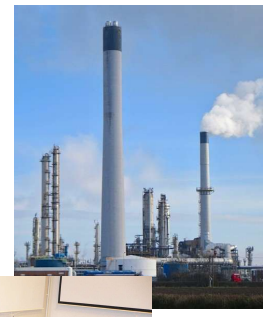
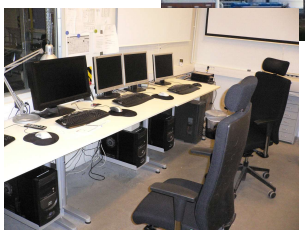
# Cybersecurity Table-Top Exercise (TTX) for Power Plants





**MLM-020-C**

| | |
|---|---|
| Industry | – Process Industry |
| Principal Role | – All |
| Professional Role | – Control Engineer + IT Specialists |
| Enterprise Phase | – All |

Turn on your audio and click start to begin video

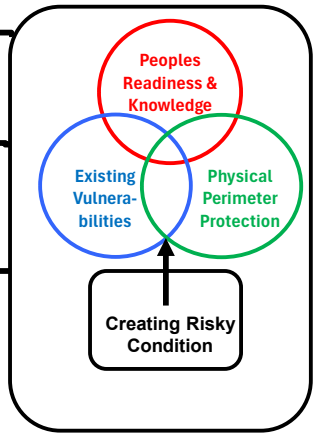
START

This MLM provides an introduction to the use of Table-Top Exercises for Process Industry plants. It is intended for design engineers and plant engineers who will use Table-top studies to investigate cybersecurity issues in Power Plants and other Process industry facilities.

Click the NEXT button when you are ready to advance to the next slide.

## The Cyber Attack Surface - 3 Main Vectors

- **Internally Generated Cyber Attacks**
  - Start with breaching the physical perimeter
  - The attacker can be an employee, visitor, or hacker
- **Externally Generated Cyberattacks**
  - May start through external networks or the internet with Social Engineering
  - May operate for months prior to being detected
- **Supply Chain Cyber Attacks**
  - Vendors of products and supply services
  - Expert service personnel (in the country or abroad)
  - Increased frequency of Remote support access > Higher Risk





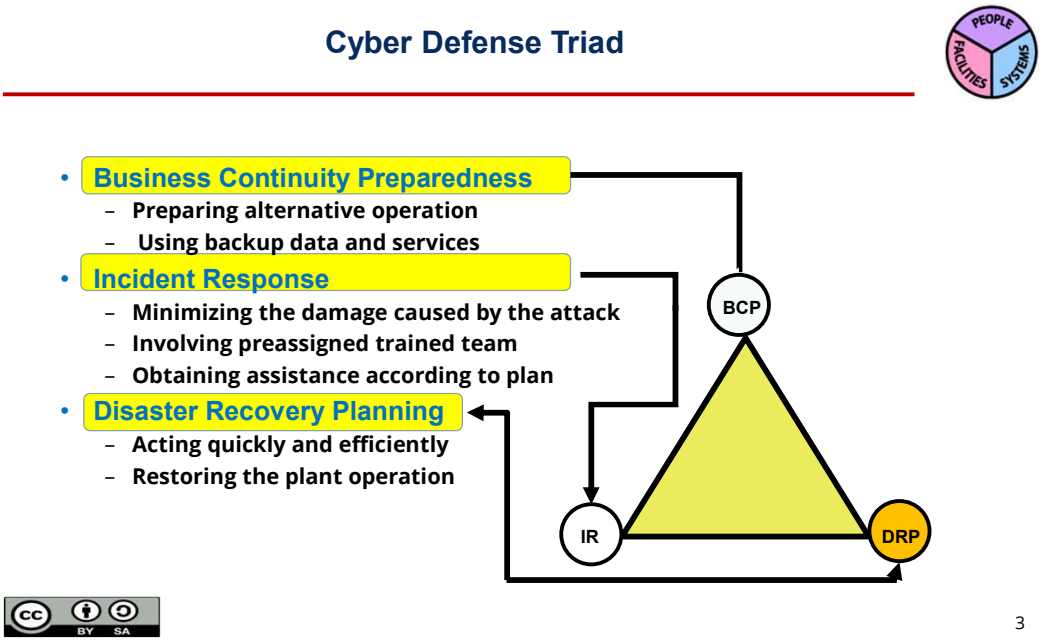

2

Internally Generated Cyber Attacks
- Start with breaching the physical perimeter
- The attacker can be an employee, visitor, or hacker

Externally Generated Cyberattacks
- May start through external networks or the internet with Social Engineering
- May operate for months prior to being detected

Supply Chain Cyber Attacks
- Vendors of products and supply services
- Expert service personnel (in the country or abroad)
- Increased frequency of Remote support access > Higher Risk

## Cyber Defense Triad



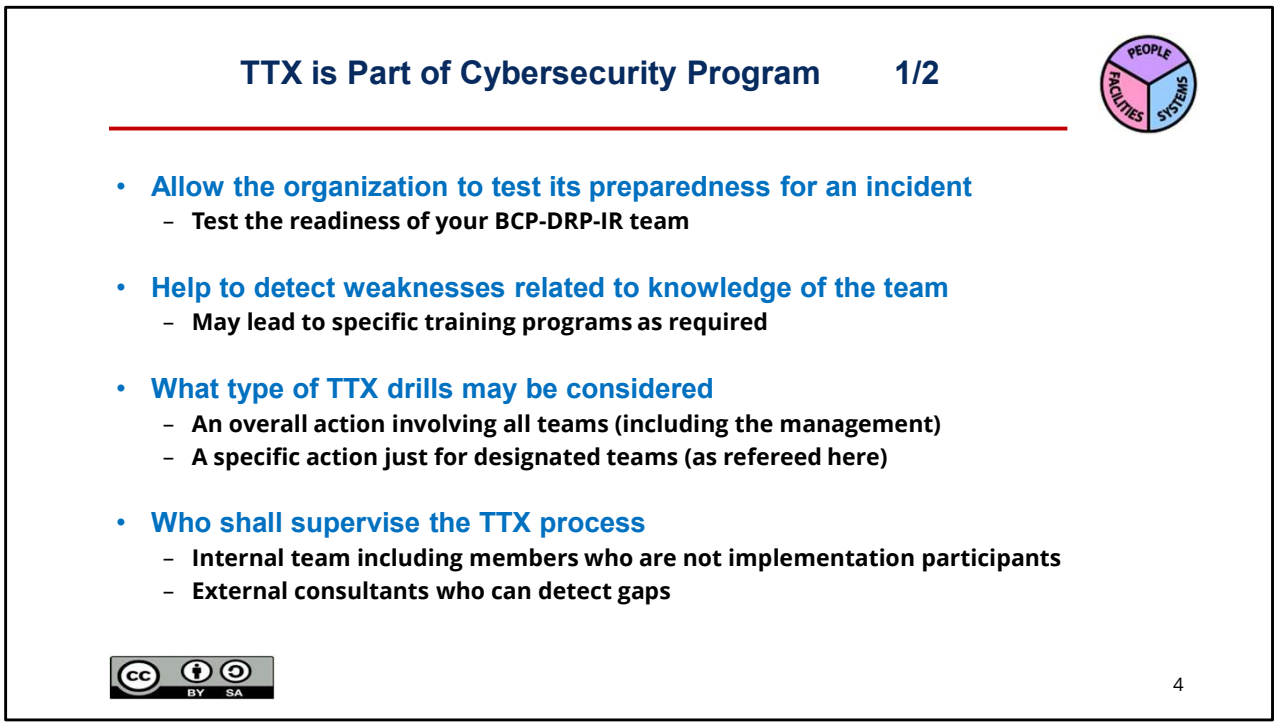

- **Business Continuity Preparedness**
  - Preparing alternative operation
  - Using backup data and services
- **Incident Response**
  - Minimizing the damage caused by the attack
  - Involving preassigned trained team
  - Obtaining assistance according to plan
- **Disaster Recovery Planning**
  - Acting quickly and efficiently
  - Restoring the plant operation






3

The time base of Business Continuity Preparedness (BCP) is years,
Incident Response is minutes, and
Disaster Recovery Planning (DRP) is weeks.



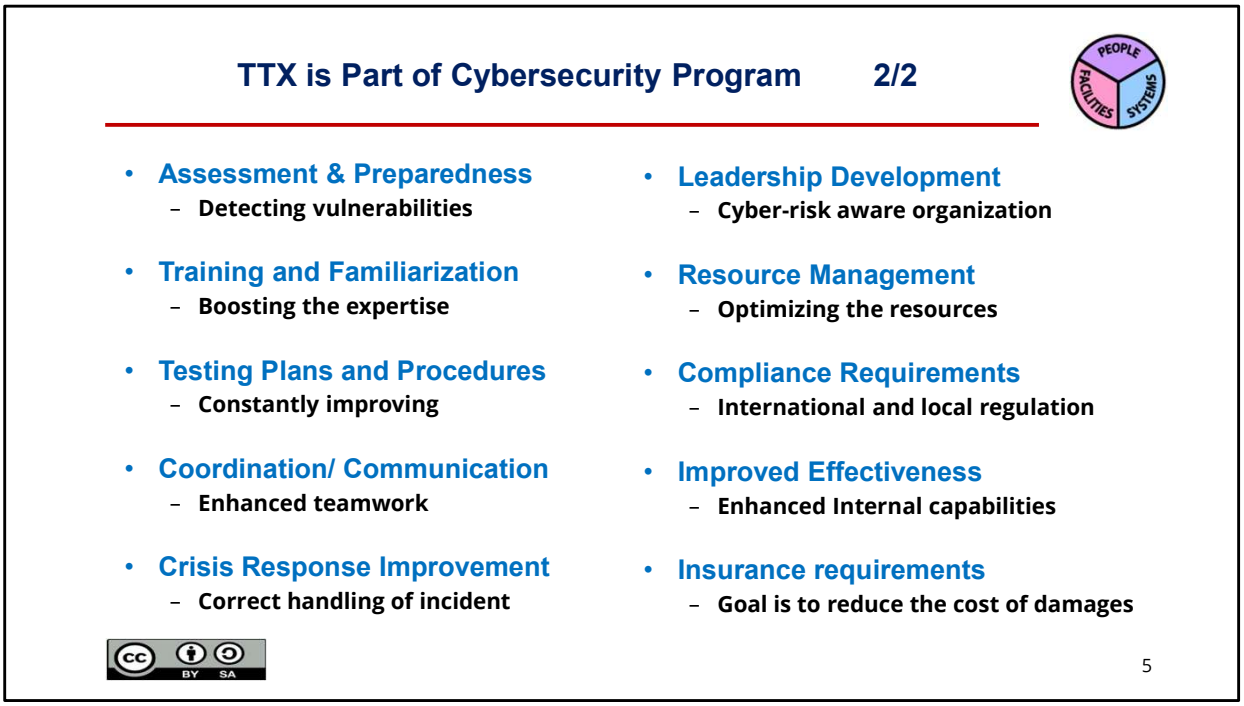

The Table Top Exercise is part of the Cybersecurity Program which has the following objectives:

Allow the organization to test its preparedness for an incident
Test the readiness of your BCP-DRP-IR team

Help to detect weaknesses related to the knowledge of the team
May lead to specific training programs as required

What type of TTX drills may be considered
An overall action involving all teams (including the management)
A specific action just for designated teams (as refereed here)

Who shall supervise the TTX process
Internal team including members who are not implementation participants
External consultants who can detect gaps

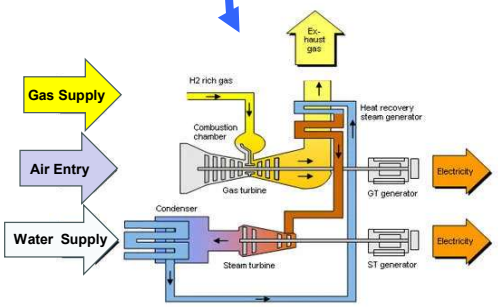



Other TTX objectives include:

- Assessment & Preparedness -Detecting vulnerabilities
- Training and Familiarization - Boosting the expertise
- Testing Plans and Procedures - Constantly improving
- Coordination/ Communication - Enhanced teamwork
- Crisis Response Improvement - Correct handling of the incident
- Leadership Development - Cyber-risk aware organization
  Resource Management - Optimizing the resources
- Compliance Requirements - International and local regulations
  Improved Effectiveness - Enhanced Internal Capabilities
  Insurance requirements - Goal is to reduce the cost of damages

# Combined Cycle Power Plant Example

- **Combined Cycle Power Plant (CCPP) Main Components**
  - Supply& Storage of Gas
  - Gas Turbine operation
  - Heat transfer to boiler
  - Steam Boiler function
  - Steam Turbine operation
  - Power generator
  - Step-up transformer.
  - Protected HV feeders
  - Onsite control room
- **Process Areas**
  - Gas Supply
  - Gas Turbine
  - Steam Boiler
  - Electric Power



## Typical scenarios examined in TTX

- **Typical Incident Scenarios examples**
  - **The HMI Screen is not getting field updates**
  - **The Power Plant stopped producing energy**
  - **Alert on severe vibration of the gas turbine**
  - **The mouse on the HMI screen is moving**
  - **CCTV shows people near the generator**
  - **The operator sees high boiler pressure**



7

Typical Incident Scenarios Examined in the Table Top Exercise:

- The HMI Screen is not getting field updates
- The Power Plant stopped producing energy
- Alert on severe vibration of the gas turbine
- The mouse on the HMI screen is moving
- CCTV shows people near the generator
- The operator sees high boiler pressure

## Typical Incident Response Actions

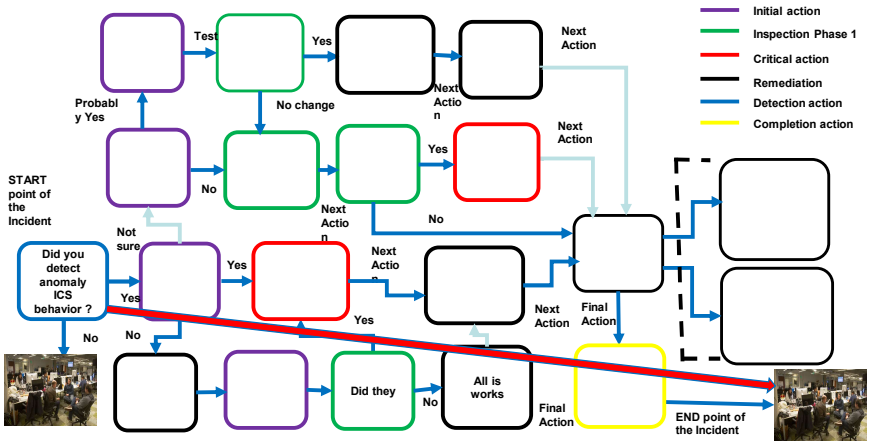

- **Incident response actions**
  - **How to detect accurately?**
  - **Who must participate?**
  - **How to Respond quickly?**
  - **Conduct Emergency Shut Down (ESD)**
  - **Conduct Controlled Shut Down**
  - **How to Investigate the incident?**
  - **Documenting the event?**
  - **Public Relations Handling**

8

Incident response actions include:

- How to detect an incident accurately?
- Who must participate?
- How to respond quickly?
- Conduct Emergency Shut Down (ESD)
- Conduct Controlled Shutdown
- How to Investigate the incident?
- Documenting the event?
- Public Relations Handling

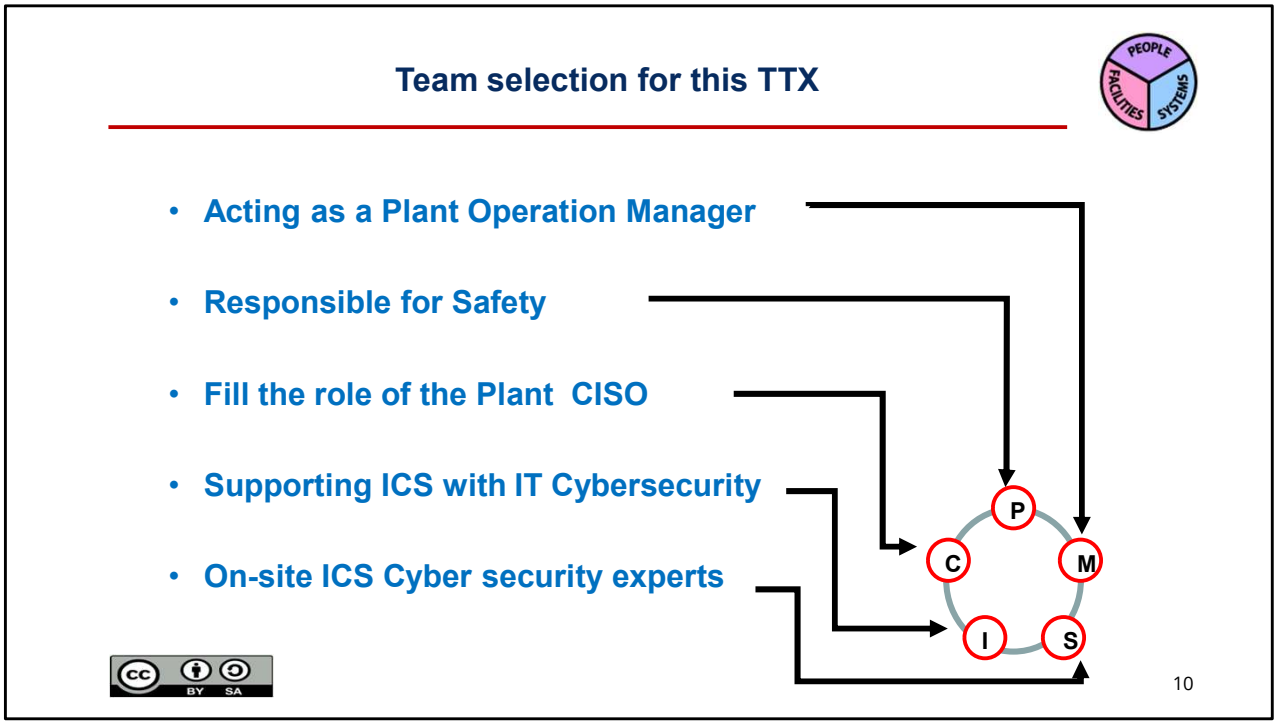
## TTX Example for a Combined Cycle Power Plant






9

Typical Work Process used in response to an incident in a Combined Cycle Power Plant




The TTX team should be include individuals who will:

Act as a Plant Operations Manager - Dealing with IR and the preparedness of the organization

Responsible for Physical Security and Safety - 1-2 people dealing with physical security and safety assurance

Fill the role of the Plant CISO - Ensures the technical/regulatory compliance requirements

Supporting ICS with IT Cybersecurity - 2-4 Dealing with all aspects related to network connectivity

On-site ICS Cyber security experts - 2-4 people capable of dealing with the on-site process and appliances

## Incident - The HMI is not getting updates 1/4

### Assessing the seriousness of the Incident

| Concerns and Risks | Fin. Losses | Bus. Cont. | Damage | Safety | Risk to Lives |
|---|---|---|---|---|---|
| ?- Unknown/ H-High/ M-Medium/ L-Low | L | L | M | L | L |

- no immediate risk of severe damage to equipment
- no immediate risk to people
- The decision is to start an investigation of the incident





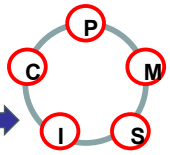
The team decided that there is no immediate risk of severe damage to equipment and no immediate risk to people.

The decision is to start an investigation of the incident by calling several specialists to the control room

# Incident - The HMI is not getting updates 2/4

| Concerns and Risks | Fin. Losses | Bus. Cont. | Damage | Safety | Risk to Lives |
|---|---|---|---|---|---|
| ?- Unknown/ H-High/ M-Medium/ L-Low | L | L | M | L | L |

- **Whom to dispatch to help?**
  - **P?** Responsible for Physical & Perimeter Security
  - **M?** The CCPP Manager responsible for operations?
  - **S?** On-site Industrial Cyber Security Expert
  - **I?** Onsite Information technology cyber security expert?
  - **C?** The onsite person filling the role of a CISO




- **Whom to dispatch to help?**
  - **IT Cybersecurity Experts (I)**
  - **ICS Cyber security experts (S)**

# Incident - The HMI is not getting updates 3/4

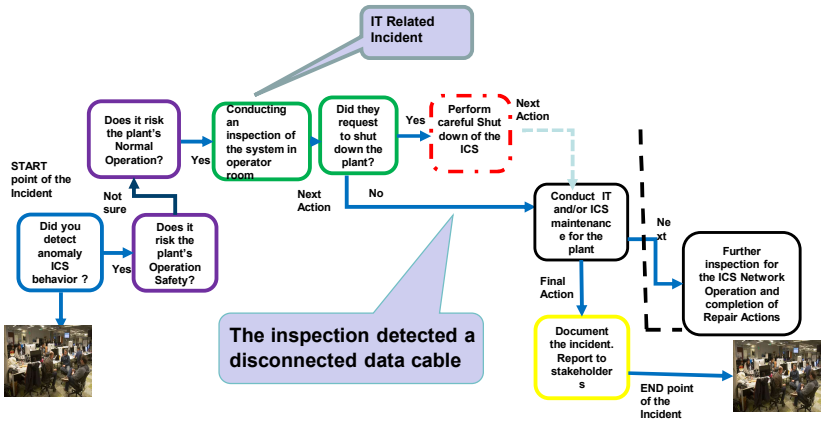
| Concerns and Risks | Fin. Losses | Bus. Cont. | Damage | Safety | Risk to Lives |
|---|---|---|---|---|---|
| ?- Unknown/ H-High/ M-Medium/ L-Low | L | L | M | L | L |

Selected actions to be decided by the team

- **Recommended Actions**
  - Control room manager to activate the secondary HMI
  - In parallel to onsite inspections, take actions to restart the HMI.
  - Inspect the ICS Zone networks: Switches, firewalls, routers, etc.)
  - If the fault continues, perform a controlled plant shutdown.

# Incident - The HMI is not getting updates 4/4

- **Incident Response Flowchart**
  - Series of step-by-step actions
  - The team must make decision at each step



## About the Author

**Daniel Ehrenreich**

Consultant, workshop lecturer, and Secure Communications and Control Expert. Daniel has over 32 years of experience with control solutions of industrial operations and integration with Cyber security

Acting as an expert and volunteer contributor to multiple ISA 62443 workgroups.