OT / ICS – COMMON MISTAKES AND RAPID RETURN ON INVESTMENT

ASSESSMENT PLUS

#WHOAMI – GAVIN DILWORTH

Background: Operator, Control System Engineer / Industrial Automation Engineer, Managing Consultant

Experience: 17 Years in OT / ICS environments

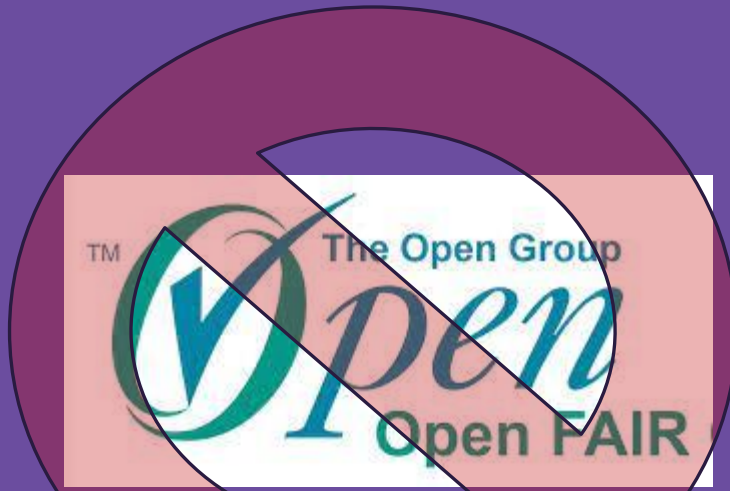
Qualifications:

- Master of Professional Practice in ICS Cyber Security
- Graduate Diploma in Project Management
- Advanced Diploma in Industrial Automation
- SANS GICSP and GRID
- Offensive Security: OSCP
- Assessing and Exploiting Control Systems and IIoT
- ISA/IEC-62443 Expert

WHAT THIS TALK IS NOT ABOUT – RETURN ON INVESTMENT

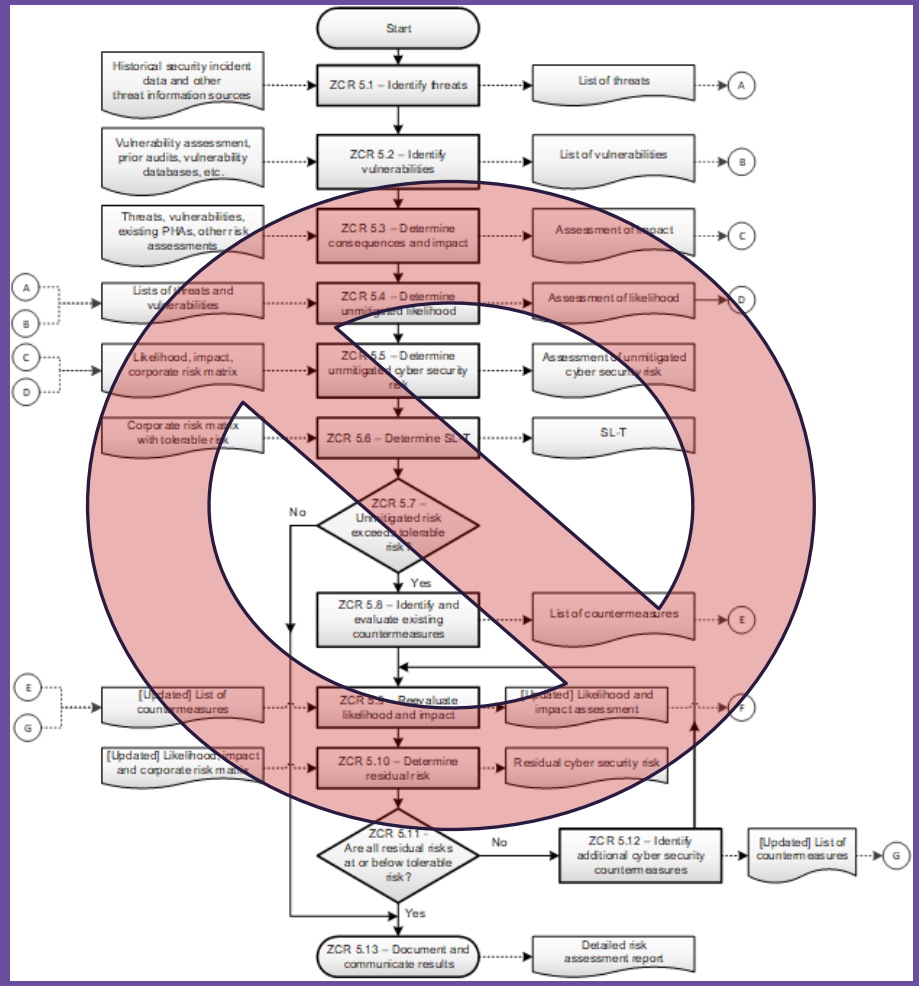
- Douglas W. Hubbard & Richard Seiersen – How to Measure Anything In Cyber security Risk

- Open FAIR (Factor Analysis of Information Risk)



WHAT THIS TALK IS NOT ABOUT – THE 'CORRECT' METHOD

- Doing it the right way is easy, get the right budget, right people, with the right culture and follow a process like ISA/IEC-62443



ASSESSMENT PLUS

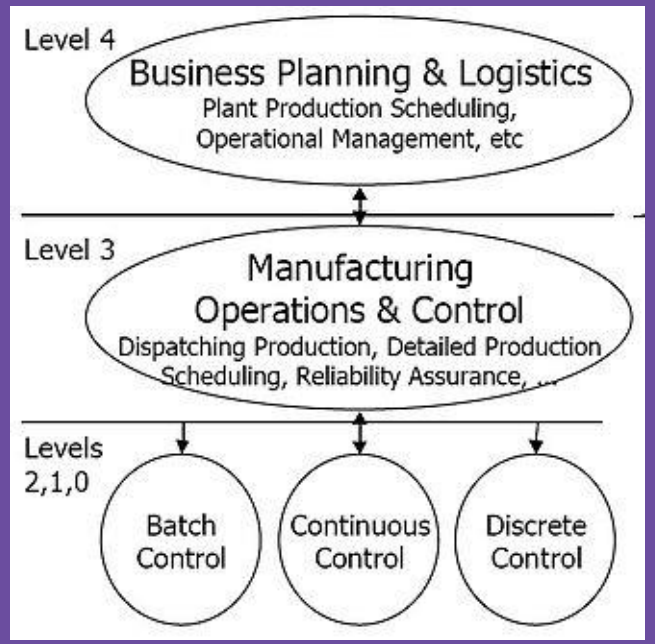
WHAT THIS TALK IS ABOUT – INDUCTIVE REASONING

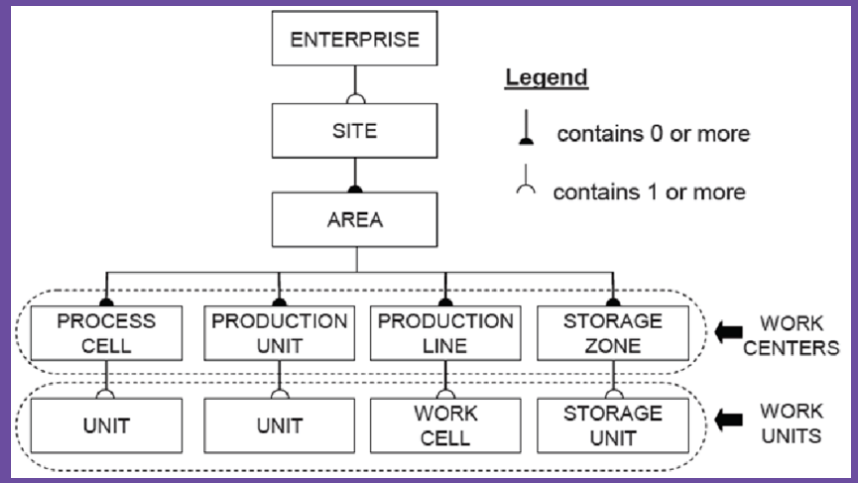
Inductive reasoning is a method of reasoning in which a general principle is derived from a body of observations. It consists of making broad generalizations based on specific observations.

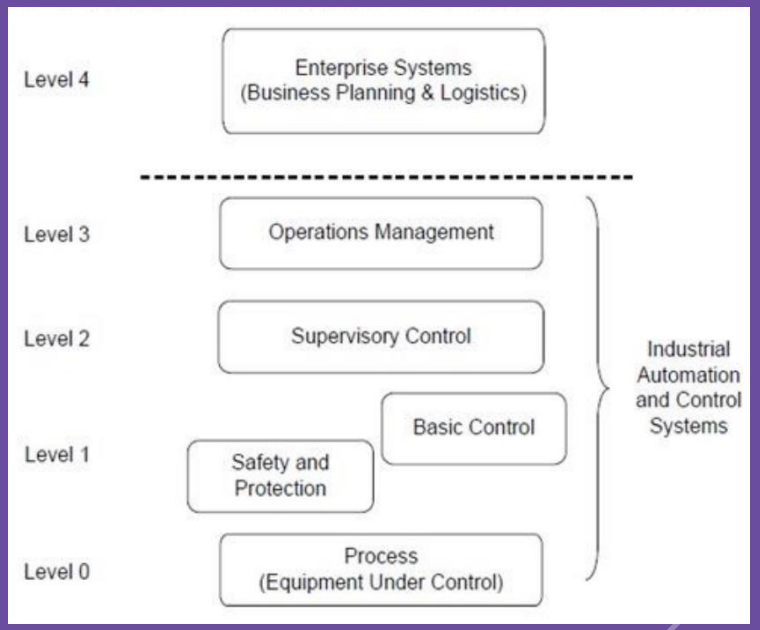
- https://en.wikipedia.org/wiki/Inductive_reasoning

INTRODUCTION - PURDUE MODEL TYPES

Purdue University != ISA-95 != IEC-62443







INTRODUCTION - PURDUE MODEL – ISA/IEC-62443

IEC 62443 Purdue Model – based on function

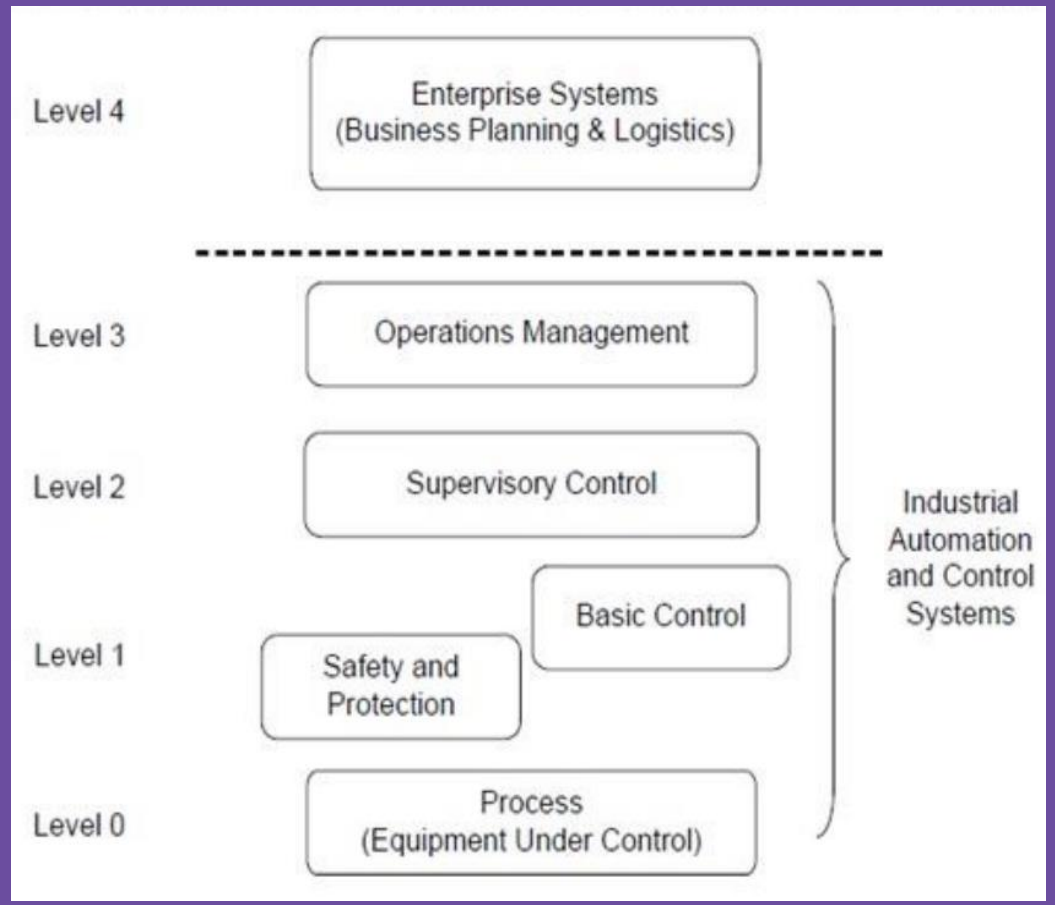
Level 4: Enterprise Systems
General IT Systems (Servers, Workstations)

Level 3: Operations Management
Historians, Domain Controllers, Jump Hosts, File Servers

Level 2: Supervisory Control
Local Visulisation

Level 1: Basic Controllers and Safety/Protection
PLC, Controllers, IED's potentially RTU's

Level 0: Process
Instruments, Sensors and Actuators



COMMON MISTAKES #1 - TERMINOLOGY

- Adapt to the organisation's terminology
- Don’t bring in yours.

COMMON MISTAKES #2 – STARTING AND DOING NOTHING OR THINKING YOU CAN'T START WITHOUT KNOWING ALL THE RISKS

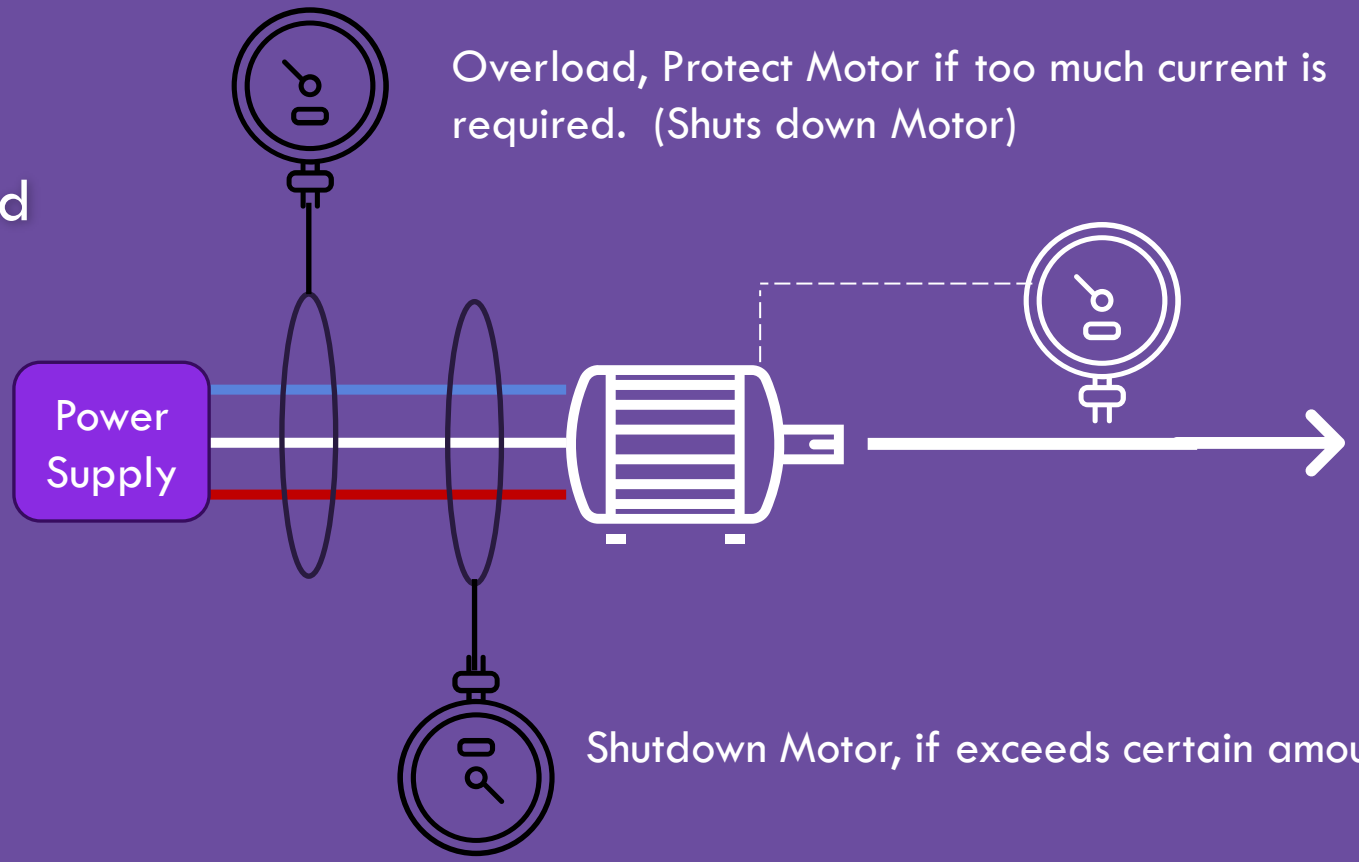
- Spending Three Years to Identify Risk and not implement any Security Controls or Countermeasures
- Doing the inverse (no Risk Management)
- Arguing over the basic's
- Stagnating program of works

COMMON MISTAKES #3 – SHOOTING FOR PERFECT

- Perfect in the enemy of good
- Good enough, is….. good enough
- Cyber Security Risk as a fraction of the business Risk

COMMON MISTAKES #3 – SHOOTING FOR PERFECT – CONTI'D

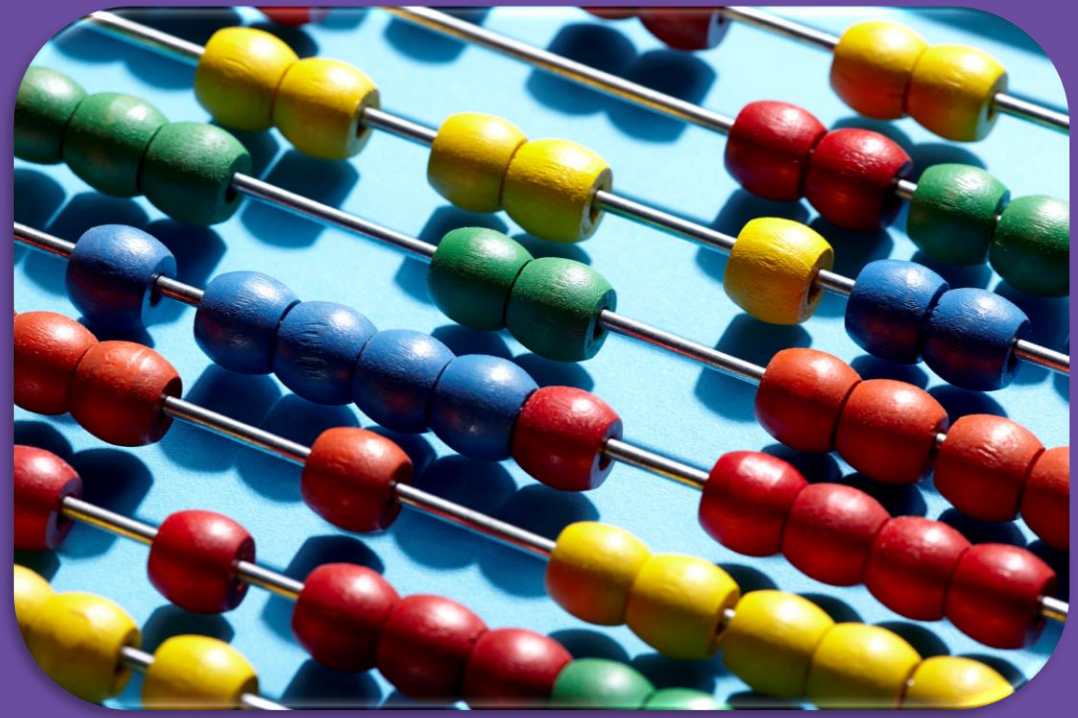
- Motor is controlled based on transmitter output
- Overload Transmitter (protection)
- Another Transmitter?



COMMON MISTAKES #3 – SHOOTING FOR PERFECT – CONTI'D

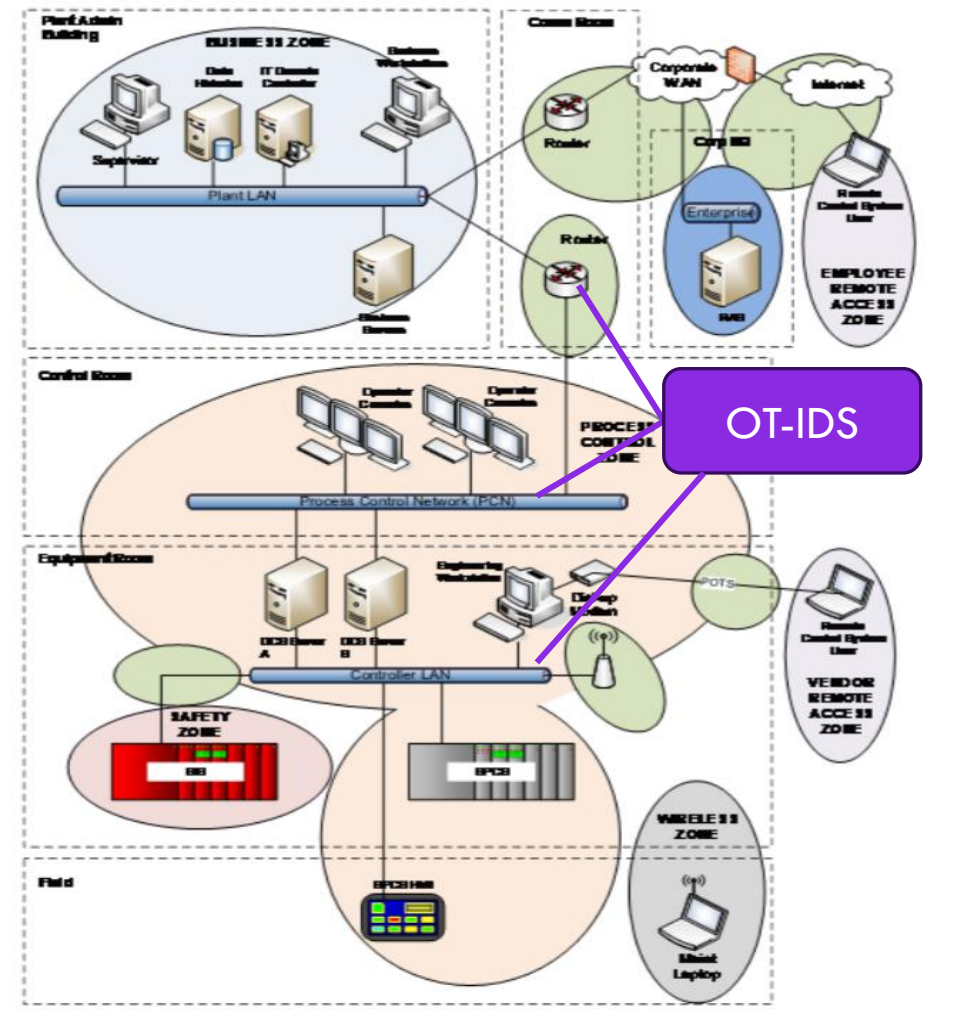
- Yellow is the adjustable current trip setpoint
- This would be sitting on Level 0 of the purdue model

COMMON MISTAKES #4 – ASSET INVENTORY



- Using a Network IDS and expecting perfect results.
- Scanning tools are extremely dangerous in a production environment.
- Scanners have to be designed for OT
- Sometimes pen and paper can be the most effective.

COMMON MISTAKES #4 – ASSET INVENTORY – CONTI'D

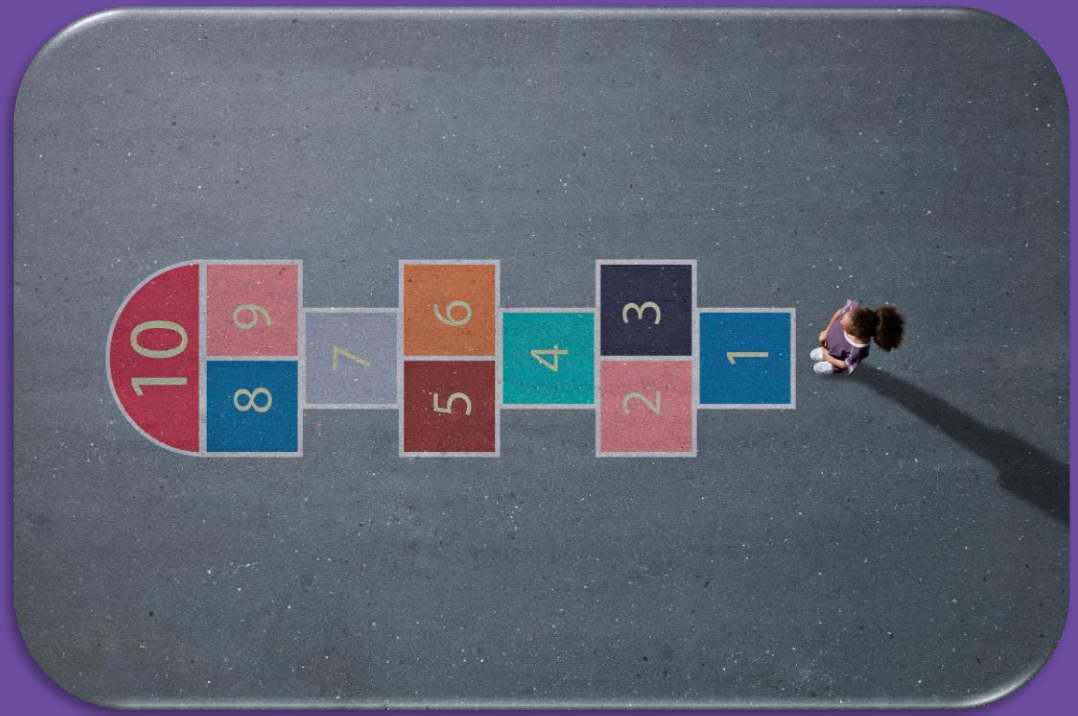


- Deploying an OT-IDS (Network Intrusion Detection System)
- Need that second link for decent coverage.
- Side Note, Asset Inventories require a software list as well.

COMMON MISTAKES #5 – NOT DOING TABLETOP EXERCISES (TTX)

- A Practice run
- An Exercise in understanding what you don't know
- Should be regular occurrence

COMMON MISTAKES #6 – TRYING TO MOVE TOO QUICKLY



- A lot of frustration with senior management,
- It's a lack of understanding
- Things are done in phases

COMMON MISTAKES #7 – THINKING EVERYONE CARE'S

- Perfect in the enemy of good
- Good enough, is….. good enough

COMMON MISTAKES #8 – PHYSICAL SECURITY

- Physical Security is underrated
- It's doesn't get the attention it deserves. Neither does BMS (Boiler Management Systems? , Burner Management Systems?, Building Management Systems?)
- If anyone can rock up and plug into your ICS / OT devices you're in trouble.

RAPID RETURN ON INVESTMENT (ROI)

WHAT THIS TALK IS NOT ABOUT – RETURN ON INVESTMENT

- Douglas W. Hubbard & Richard Seiersen – How to Measure Anything In Cyber security Risk

- Open FAIR (Factor Analysis of Information Risk)

RAPID RETURN ON INVESTMENT - THEORY

- It's about creating a story, a timeline of self-improvement
- Most self-improved certificate, that's you/your company

RAPID RETURN ON INVESTMENT - THEORY

- You don’t know, what you don’t know
- Highlight Assumptions
- Keep documenting your progress even if it looks like failure
- The documented reports are your story

RAPID RETURN ON INVESTMENT - THEORY

- It's not failure
- It will not hurt your career
- You now know more than when you started

RAPID RETURN ON INVESTMENT – PRACTICAL, THE HOW

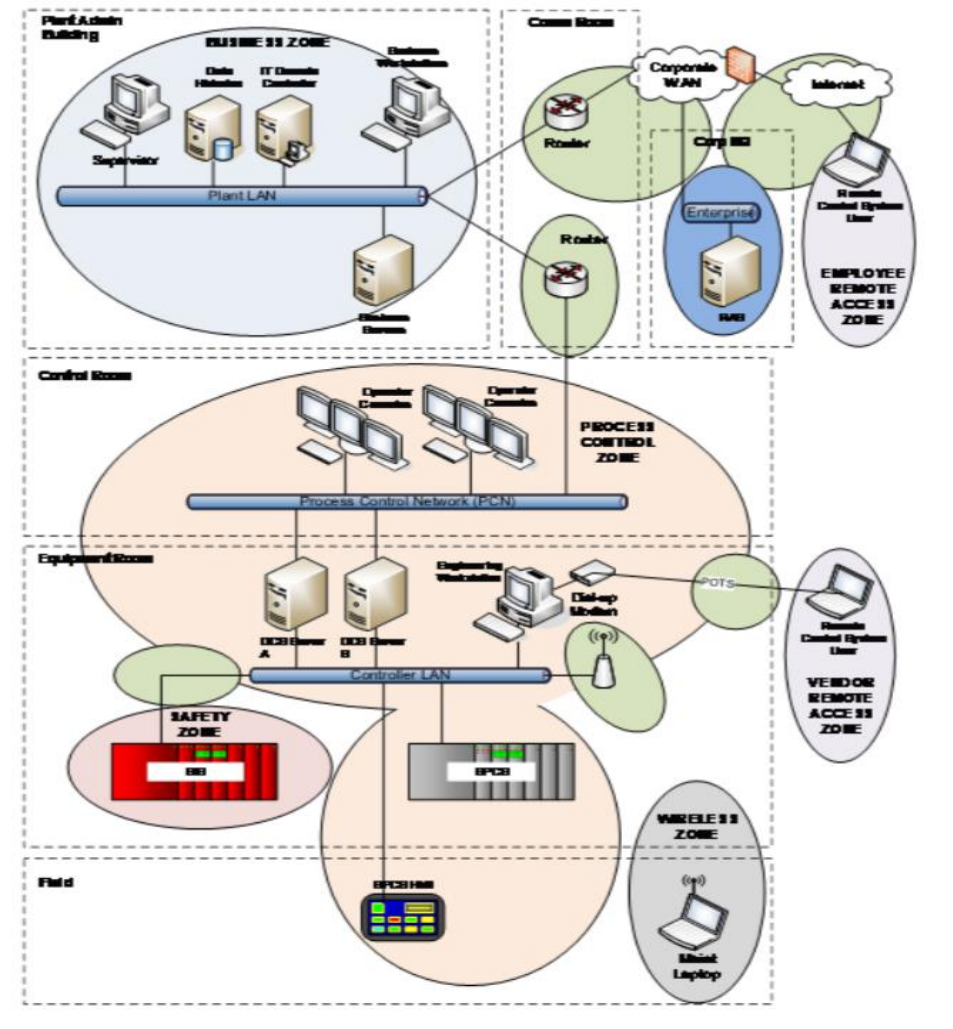
OK but how, how do I actually:

- Reduce my risk
- Demonstrate ROI

RAPID RETURN ON INVESTMENT – PRACTICAL, THE TECHNICAL

- Disaster Recovery, make sure you can restore from a Situation ‘Black’.
- System Hardening.
- Patching is difficult but can be done.
- Logging can be enabled
- Use what you’ve got

RAPID RETURN ON INVESTMENT – PRACTICAL, THE REPORTING



- System by System
- Zone by Zone
- Level by Level

- Restoring: configuration, OS's, functionality
- Hardening and patching

KEY TAKE AWAY'S

- Have a sense of humour, even when talking at a serious event
- There are plenty of mistake to make, focus on the basic's, don't go for perfect
- Use what you've got
- Tabletop Exercises (TTX) can achieve a lot, test many things from physical security to disaster recovery
- ROI is hard to quantify, start with documenting your steps