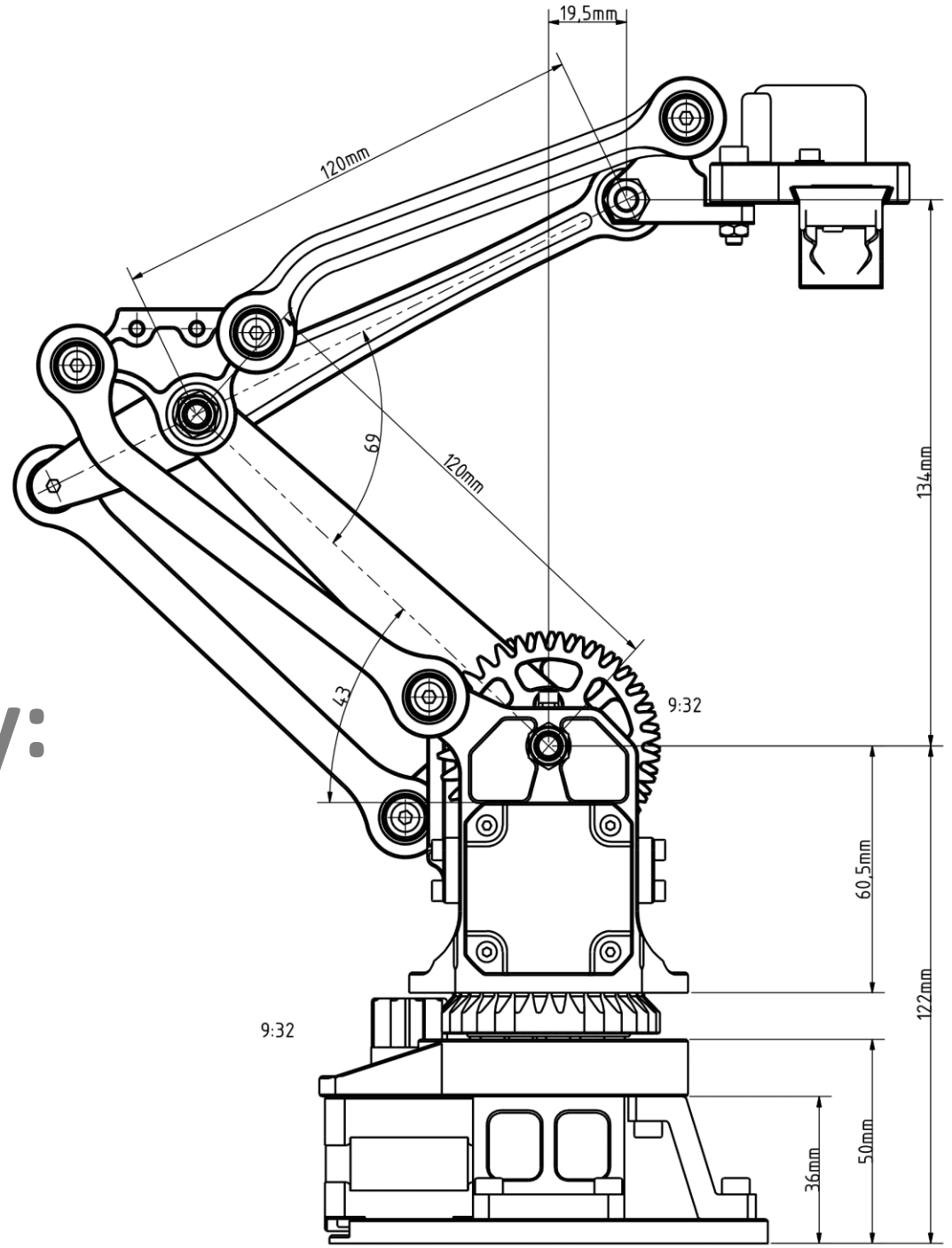
Manufacturing Cybersecurity: Protecting your Shop floor from Cyber Attacks

Tommy Thompson – Lead Consultant, Nclose

KZN Industrial Technology Exhibition

28 July 2017



“If you reveal your secrets to the wind, you should not blame the wind for revealing them to the trees.” — Kahlil Gibran, (Artist, Poet)

Nclose
security within

Introduction

Nclose Overview

Established in 2008 with a focus on IT Security. Started on the Operational Technology Cybersecurity journey 3 years ago. We are one of the very few organisations that offer resources with ICS/SCADA security specific training and certification:

- Nclose consultants have attained the Certified SCADA Security Professional (CSSP) qualification.
- Our consultants have also completed the Operational Security (OPSEC) for Control Systems (100W) and Cybersecurity for Industrial Control Systems (210W) certifications offered by ICS-CERT.

Nclose
security within

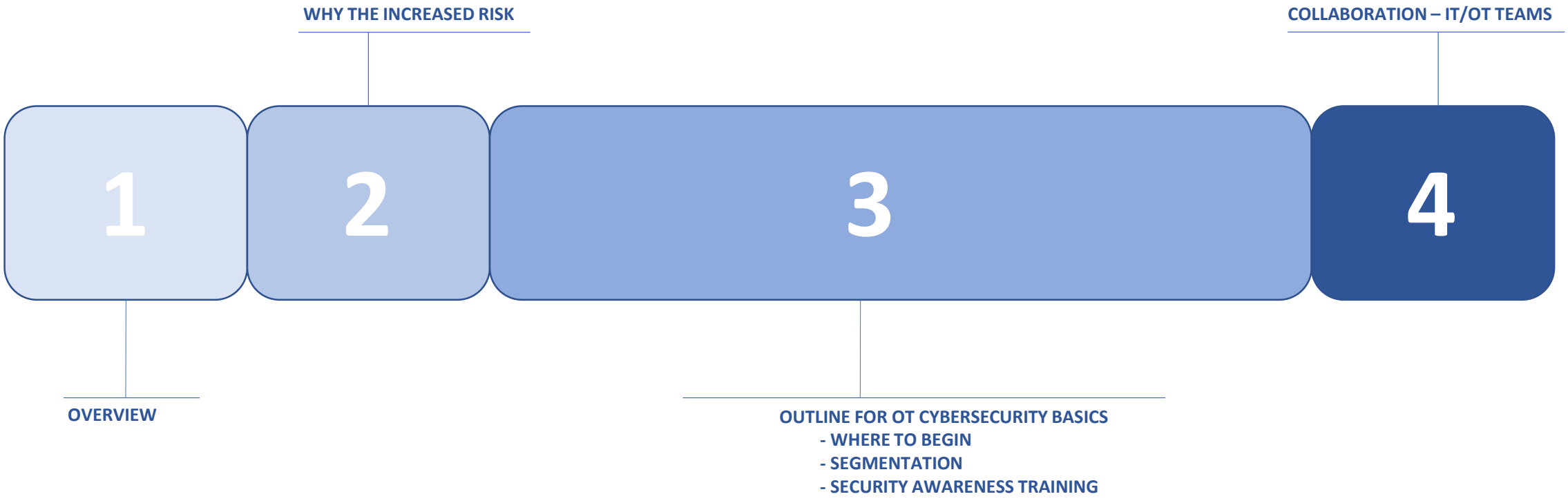
Introduction cont.

Take-away's from today's session:

- No silver bullet for OT Cybersecurity
- The threats are real and increasing
- OT & IT teams collaborating
- Get the basics right
- Segmentation (Purdue Model)
- The Cybersecurity process is continuous
- OT Cybersecurity (and IT Cybersecurity) is a never-ending Chess game

Nclose
security within

Agenda



Nclose
security within

Overview

Operational Technology (OT) defined:

- Supervisory Control and Data Acquisition (SCADA)
- Critical Infrastructure
- Manufacturing Execution Systems (MES)
- Distributed Control Systems (DCS)
- Industrial Control Systems (ICS)

Gartner defined: *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.*

Nclose
security within

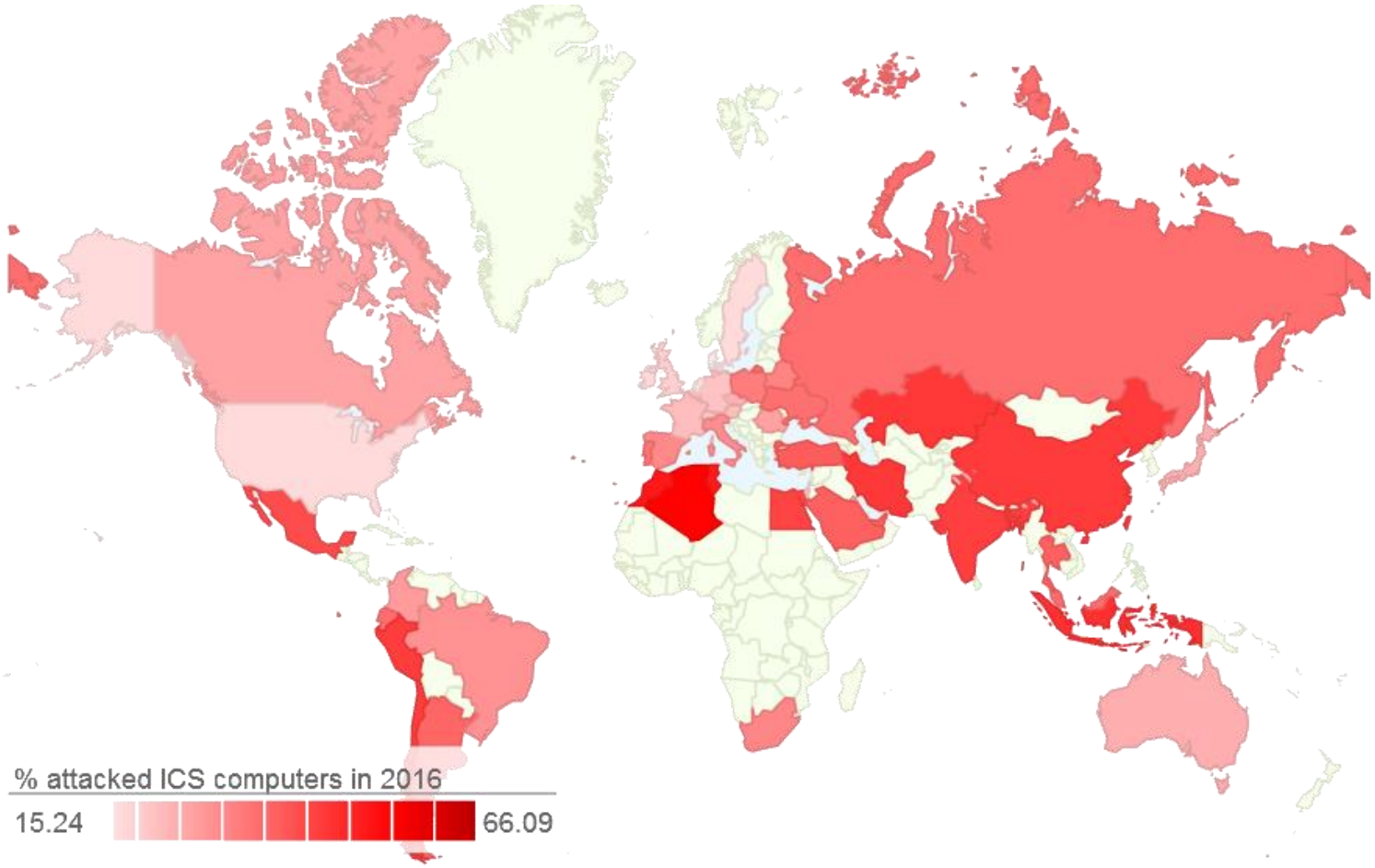
Overview cont.

- Threats to Operational Technology (OT) have increased
- 67% of companies with OT suffered at least one attack in the previous 12 months and 78% expected a successful exploit of their OT systems within the next two years. *
- Systems are becoming more interconnected
- Misunderstanding of the difference between IT (information technology) and OT. OT Cybersecurity concerns are vastly different from IT concerns
- There is little or no training to staff around Cybersecurity

** Ponemon Institute.*

Nclose
security within

Overview cont.

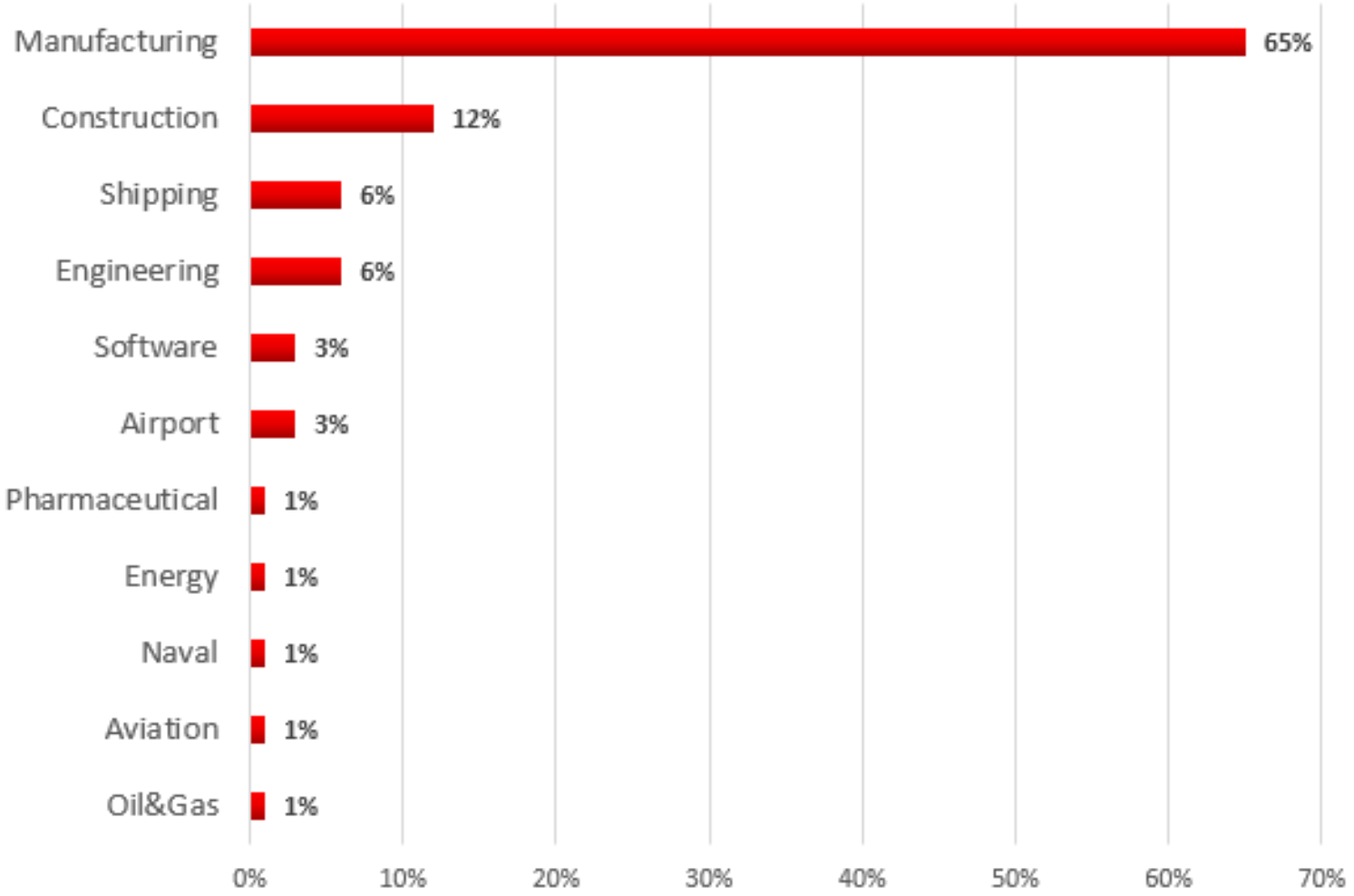


% of Infected OT Computers

- South Africa is at 28%

Nclose
security within

Overview cont.



Who is most affected
(International)

- Manufacturing is at 65%
- Construction is at 12%
- Shipping is at 6%

Nclose
security within

the increased risk to OT networks

Nclose
security within

the increased risk to OT networks

Why the increased risk:

Security Landscape 15 years ago

- Most hacks were initiated by small groups of 1-3 people.
- A firewall and an AV solution were adequate.
- OT networks were separate aka Air Gapped.
- Proprietary protocols (Modbus, PROFINET, DNP) were used for communications.

Security Landscape Today

- Establishment of Cybercriminal gangs, with focused, targeted efforts.
- OT Vendors embracing COTS and adopting open standard protocols like TCP/IP and Bluetooth communications = reduced design time and cheaper solutions.
- Industrial Internet of Things (IIoT)
- Previously separate OT networks are now connected

Nclose
security within

the increased risk to OT networks

Emerging Threats

- Hacktivist Group Activity
- Cybercriminal gangs knowledge on OT/ICS systems is increasing.
- Industrial espionage.
- Ransom/Ransomware attacks on OT/ICS are increasing.
- Specialized Search Engines are now available like ***Shodan.***

Some Examples

- Maroochy Water Services, Australia
- Georgia-Pacific, USA
- Target, USA
- Bowman Avenue Dam, USA
- Kemuri Water Company*, Unknown
- Ukrenergo Power Company, Ukraine

** Pseudonym, Kemuri Water Company, and its location is not revealed.*

Nclose
security within

the increased risk to OT networks

What are the consequences:

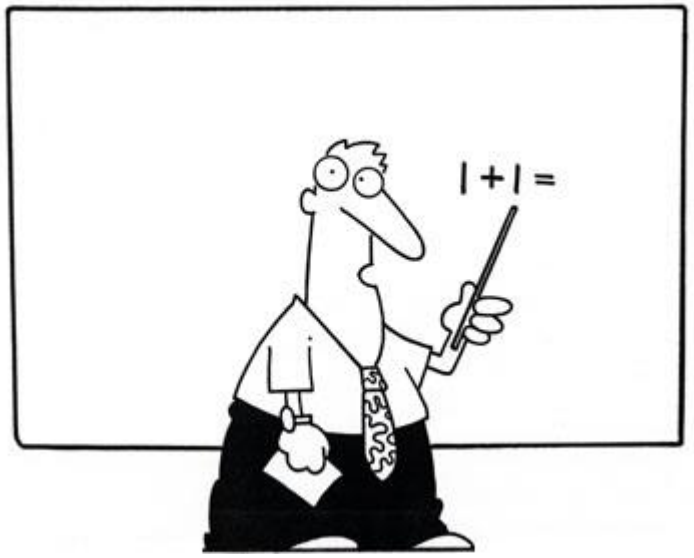
- Hazardous materials released into the environment
- **Stopped production**
- Financial loss
- Potential fines and lawsuits.
- Reputational damage.
- Increased risk to the health and safety of ICS staff.

Nclose
security within

an outline for OT Cybersecurity basics

Nclose
security within

an outline for OT cybersecurity basics



Where to begin

- Establish an OT Cybersecurity Policy/Program
- Perform an OT Risk Assessment (not the same as IT…)
- Implement a passive vulnerability scanning solution.
- Segmentation based on the Purdue Model (PERA)
- Use a secure remote access solution. (with monitoring if possible)
- Ensure there is adequate physical security (i.e. Access Control) to all control rooms and remote stations
- Secure privileged accounts
- Insert Honeypots into the OT Network

Nclose
security within

an outline for OT cybersecurity basics

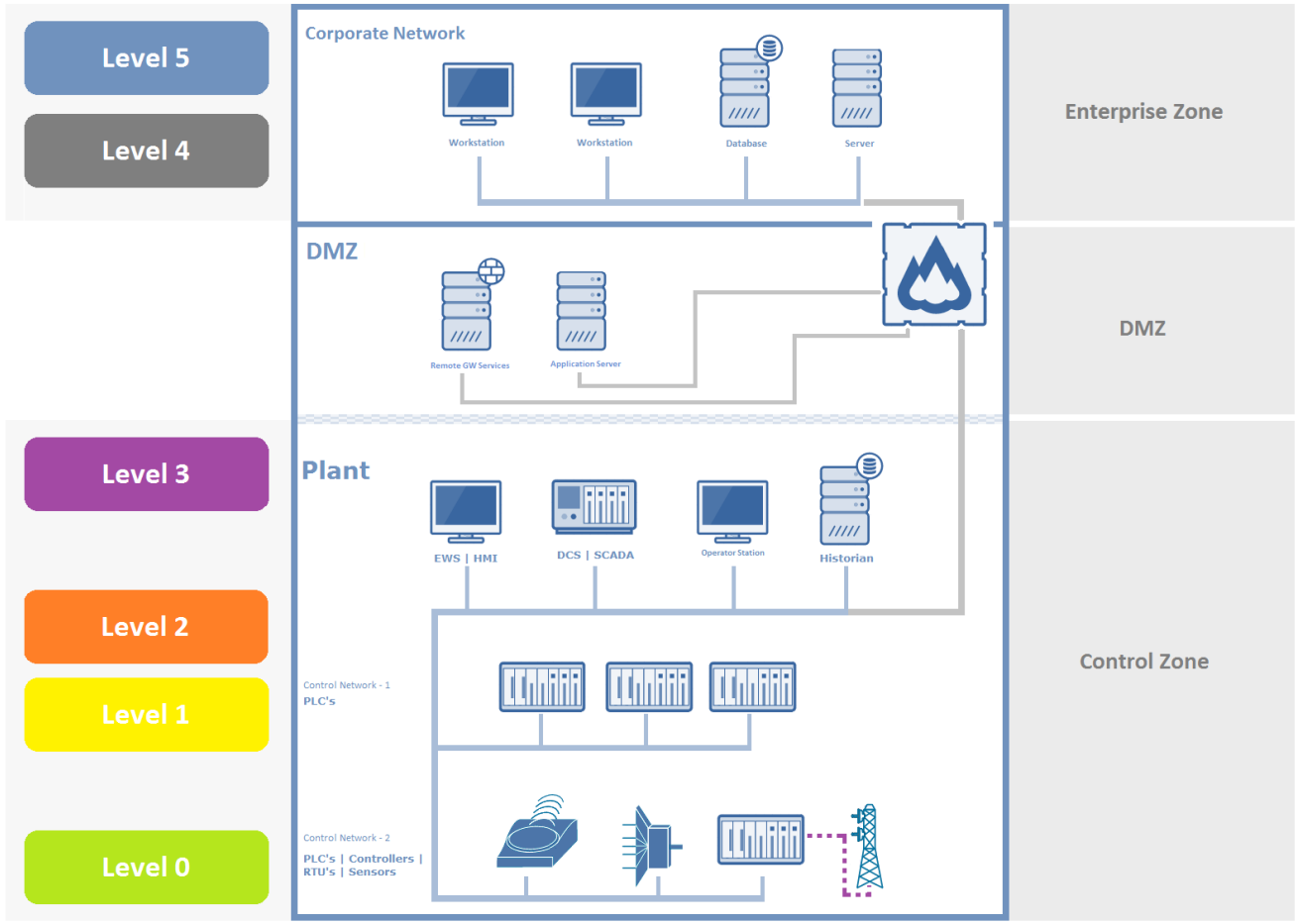
Segmentation

- Purdue Framework (PERA):
  - The Purdue Framework, developed by the Industry-Purdue University Consortium for Computer Integrated Manufacturing. The model consists of 4 zones* and 6 levels of operations.
  - Adopted by ISA/IEC 62443 and NIST 800-82 Cybersecurity Frameworks.
- Create Zones (critical & non-critical):
  - A zone is defined as a group of assets that share common requirements based on aspects such as control, security, criticality and consequence.
  - Define and partition the OT Network into distinct zones
- Define communication channels:
  - All communications between zones must be via a defined Channel
  - This will help to control access, shield other networks and protect network traffic.

Nclose
security within

Purdue Framework

(Purdue Enterprise Reference Architecture – PERA)



- **Level 5:** Enterprise Network
- **Level 4:** Business Planning & Logistics
- **Level 3:** Site Manufacturing and Operations Control
- **Level 2**: Area Control
- **Level 1:** Basic Control
- **Level 0:** Process

Nclose
security within

an outline for OT cybersecurity basics

Security Awareness Training

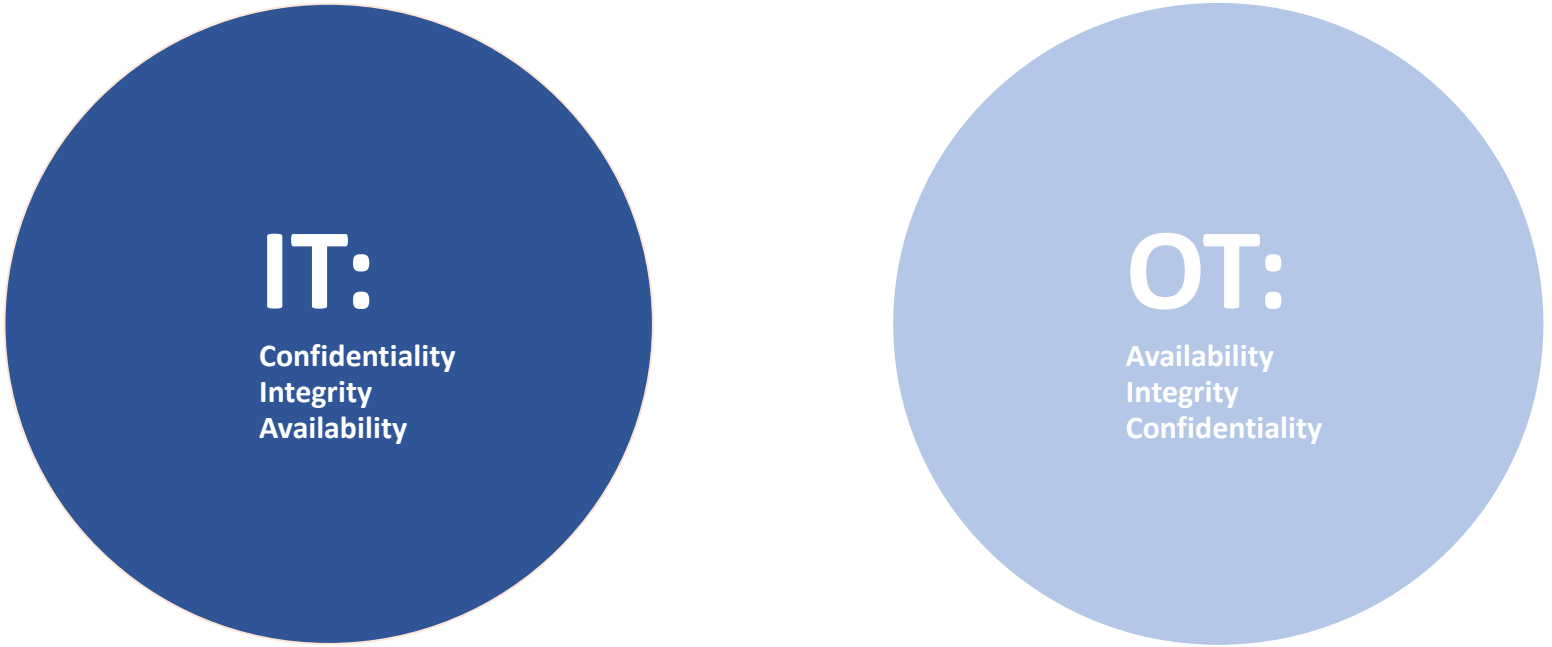
- Make it part of the OT Cybersecurity policy:
  - Training is often overlooked as employees schedules are busy.
  - Add layers of training – Basic | Intermediate | Advanced/Expert
- Increases awareness of the risks associated with OT Networks:
  - Informed and trained employees are better positioned to implement and maintain OT Cybersecurity.

If we can learn 1 valuable lesson from the Stuxnet (and the like), it would be that security training needs to be implemented as part of the OT Cybersecurity policy. If the employees had known about the potential risk by inserting a random USB drive into an OT Network, the likelihood of them doing so would have been greatly reduced.

Nclose
security within

collaboration between IT & OT teams

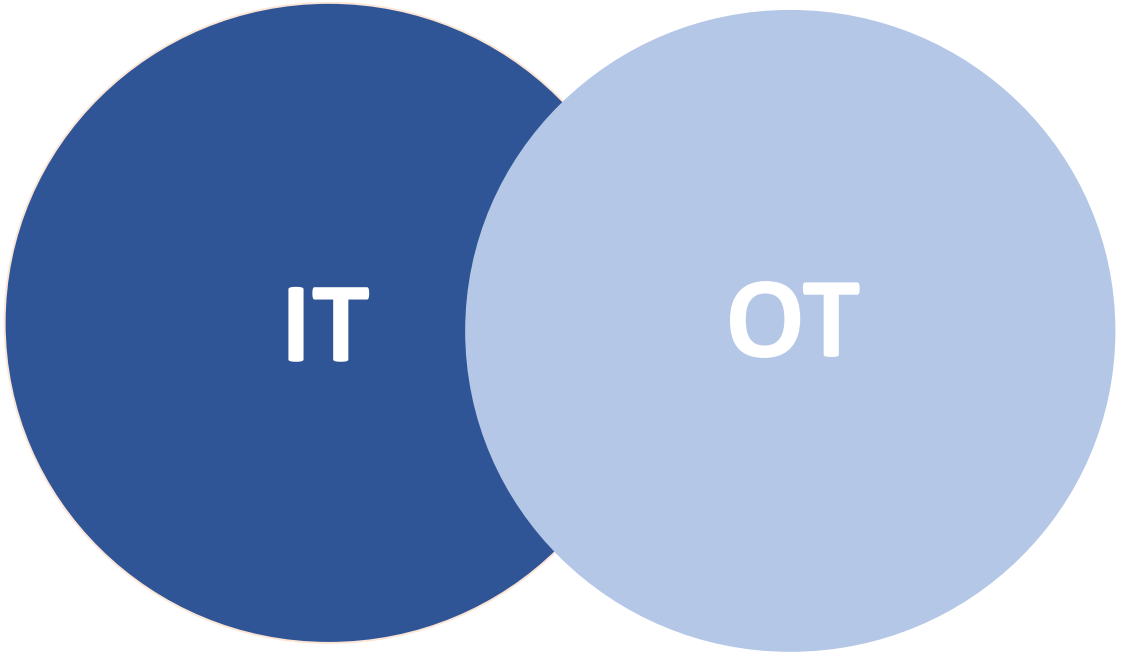
collaboration between IT & OT Teams



- A world apart for OT Cybersecurity
- IT says its an OT problem
- and OT says its an IT problem
- So who's problem is it??
- Well it's both…

Nclose
security within

collaboration between IT & OT Teams



- There has to be synergy between both teams
- IT Understands the cybersecurity problem
- OT understands OT and its unique requirements
- 70/30 split between risks
- Create a team with an accountable resource(s)

Nclose
security within

Closing

Securing our OT Systems is not a one woman/man job! Working together, communicating openly, and collaborating with each other will be beneficial to increase our overall maturity level.

Security waits for no one, get started today.

Operational Technology Cybersecurity Group Africa (OTCGA):

- https://www.linkedin.com/groups/13504917
- www.otcga.org

Nclose
security within