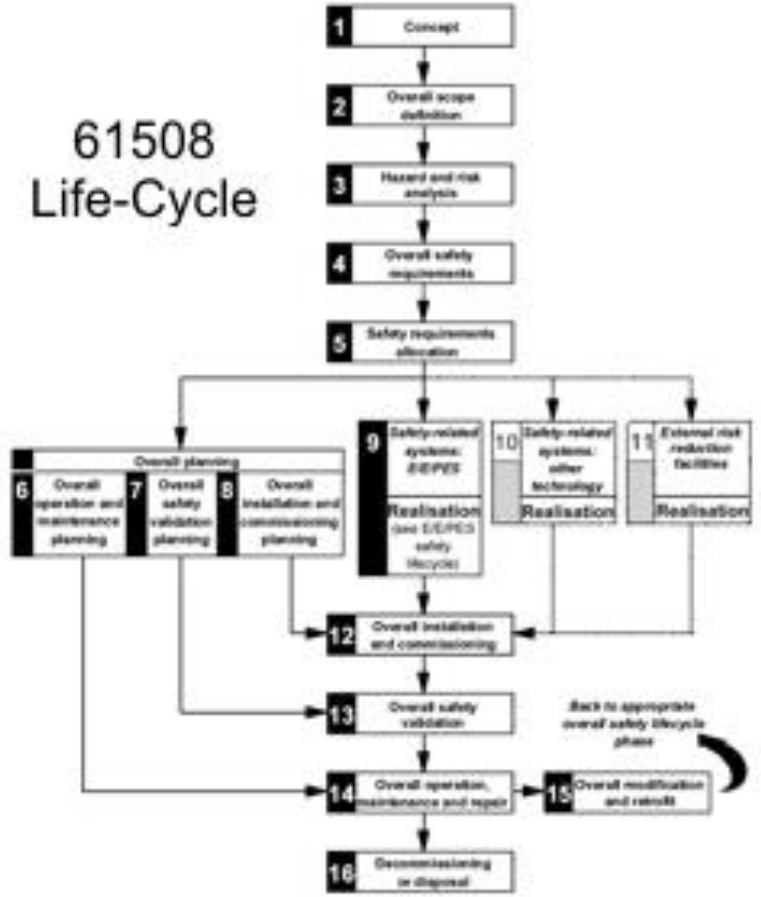
# Standards for Functional Safety

**Fundamental change from Qualitative to Quantitative:**

Safety Life Cycle Model

Safety Integrity Level

Third party certification, e.g. TUV

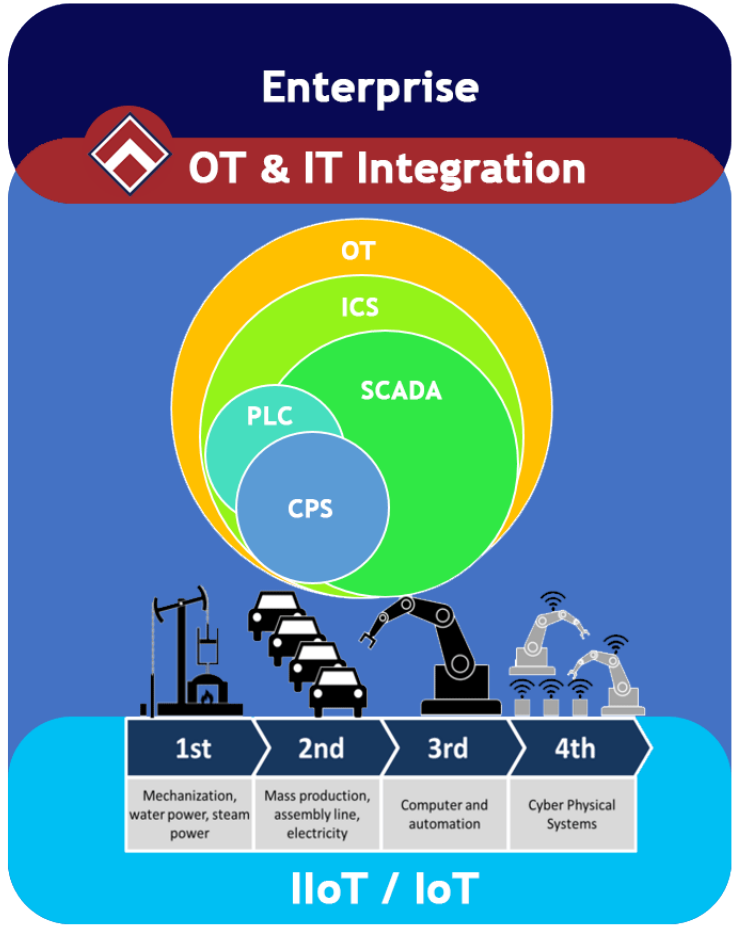


# Connectivity … Hello World

- Communications capability
  - interface to EWS, DCS, HMI, Peer to Peer
- Uni-directional communication, read-only
- Bi-directional communication, read-write
- Integrated Control & Safety Systems

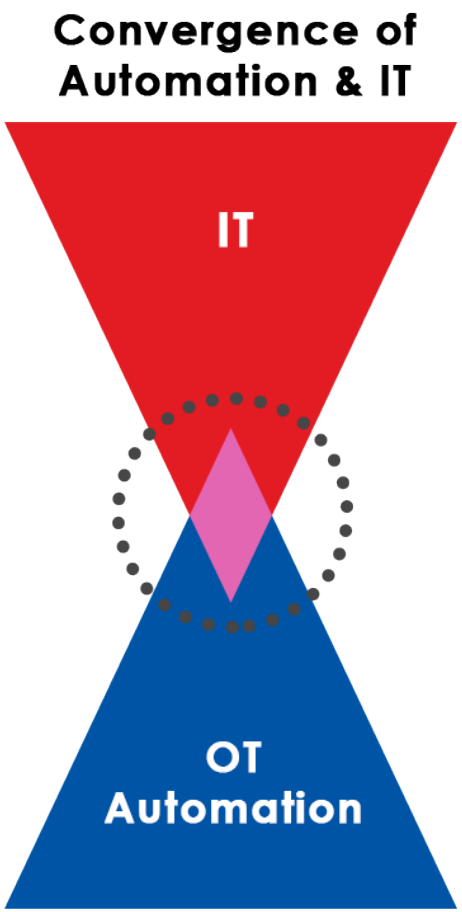
# Convergence of IT and OT

- Historically, IT and OT have had fairly separate roles and were managed separately within an organization
- ICS were traditionally developed using specialized hardware and proprietary software
- Deployed as standalone platforms using vendor proprietary communication protocols to communicate with similar systems



# Convergence of IT and OT

- Reduce manufacturing and operational costs.
- Increase productivity.
- Provide access to real-time information.
- Utilize modern networking systems to interconnect ICS with business and external networks.
- ICS makers switched to commercial-off-the-shelf equipment and software



# Convergence of IT and OT

- Whatever Windows is vulnerable to exploitation, so is ICS?
- Can you Hack an SIS?
- Can you Hijack a plane?
- Now can you Cyber hack an SIS?

# Top 10 Cybersecurity attacks of ICS

| FY 2014-2016 TOP SIX WEAKNESS CATEGORIES IN ORDER OF PREVALENCE | | |
|---|---|---|
| **FY 2014** | **FY 2015** | **FY 2016** |
| 1. Boundary Protection | 1. Boundary Protection | 1. Boundary Protection |
| 2. Information Flow Enforcement | 2. Least Functionality | 2. Least Functionality |
| 3. Remote Access | 3. Authenticator Management | 3. Identification and Authentication |
| 4. Least Privilege | 4. Identification and Authentication | 4. Physical Access Control |
| 5. Physical Access Control | 5. Least Privilege | 5. Audit Review, Analysis and Reporting |
| 6. Security Function Isolation | 6. Allocation of Resources | 6. Authenticator Management |

Table 1: FY 2014-2016 Top Six Weaknesses

| FY 2016 MOST PREVALENT WEAKNESSES | | |
|---|---|---|
| **Area of Weakness** | **Rank** | **Risk** |
| Boundary Protection | 1 | • Undetected unauthorized activity in critical systems<br>• Weaker boundaries between ICS and enterprise networks |
| Least Functionality | 2 | • Increased vectors for malicious party access to critical systems<br>• Rogue internal access established |
| Identification and Authentication | 3 | • Lack of accountability and traceability for user actions if an account is compromised<br>• Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access |
| Physical Access Control | 4 | • Unauthorized physical access to field equipment and locations provides increased opportunity to<br>o Maliciously modify, delete, or copy device programs and firmware<br>o Access the ICS network<br>o Steal or vandalize cyber assets<br>o Add rogue devices to capture and retransmit network traffic |
| Audit Review, Analysis and Reporting | 5 | • Without formalized review and validation of logs, unauthorized users, applications, or other unauthorized events may operate in the ICS network undetected detection |
| Authenticator Management | 6 | • Compromised unsecured password communications.<br>• Password compromise could allow trusted unauthorized access to systems |

Table 2: Risk Associated with FY2016 Most Prevalent Weaknesses

***Source: ICS-CERT Annual Assessment Report FY2016***

# Top 10 Cybersecurity attacks of ICS

**#10:** Cell-phone WIFI

**#9:** Sophisticated Market Manipulation

**#8:** Market manipulation

**#7:** Ukraine Attack

**#6:** Sophisticated Ukraine Attack

**#5:** Zero-day ransom ware

**#4:** Targeted ransom ware

**#3:** Common ransom ware

**#2:** IT insider

Source: https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf

# Top 10 Cybersecurity attacks of ICS

**#1: ICS Insider** – A disgruntled insider with access to ICS equipment uses social engineering to steal passwords able to trigger a partial plant shutdown.

Source: https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf

# ICS Cybersecurity Attacks

Some infamous ICS Cybersecurity Attacks :

- Stuxnet
- Black Energy (Ukraine)
- Maroochy Shire sewage

# Overview of Stuxnet

- A malicious computer worm, first uncovered in 2010 by Kaspersky Lab
- Specifically targets – only Siemens PLC
- Brought down 1/5 of Iran's nuclear centrifuges by causing them to rotate unusually fast and then slowing down abruptly – with no indication on HMI
- Alleged state sponsored attacked by the US/Israel

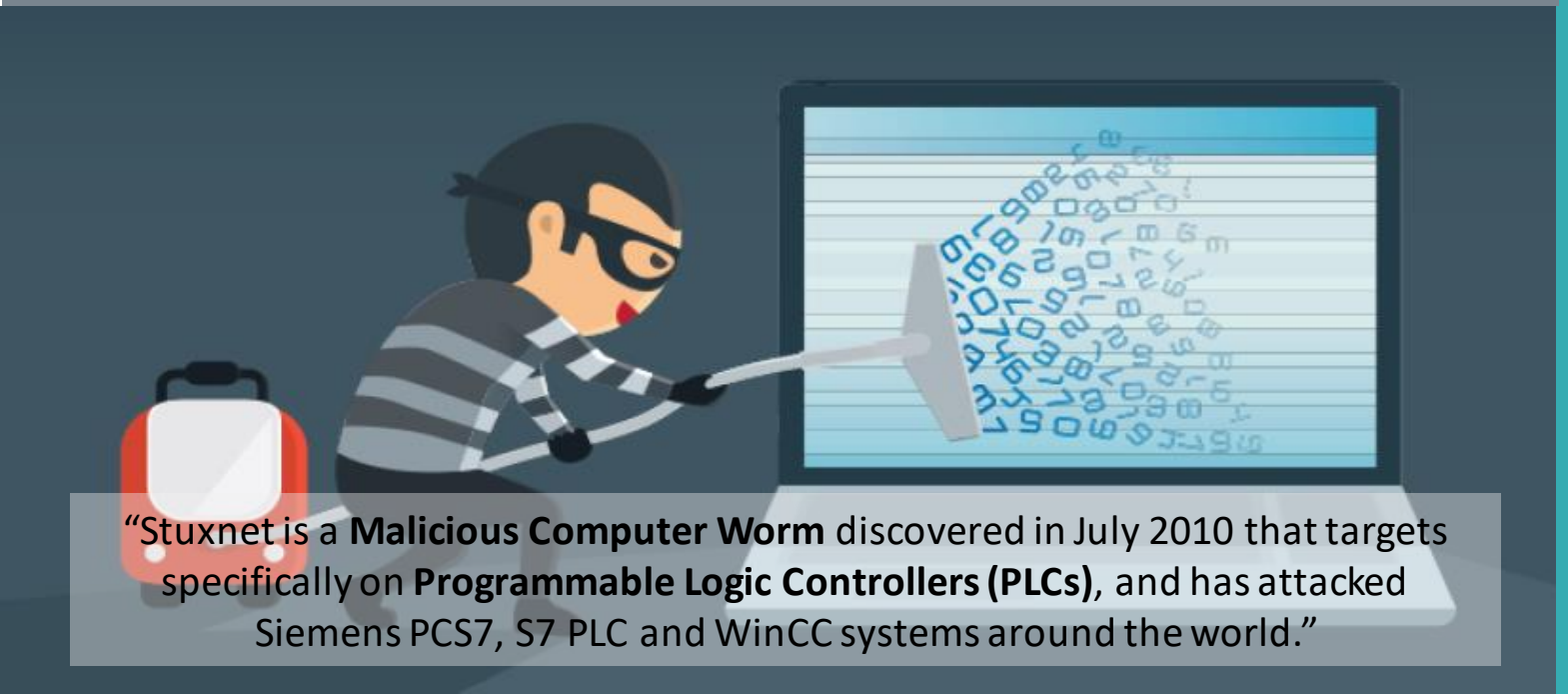
# How Stuxnet works

**Infection**

Stuxnet enters a system via a USB stick and proceed to infect all machines running Microsoft Windows.

**Search**

Stuxnet checks whether a given machines is part of the targeted Industrial Control Systems made by Siemens



"Stuxnet is a **Malicious Computer Worm** discovered in July 2010 that targets specifically on **Programmable Logic Controllers (PLCs)**, and has attacked Siemens PCS7, S7 PLC and WinCC systems around the world."

**Update**

Stuxnet attempt to access the internet and download a more recent version of itself.

**Compromise**

Stuxnet compromises the targeted system's logic controllers exploiting zero-day vulnerabilities that hasn't been identified by security experts.

**Control**

Stuxnet spies on the Operations of the targeted system and use the information it has gathered to take control of centrifuges, making them spin themselves to failure.

**Man-In-The-Middle**

Stuxnet provides false feedback to outside controllers, ensuring that they wont know what's wrong until it is too late to rectify.

# Black Energy (Ukraine)

- Prior compromise of corporate networks using spear-phishing emails with BlackEnergy malware
- Seizing SCADA under control, remotely switching substations off
- Disabling/destroying IT infrastructure components (uninterruptible power supplies, modems, RTUs, commutators)
- Destruction of files stored on servers and workstations with the KillDisk malware
- Denial-of-service attack on call-center to deny consumers up-to-date information on the blackout.

# Maroochy Shire Sewage Attack

- More than 1,000,000 litres of sewage fluid released into local parks
- Insider ICS attack (listed as no.1) – disgruntled ex employee
- Stole configuration program and control equipment, “impersonated” a pump to cause malfunction

# ICS/SIS Vulnerability

**ICS**

- USB Drive malware
- DOS/DDOS

Common Mode Failure

- Human factor
- Power Source
- Environment

**SIS**

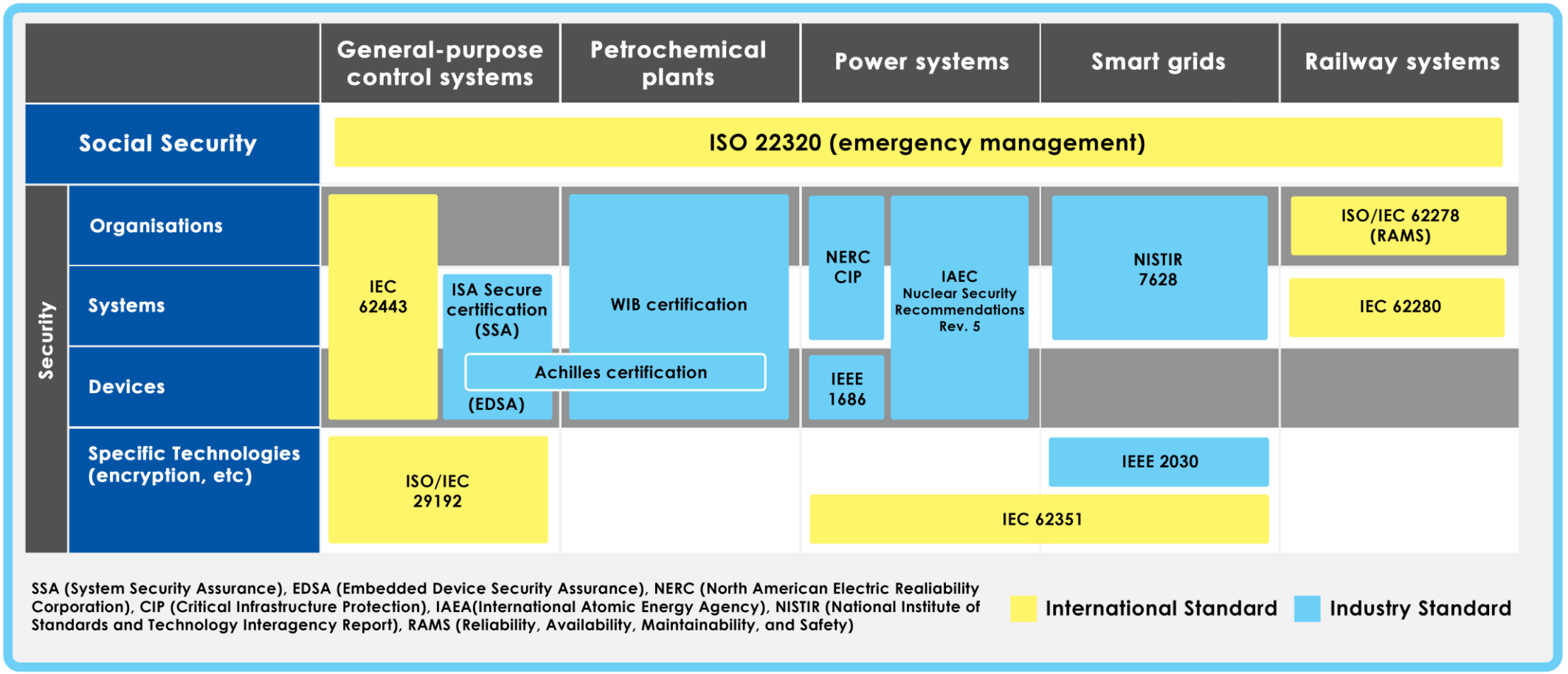
- USB drive on EWS

# Information Security Standards

- ISO27001 / 27002 / 15408
- NIST 800-82
- IEC62443/ISA99
- CISQ
- NERC 1300
- RFC 2196
- ISA/IEC 62443 (previously ISA-99)

Source: https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf

# Standards and Best Practices for ICS




Source: Hitachi Review Vol. 63 (2014)

# Standards and Best Practices for ICS

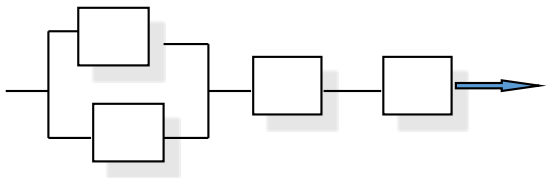

- American Petroleum Institute (API): API-1164 - Pipeline SCADA Security, 2nd ed.
- National ICS Security Standard (Qatar), v3, Mar 2014
- Australian Signals Directorate (ASD): Strategies to Mitigate Cyber Security Incidents – Mitigation Details, Feb 2017 (Note: It claims implementing the Top 4 can mitigate over 85% of intrusions)

# Functional Safety vs Cyber Security

**Functional Safety**

- Risk Assessment
- Quantitative Risk Analysis (QRA)
- Layer of Protection Analysis (LOPA)
- SIL Determination
- Safety Requirement Specification (SRS)

*Reliability Block Diagrams*

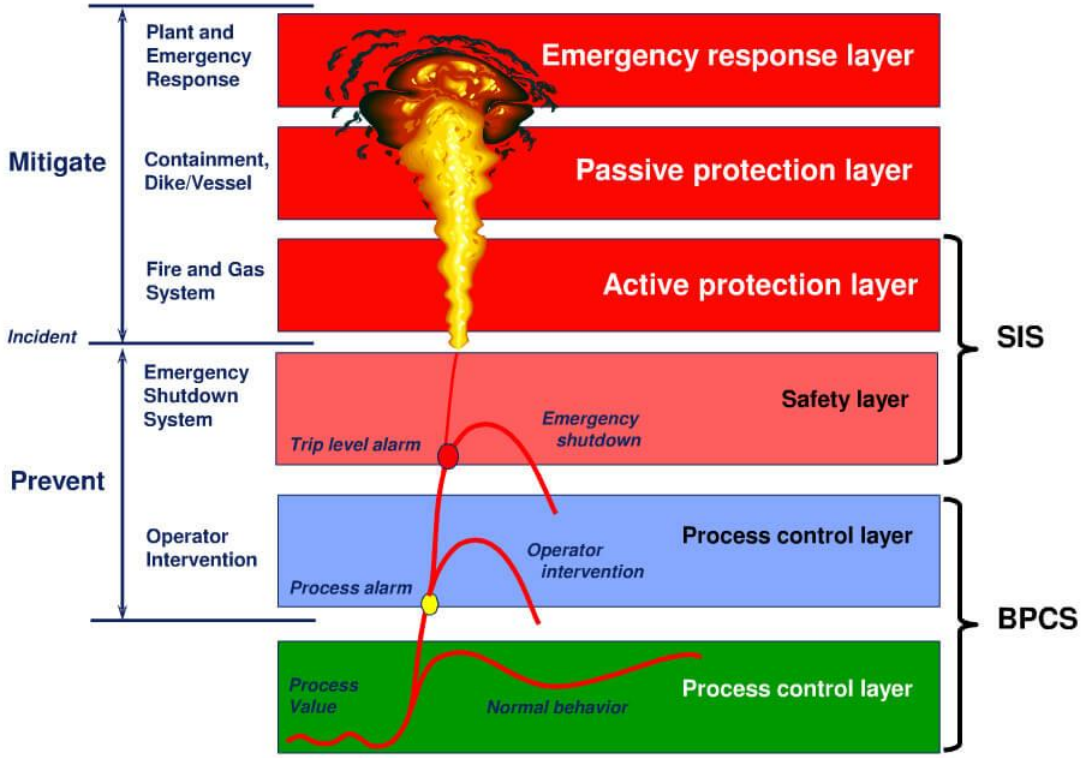


**Cyber Security**

- Risk Assessment
- Threat, Vulnerability & Risk Assessment (TVRA)
- Defense-in-Depth
- Security Level (SL)
- Security by Design

# LOPA vs Defense-in-Depth

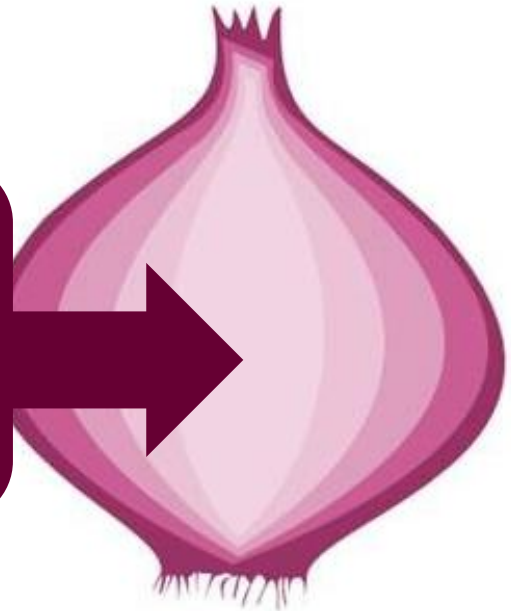
## Layer of Protection Analysis (LOPA)




## Defense-In-Depth (DiD)

- Defense-in-depth approach: Employs multiple layers of defense (physical, procedural and electronic) at separate levels. The layers are:

- Policies, Procedures and Awareness
- Physical Security
- Network Security
- Computer Hardening
- Application Security
- Device Hardening



# Challenges: What are the problems…?

**Functional Safety**

- SIL is quantitative
- It is derive from PFD(avg)

**Cybersecurity**

- SL not widely used yet
- Not “quantifiable”, based on qualitative judgement

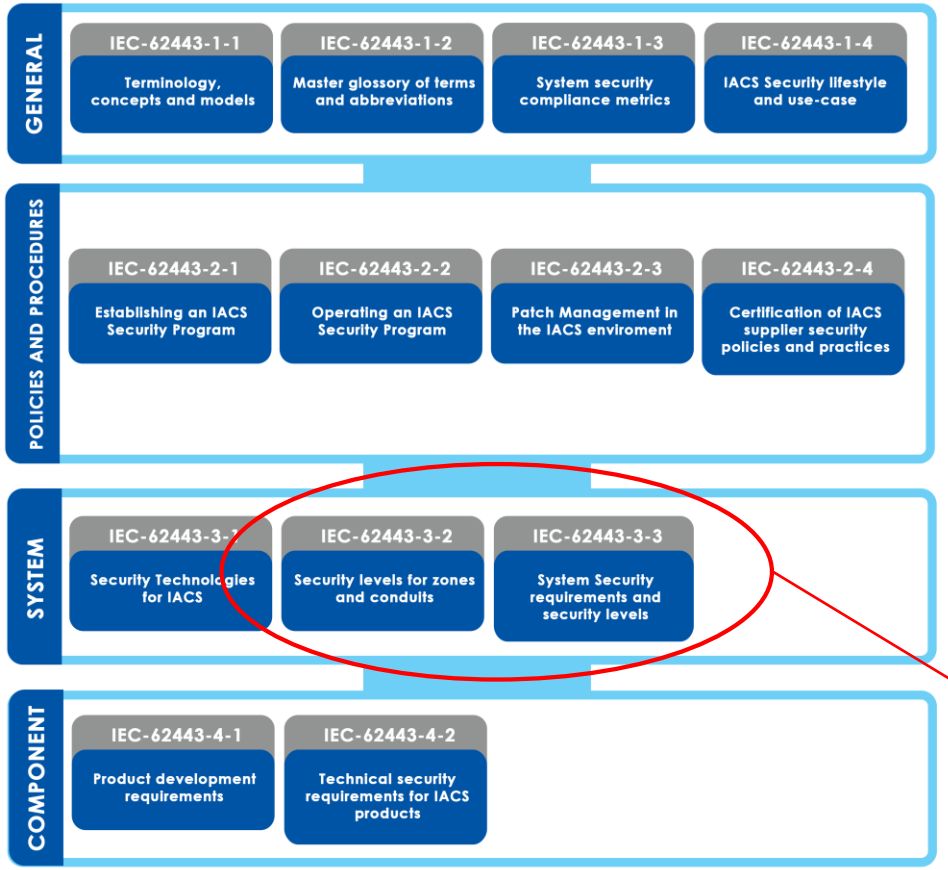
? “There are unknown unknown …. things that we don’t know what we don’t know” (Donald Rumsfield)

? What is the Probability of a Hacker attacking an ICS using a particular attack vector?
  - Depends on human behavior?
  - Can we based on historical data of attacks?

? Can we quantify what is the likelihood of a terrorist attack?

# Rating Cyber Security Risk: Security Level

**Cybersecurity Risk can be rated via Security Level or Common Vulnerability Scoring System (CVSS)**

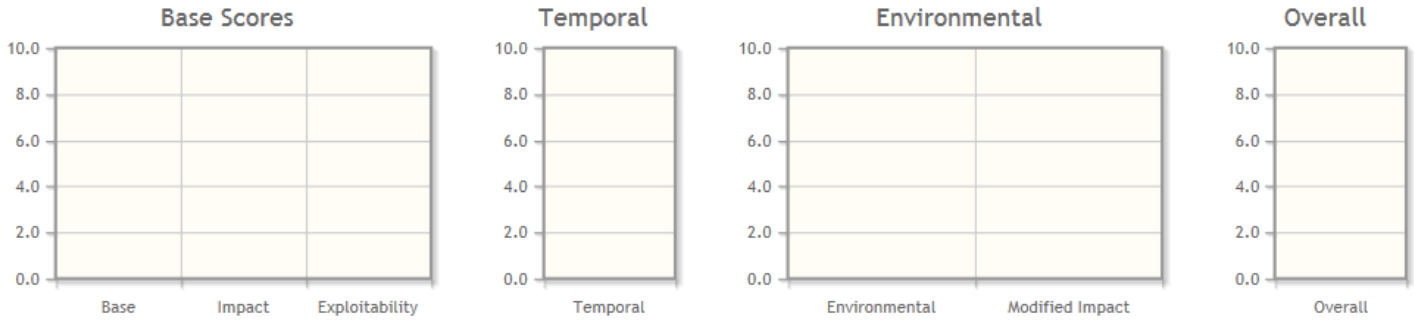



| Security Level Definition | |
|---|---|
| SL 1 | Protection against casual or coincidental violation |
| SL 2 | Protection against intentional violation using simple means with low resources, generic skills and low motivation |
| SL 3 | Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation |
| SL 4 | Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation |

Part 3-2: asset owner / system integrator define zones and conduits with target SLs
Part 3-3: product supplier provides system features according to capability SLs

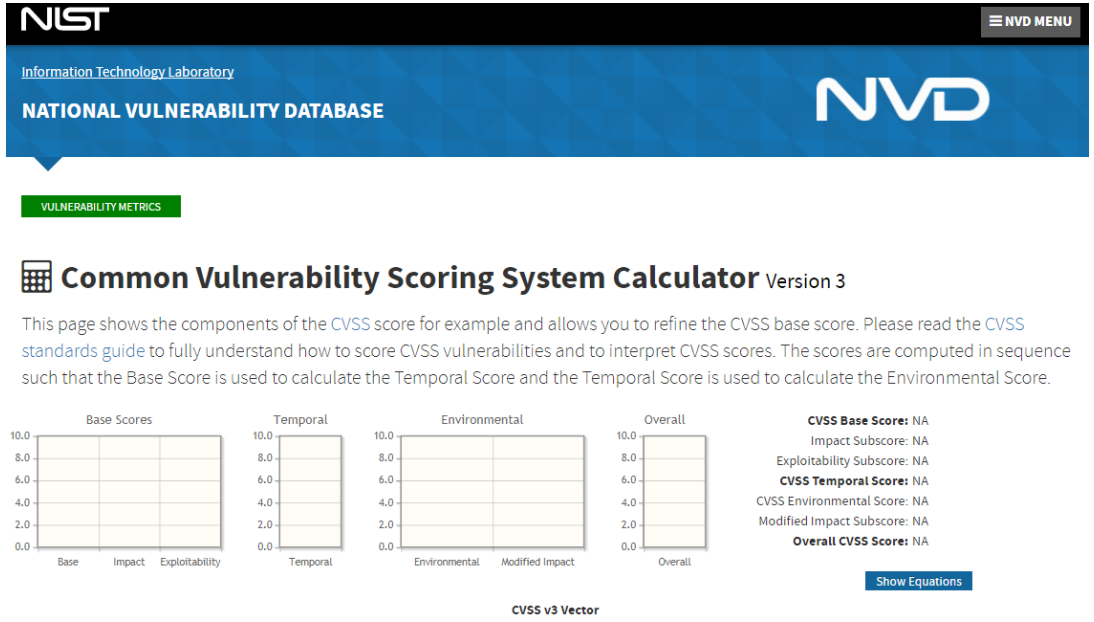
# Rating Cyber Security Risk: CVSS

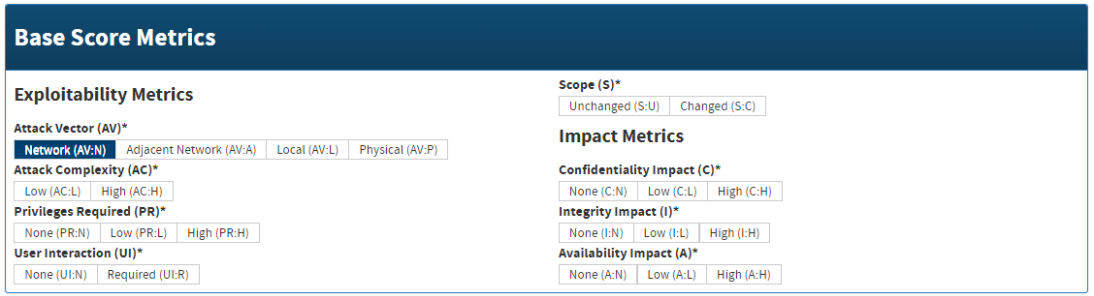
- The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities.
- CVSS consists of three metric groups: Base, Temporal, and Environmental.
  - The Base group represents the intrinsic qualities of a vulnerability,
  - The Temporal group reflects the characteristics of a vulnerability that change over time.
  - The Environmental group represents the characteristics of a vulnerability that are unique to a user's environment.

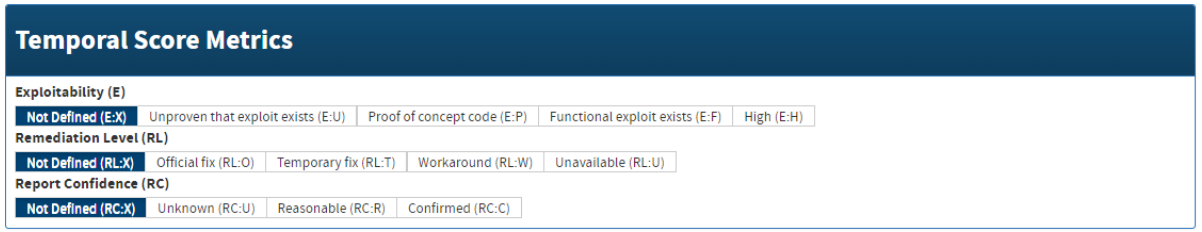


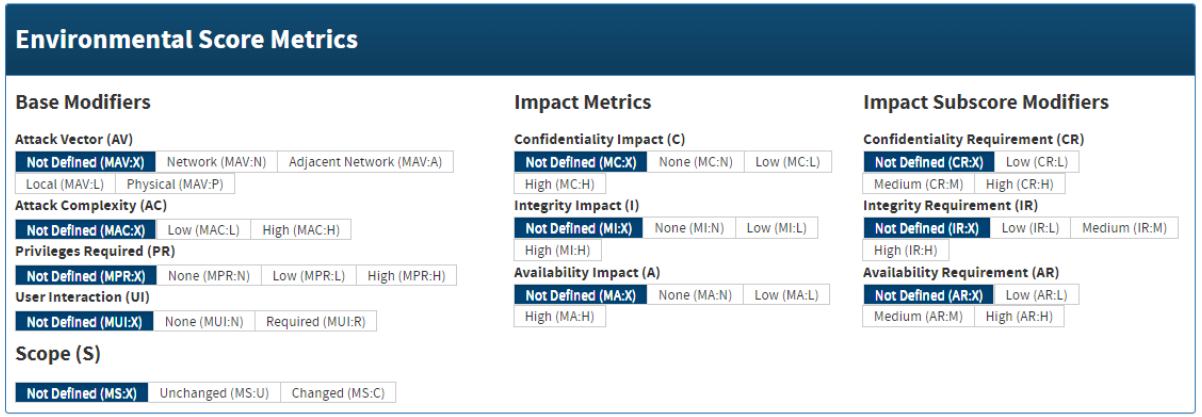

Source : https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

# Rating Cyber Security Risk: CVSS




**Source :** https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

# Solutions

- Are we able to apply IT Cybersecurity to OT (ICS)?

- Why not?

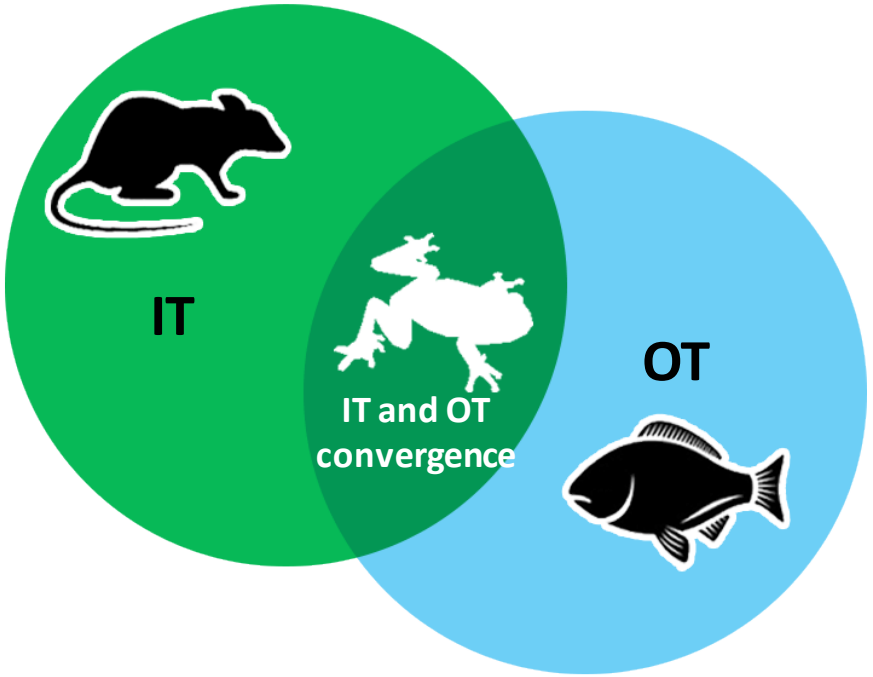
  IT Protocol: TCP/IP
  Secured by: HTTPS, DNNSEC, AES128 etc…

  Industrial Protocol: Modbus, Industrial Fieldbus, Industrial Ethernet (Ethernet/IP, Profinet)
  Secured by: Threat modelling, risk mitigation, signature-based and anomaly detections

  Tapping in to OT networking!

# Understanding IT and OT

- **Operational Technology (OT)**
  - ICS, PLC, DCS, SCADA, IACS synonymously used terms
- The Difference between **IT vs OT**
  - Modus Operandi
  - External Inputs
  - CIA and AIC
  - Latency issues
  - False Positives
  - Functional Safety
  - Proofing

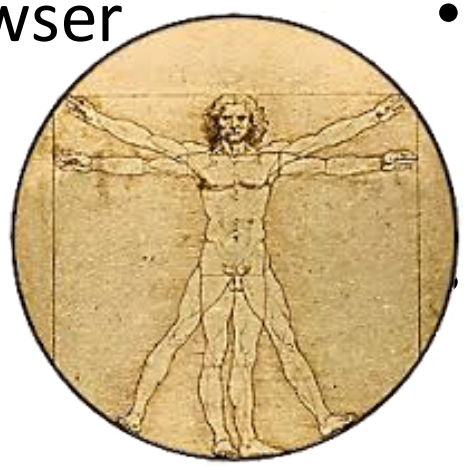


# Differences between IT vs OT

## External Inputs – Human initiated vs Sensor triggered

**Source of Input to IT**

- PC user: keys, mouse, trackball etc.
- Internet / Intranet download, web browser
- Emails
- ERP



**Source of Input to OT**

- Sensors e.g. Pressure, Flow, Level, Position, Limit, Smoke, Gas etc
- Operator action such as alarm acknowledgement, auto/manual mode selection
- Set-point entry

# Differences between IT vs OT

## False Positives

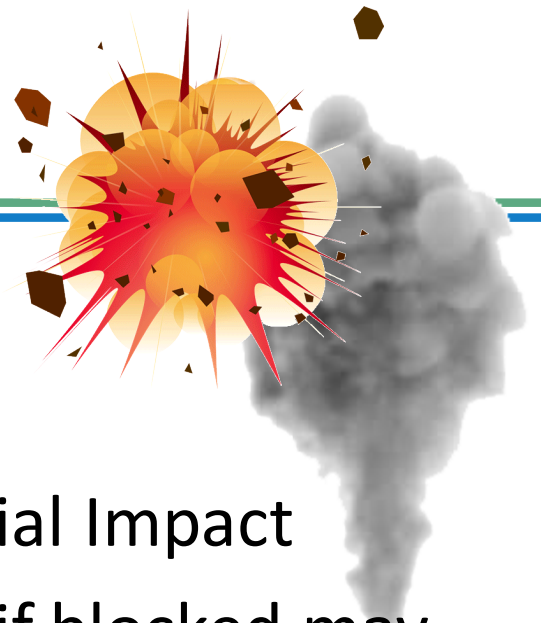
### IT

- Suspicious Packets may be blocked, rejected or quarantine

### OT

- Suspicious Packets may **trigger alerts**
- Unless determined unambiguously as malicious packets, it may not be blocked
- False Positives leads to indifference, which leads to "**switching off**"

# Differences between IT vs OT



## Functional Safety

### IT

- Low Consequential Impact
- Blocking a email or Approval of legitimate online payment may be inconvenient but not life - threatening

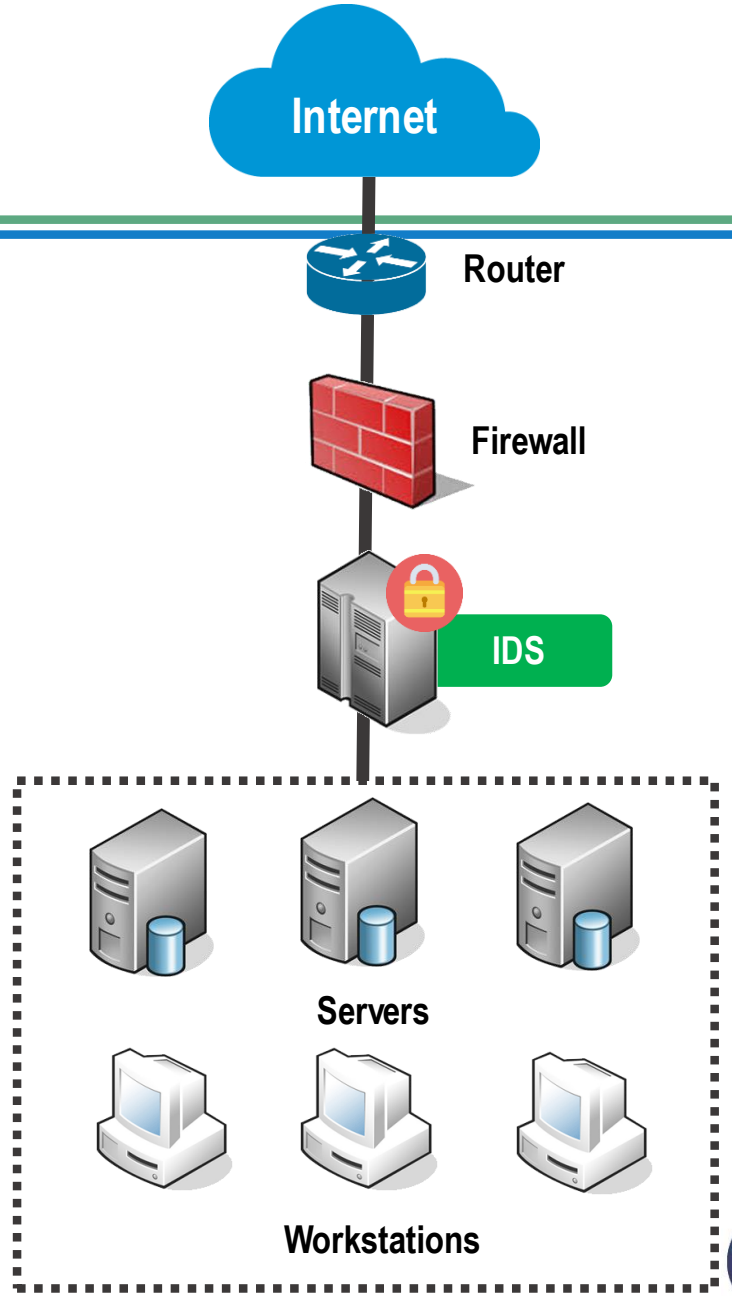
### OT

- High Consequential Impact
- Shutdown signal if blocked may prevent bringing Process to a “Safe State”, could be life threatening

# Solutions

- Industrial firewall
- Intrusion Detection System (IDS)
- Whitelisting
- Hardening
  - Active directory

**Don’t throw away common sense, use it!**



# Cyber Security Law - Regulatory Compliance Standards

## Regulatory Compliance Standards

- NERC Critical Infrastructure Protection (CIP) Version 6, July 2016, USA.
- DHS Chemical Facility Anti-Terrorism Standards (CFATS), 9 April 2007 and the CFATS Act 2014, USA.
- Cyber Security Programs for Nuclear Facilities, NRC Regulation 5.71 (Jan 2010), USA.
- German IT Security Law (IT-Sicherheitsgesetz), 25 July 2015, Germany.
- The Directive on Security of Network and Information Systems (NIS Directive), (EU) 2016/1148, European Union.
- Military Programming Law (LPM), Article 22, 1 July 2016.
- The Cybersecurity Law of the People's Republic of China, 1 June 2017, China.
- Security of Critical Infrastructure Bill 2017, 7 December 2017, Australia.

# Conclusion

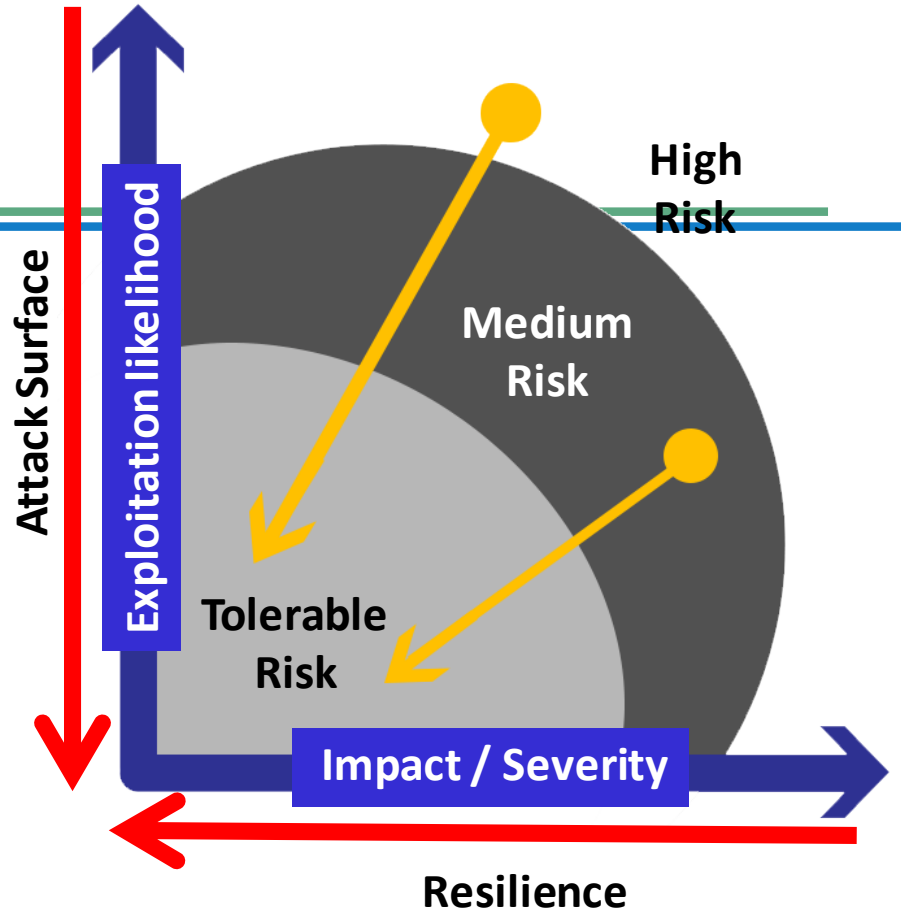
- SIS – no such thing as zero risk
- Cybersecurity – no such thing as zero risk

**Functional Safety**

- No zero risk
- Risk Reduction
- ALARP

**Cyber Security**

- No zero risk
- Risk Reduction
- ALARP




**Zero Risk is non existent!**

**We have to be Cybersecurity Resilient!**

# Conclusion

**Common Mode Failure**

- Human Factor (During Operation)
- Wrong Assumption (At Design Stage)
- Exploring “New” Technology
- HVAC / Chiller
- Power

# References


https://ics-cert.us-cert.gov/sites/default/files/ICSJWG-Archive/QNL_DEC_17/Waterfall_top-20-attacks-article-d2%20-%20Article_S508NC.pdf

https://en.wikipedia.org/wiki/Stuxnet

https://en.wikipedia.org/wiki/Cyber_security_standards

https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

# Contact

## Presenter Information


**Presenter Name** : **David Ong**

**Company** : **Excel Marco Industrial Systems Pte Ltd**
**Attila Cybertech Pte Ltd**

**Email** : **david.ong@excelmarco.com**

**Website** : **www.excelmarco.com**
**www.attilatech.com**


Safety Case Symposium 2018 Singapore
www.SafetyCaseSymposium.com

# Thank You

**visit us at www.excelmarco.com**

Спасибо
благодаря
Dankeschoen
Dank U wel
Gracias
Shukran
Merci
Terima Kasih
(Kam-sa-ham-ni-da)
ありがとう！
(Arigatou Gozaimasu)
谢谢！
Cám ơn
Khob Khun
Obrigado

Safety Case Symposium 2018
Singapore
www.SafetyCaseSymposium.com