8 December 2017

HITCON PACIFIC 2017

# ICS/SCADA Cybersecurity and IT Cybersecurity:
## Comparing Apples and Oranges

Presented by David Ong | CEO of Attila Cybertech

ATTILA CYBERTECH
www.attilatech.com

Resilience Beyond **Defense**
Cyber-Resilience for ICS, SCADA & CPS

# Quote by Donald Rumsfeld

"... But there are also unknown unknowns. There are things we don't know we don't know."

Donald Rumsfeld, former Secretary of Defence

# 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 20 years of professional experience and is widely recognized as an active professional in process automation safety industries.

# About Attila Cybertech

- Cyber Security in Operational Technology (OT)
- Data Analytics for Plant and Factory Optimization
- OT and IT Integration for the Critical Information Infrastructure  Sectors (CII)

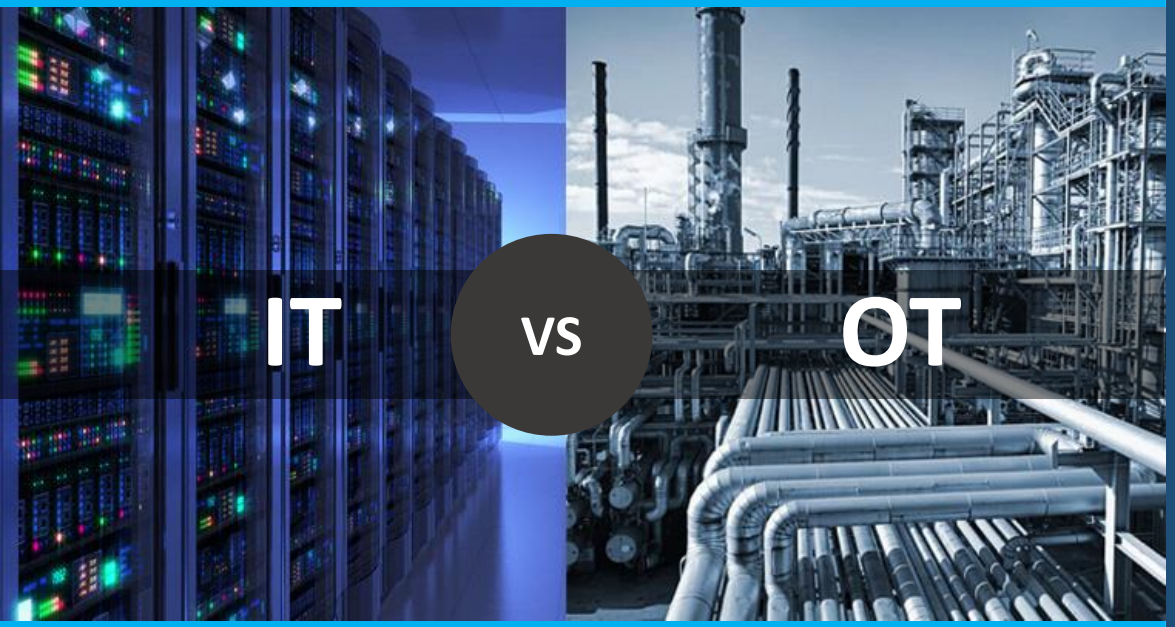
**VISION**

> “To be a leader in creating resilient Cyber Ecosystem that is safe and transformational for humanity”

**MISSION**

> “To help create Cyber-Resilience Critical Information Infrastructure (CII) and to inspire Data Analytics application using Artificial Intelligence”

## Comparing Apples and Oranges




- Terminology
- Types of ICS
- The Need to Secure ICS
- IT-OT Convergence
- Challenges in IT-OT Convergence
- Standards & Best Practices for ICS
- ICS Cyber Security Assessment
- Cyber Security Assessment & Tool
- ICS Security Architecture
- Industrial Protocols
- Security Application for ICS
- Q & A

# What is Operational Technology? OT

OT is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. (Gartner)

OT is a category of hardware and software that monitors and controls how physical devices perform. (SearchData.com)

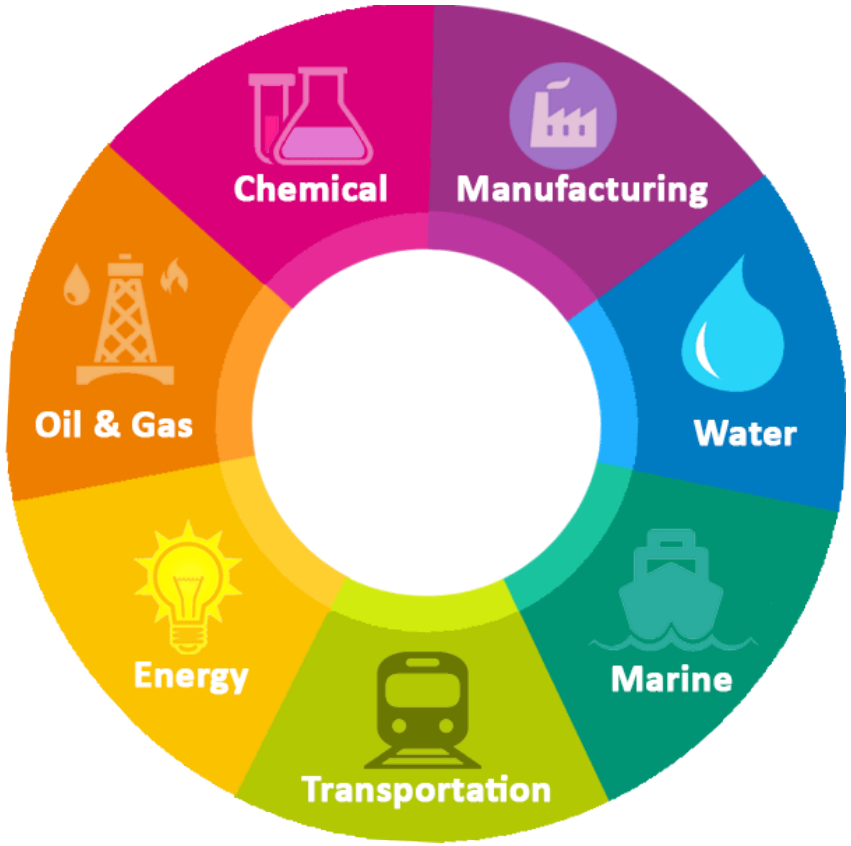
OT is the hardware and software dedicated to detecting or causing changes in physical processes through direct monitoring and/or control of physical devices such as valves, pumps, etc. (Wikipedia)

# Industrial Control System (ICS)?


Industrial Control System (ICS) is a term used to encompass the many applications and uses of industrial and facility control and automation systems. ISA-99/IEC 62443 is using Industrial Automation and Control Systems (ISA-62443.01.01) with one proposed definition being “a collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.” (SANS)

Industrial control system (ICS) is a general term that encompasses several types of control systems, including SCADA systems, DCS, and other control system configurations such as PLC often found in the industrial sectors and critical infrastructures. (NIST)

# Industrial Processes using ICS




- Electrical & nuclear plants
- Waste water treatment plants
- Oil & natural gas
- Transportation
- Air traffic control
- Manufacturing
- Food & beverage
- Etc.

# Types of ICS

- BAS: Building Automation Systems
- DCS: Distributed Control Systems
- SCADA: Supervisory Control and Data Acquisition
- HMI: Human-Machine Interface
- SIS: Safety Instrumented Systems
- PLC: Programmable Logic Controllers
- RTU: Remote Terminal Units
- IED: Intelligent Electronic Devices

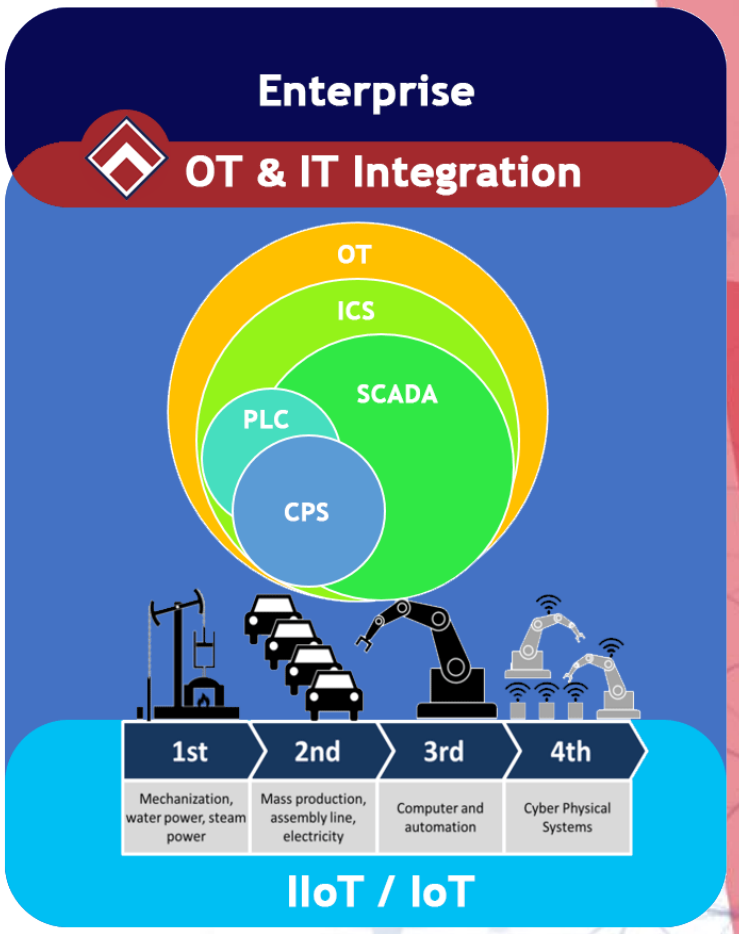
# The need to secure ICS

Possible consequences of security incidents:

- Risk of death and serious injury
- Loss of production
- Environmental impact
- Manipulation or loss of data (records)
- Damage to company image / reputation
- Financial loss

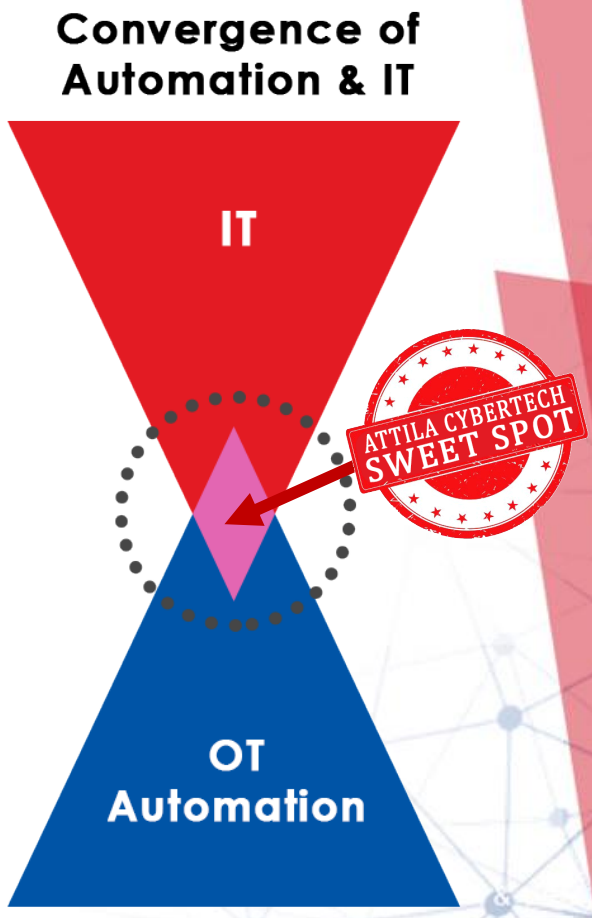
# IT-OT Convergence

- 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



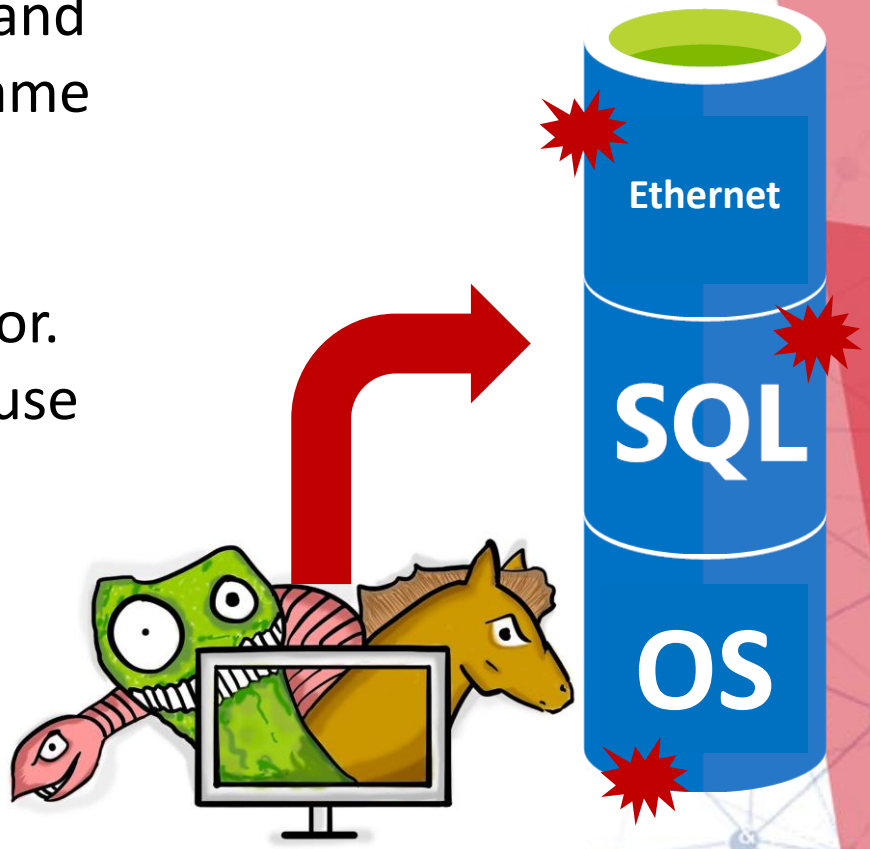
# IT-OT Convergence

- 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 vendors also switched to using commercial-off-the-shelf equipment and software to build their systems



# Challenges in IT-OT Convergence

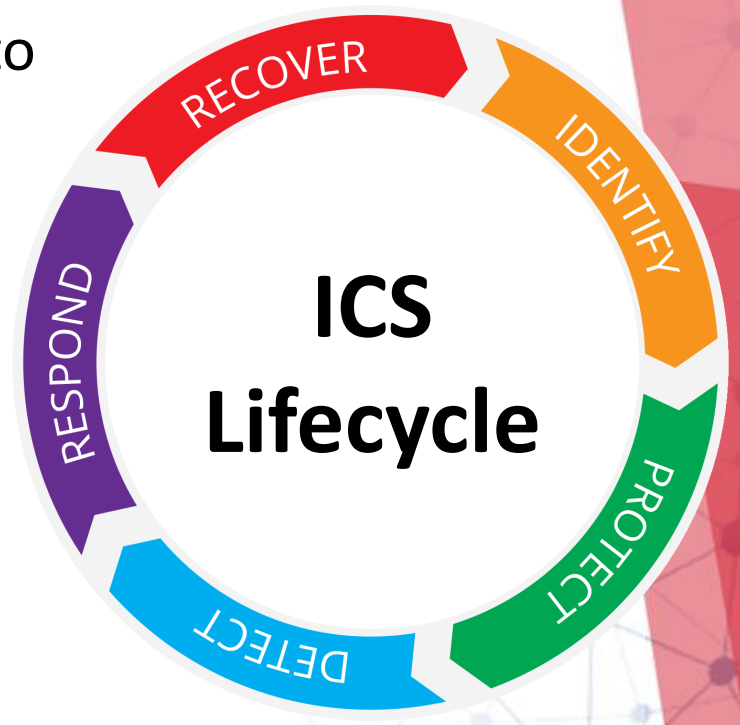
- Integration of technology such as Windows OS, SQL, and Ethernet means that ICS are now vulnerable to the same viruses, worms and trojans that affect IT systems.
- Enterprise Integration of legacy ICS means they are vulnerable to attacks which they were not designed for.
- Not all IT security solutions are suitable for ICSs because of fundamental differences between ICS and IT systems.



# Challenges in IT-OT Convergence

ICS security goal: AIC (Availability, Integrity, Confidentiality)

- Operational availability means it is very difficult and costly to interrupt these systems for security updates
- ICS lifecycle is usually 10 to 20 years and are typically not built with security in mind.
- Firmware and software are not replaced for a long time, patches are rarely applied, and network devices can be disrupted by malformed network traffic or even high volumes of well-formed traffic.



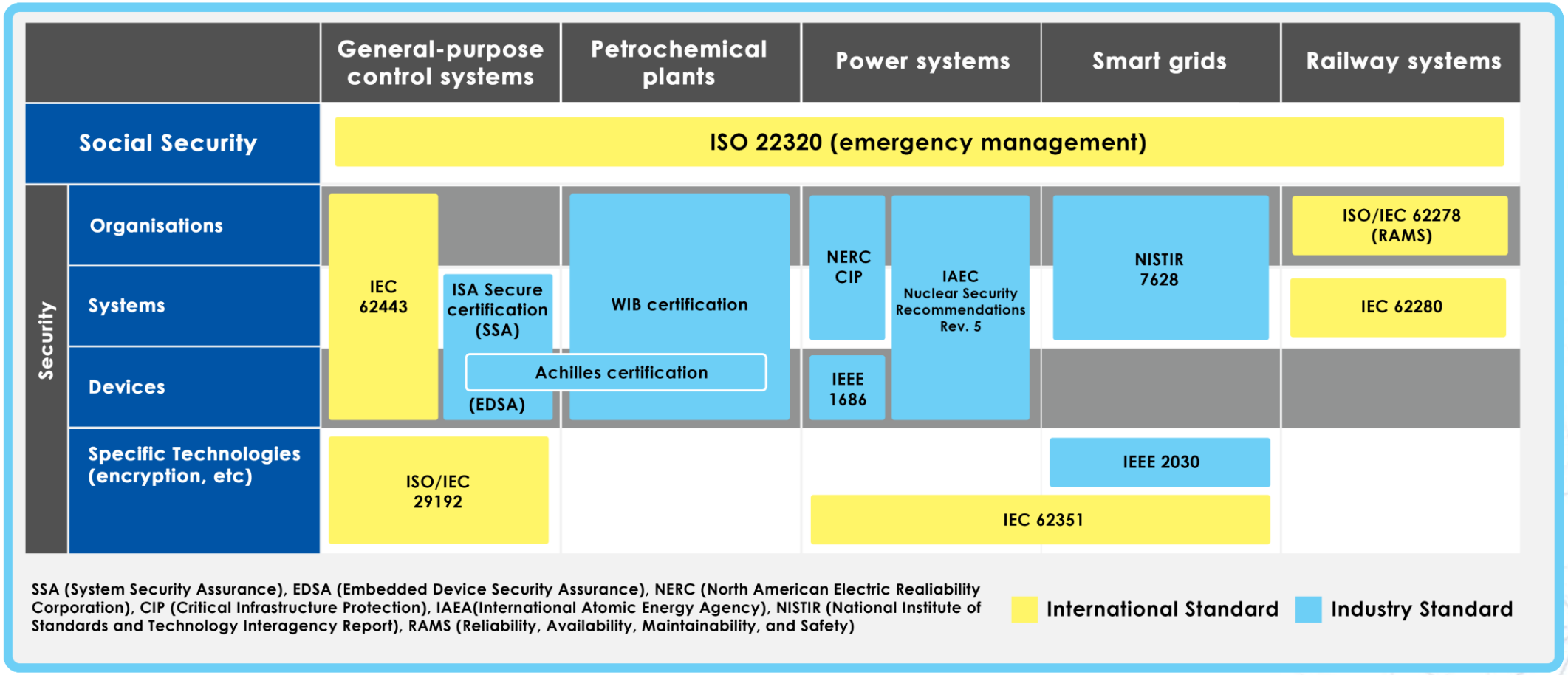
# Challenges in IT-OT Convergence

- ICS patching requires testing, approval, scheduling, and validation to ensure safe and repeatable control.
- All updates, including patches and virus definition files, have to be thoroughly tested with the ICS before being approved for installation.
- ICS often include safety instrumented system (SIS)

# Challenges in IT-OT Convergence

- Most ICS are supported by outside vendors, and are deployed with default configuration settings.
- Demand for 24/7 remote access for engineering, operations or technical support means more insecure or rogue connections to ICS.
- Manuals on ICS equipment are publicly available to both would-be attackers and legitimate users.

# Standards and Best Practices for ICS




Source: Hitachi Review Vol. 63 (2014)

# Standards and Best Practices for ICS

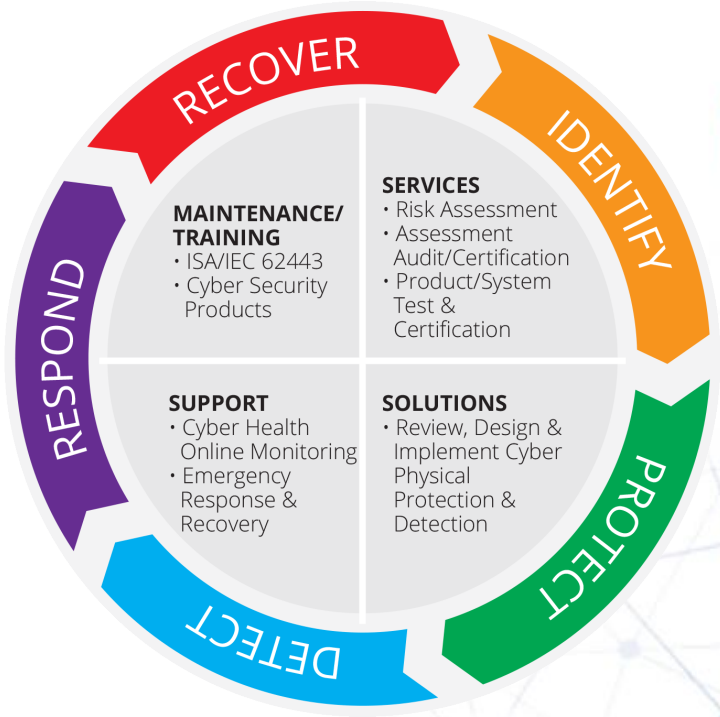
- American Petroleum Institute (API): API-1164 - Pipeline SCADA Security, 2nd ed.
- National ICS Security Standard (Qatar), v3, Mar 2014
- Australian Signals Directorate (ASD): Strategies to Mitigate Cyber Security Incidents – Mitigation Details, Feb 2017 (Note: It claims implementing the Top 4 can mitigate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


# Industrial Cyber Security Assessment

- In any security policy implementation, risk and security assessments are the starting point
- Security assessments analyse your current state, from technologies to policies, procedures to behaviour
- It offers a realistic picture of your security posture (current risk state) and what it will take (mitigation techniques) to get to where you need to be (acceptable risk state)

# Cyber Security Assessment & Tools

- NIST “Framework for Improving Critical Infrastructure Cybersecurity”
- The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk
- It identifies five essential program activities: Identify, Protect, Detect, Respond, Recover.



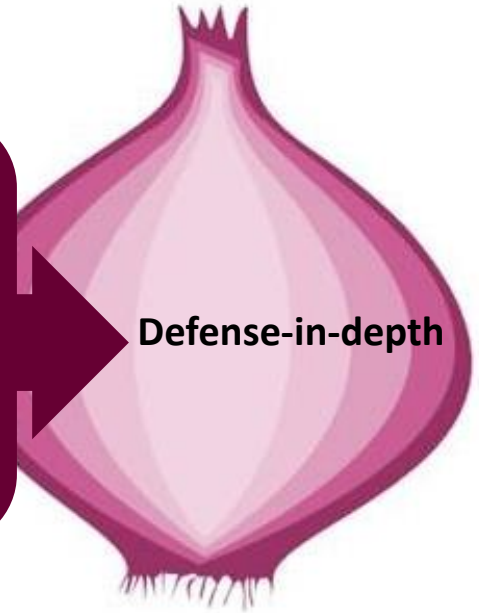
# Cyber Security Assessment & Tools

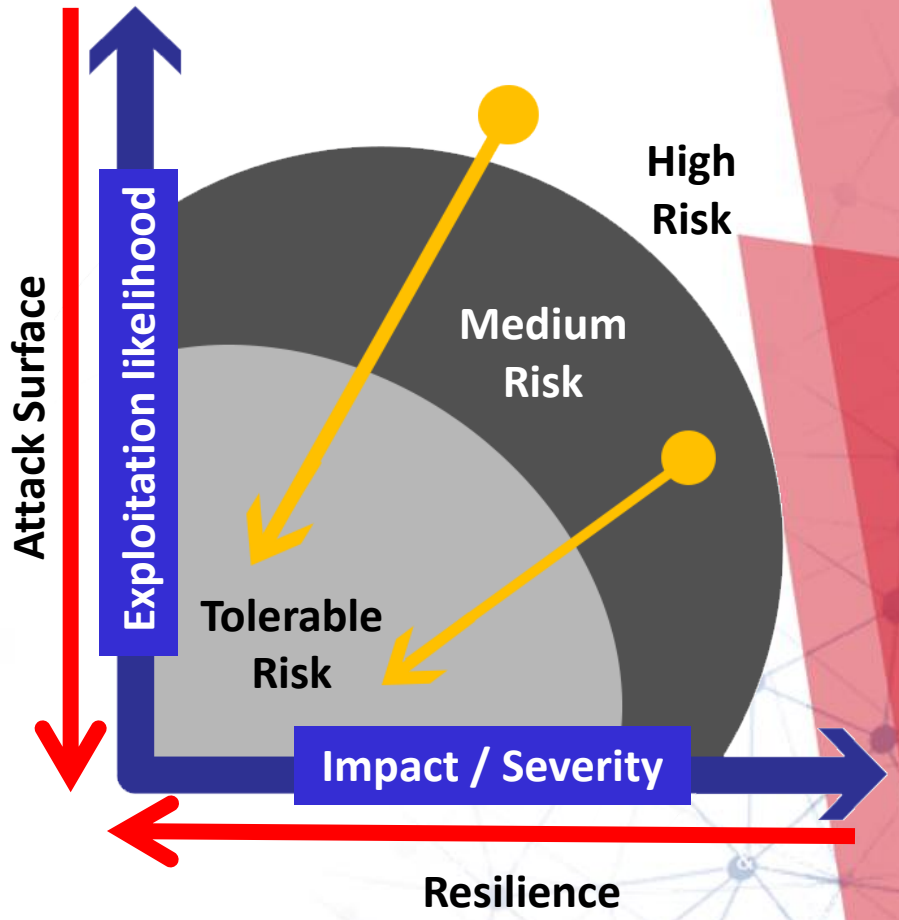
- Cyber Security Evaluation Tool (CSET) from ICS-CERT (of DHS)
- A free desktop software tool that asks the users a series of questions to evaluate their ICS and IT network security practices based on recognized industry standards

# System Controls in ICS

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

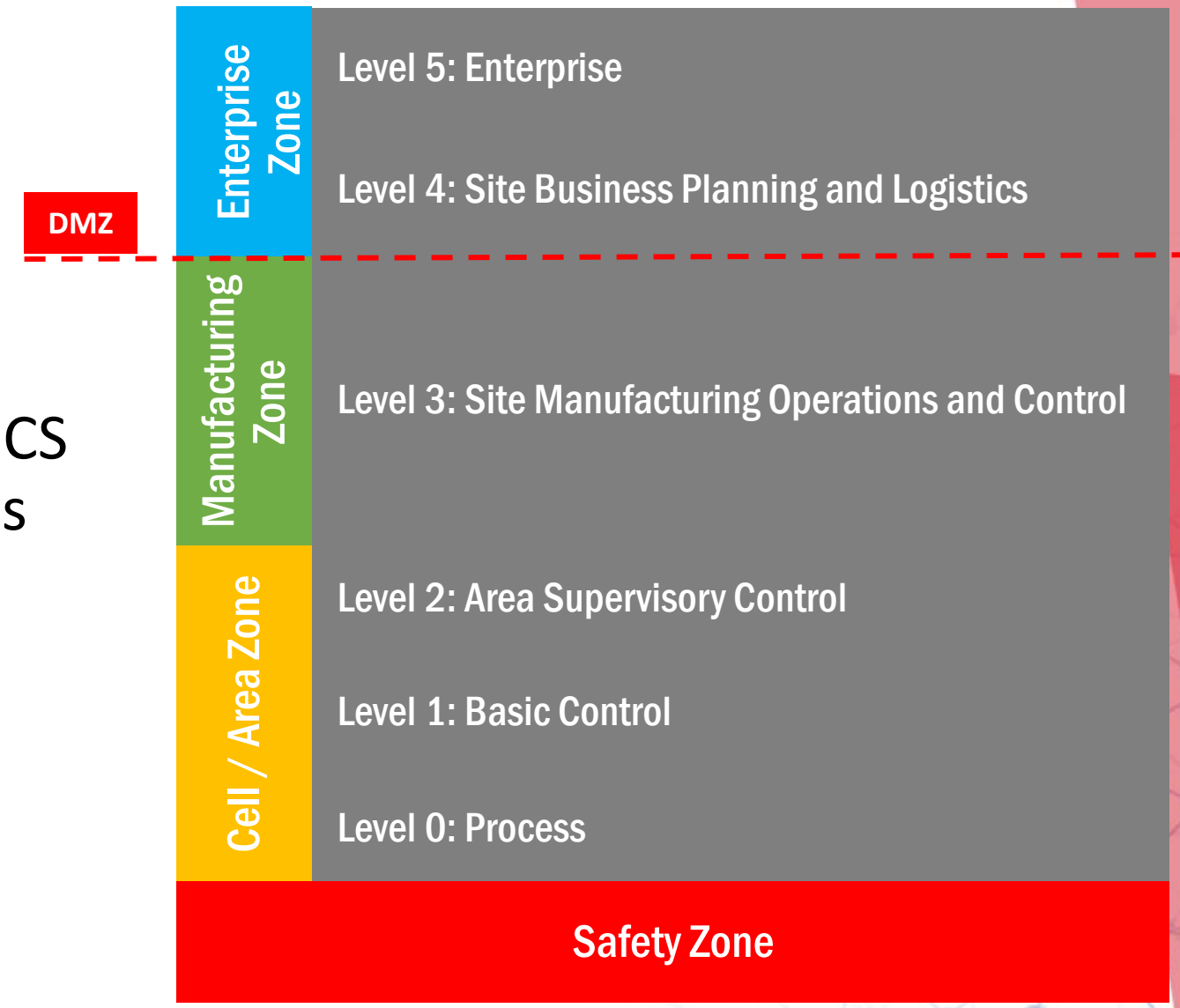
- Policies, Procedures and Awareness
- Physical Security
- Network Security
- Computer Hardening
- Application Security
- Device Hardening



# ICS Security Architecture

- Purdue Model for Control Hierarchy logical framework
- Uses the concept of zones to subdivide an Enterprise and ICS network into logical segments comprising of systems performing similar functions



# Network Security

Protects the availability, integrity and confidentiality of systems against internal and external threats using a variety of security controls

- Network Segmentation or Zoning
- Industrial Firewalls
  - Cater to different OPC Ports
- Network Intrusion Detection and Protection Systems (IPS, IDS)

# Industrial Protocol


**INDUSTRIAL CONTROL**

OPC (OLE for Process Control)

**PROCESS**

PROFINET, CIP (Common Industrial Protocol), EtherNet/IP, HART (Highway Addressable Remote Transducer), Modbus

**BUILDING**

BACnet

**AUTOMOBILE**

CAN Bus (Controller Area Network)

**POWER**

DNP3 (Distributed Network Protocol)

IEC 61850

# Security Application for ICS in the making

- Intrusion Detection System (IDS)
  - Anomaly-based Detection
  - Must teach system to identify “normal” network traffic
  - Detects deviations from normal behaviour
  - More difficult to spoof
  - Needs no foreknowledge of attack signatures
  - May raise more false positives
  - Very hard to implement in a dynamic environment
- Machine learning increasingly being used to form the baseline of “normal” network traffic

# Security Application for ICS

- Industrial Firewall
  - 3eTI CyberFence Family
  - WurldTech OpShield
  - Tofino Xenon
  - Phoenix Contact mGuard Series
  - Moxa EDR Series

May have Deep Packet Inspection (DPI) for various industrial protocols

- Data Diodes
  - Waterfall Security
  - Fox-IT
  - Nexor
  - Vado
- ICS Anomaly Detection
  - SecurityMatters
  - Claroty
  - Darktrace
  - Dragos

# Benefits of DPI for OT

- Enhanced visibility of device interactions – far beyond traditional firewalls (ex: data flow, commands, values etc.)
- Enforced rules on commands & values consistent with the rules of the process
- Option to lock down unused functionality (commands/registers)
- Detect/protect configuration/firmware changes to ICS endpoints
- Validation of messages per protocol standards
- Limitation of messages and commands to un-safe operational scenarios
- Limits impact of potential human error
- Passive implementation that reduces risk of interrupting existing system
- A holistic baseline of interconnected systems for application whitelisting

# Summary

- Cybersecurity needs to be an integral part of the IT/OT convergence.
- IT and OT were supported and managed separately. IT was traditionally associated with business/enterprise systems while OT was associated with field devices and systems for monitoring and control.
- Need to understand IT security may not apply correctly to OT cybersecurity.
- Legacy in technology is one of the many challenges faced where OT devices have virtually no security capabilities as compared to an IT device.
- Not such thing as 100% secure. It's all about:
  - Risk reduction – reduction attack surface, reduce exploitation likelihood.
  - Impact Mitigation – eliminate or reduce impact that cause loss of lives, equipment damage, environmental impact.
  - Have a back-up operational mode

**Be Resilience Beyond Defense!**

# Contact Information

## Presenter Information


| | | |
|---|---|---|
| Presenter Name | : | David Ong |
| Company | : | Attila Cybertech Pte. Ltd. |
| Email | : | david.ong@excelmarco.com |
| Website | : | www.attilatech.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

# Thank You

**Visit us at www.attilatech.com**