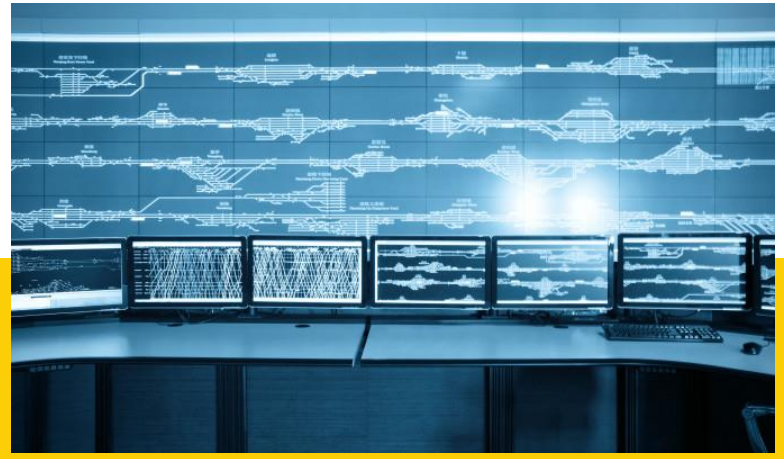
PCD Integrity – Think Secure for Suppliers



March 2020

Overview

Increased threat to Process Control Domain (PCD) Integrity
that can lead to **loss of production or an HSSE incident**

Think Secure behaviors

THINK SECURE

ACCESS CONTROL

THINK SECURE

PORTABLE DEVICE

THINK SECURE

MOC / PtW

Know the risks, feel responsible, practice Think Secure

For questions please contact your PCD Integrity Site Focal Point

THINK SECURE

Your personal responsibilities for Cyber Security

Challenge

Scan

Report

Do's

- Involve your PCD Integrity Site Focal Point (SFP) when you have a requirement to attach your device to the PCD
- Provide your PCD Integrity SFP proof of your portable device being malware free before use
- Immediately contact the PCD Integrity SFP in case of security incidents
- Keep physical security of PCD systems in place after use (e.g. keeping PCD cabinets locked or USB port blockers in place)
- Report when you see unsecure behavior in the PCD (e.g. unauthorized use of removable media)

Don'ts

- Do not connect anything or make changes to the PCD without formal authorization
- Do not use a USB stick or laptop in the PCD which has not been scanned
- Do not charge your smart device on a PCD system's USB port instead use an electrical outlet
- Do not share your password with others or use other's credentials
- Do not simply make assumptions regarding security - verify these assumptions
- Do not assume that security is someone else's job - it is everyone's job

THINK SECURE

Access Control

AUTHORISED ACCESS ONLY

Access Control Management protects PCD from

- Unauthorized access
- Unauthorized use of removable media
- Tampering with equipment or wiring
- Intentional or accidental damage

THINK SECURE

How YOU can protect the PCD

- Only access areas that you are authorized to access
- Do not tamper with physically blocked USB-ports
- Do not hop between networks, i.e. Shell PCD and Internet
- Always run a full scan of your portable media before use
- Make sure that you follow the protocol for portable device usage

THINK SECURE

How YOU can protect the PCD

- Use only Shell provided portable media where made available by the asset
- Ensure you have a valid Permit To Work before entering your work area
- Lock rooms and cabinets and ensure keys are kept safe
- Follow restricted area protocols

Portable Media

DON'T STICK IT

Use these portable media devices only when strictly necessary and after all required security checks have been passed

Laptops

CDs/DVDs

Memory sticks

Charging cables

Smartphones Tablets

Hard disks