PECB

fedco.co.id

Pedro Putu Wirya

Vulnerability Assessment and Penetration Testing in online SCADA ICS Environment Risk, Method and Recommended Practices

www.pecb.com

www.fedco.co.id

Pedro Putu Wirya

Consultant

Pedro Putu Wirya, an IT and ICS Security Consultant with an extensive experience in Information Security Management System (ISMS) and Cyber Security Assurance

+6282114858766

pedrowirya@fedco.co.id

www.fedco.co.id

linkedin.com/in/pedro-putu-wirya-37491734

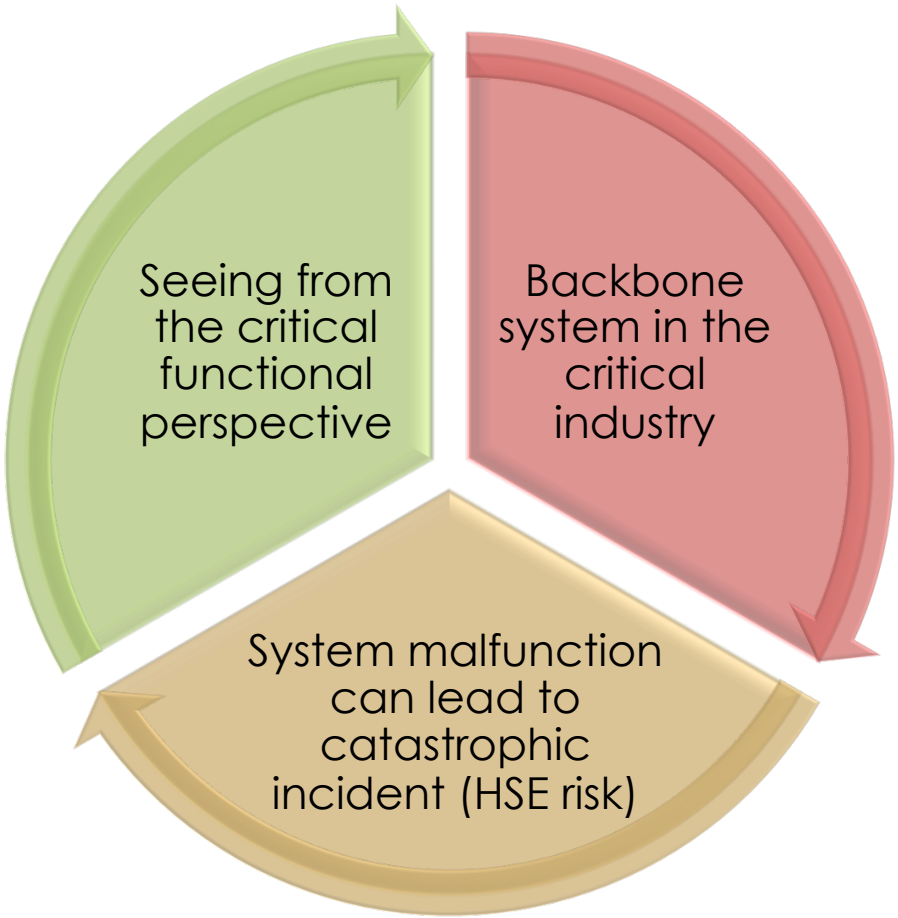
pedro.putuwirya

Content

- Background
- IT vs. ICS from Cyber Security Perspective
- VA and Pen Test in IT vs. SCADA ICS
- Recommended Practices
- Summary

Background

Why ICS is IMPORTANT?



"One aspect that most likely being ignored in ICS engineering & operations is the ICS Cyber Security Assurance"

PECB fedc fedco.co.id

Background

- The importance of Industrial Control System security
  - Critical function that controls the plant, ensure the safety operations and meet the business goal
    - Critical industry
    - Public infrastructure
    - Energy and fundamental human needs
  - Safety risk exposure vs. Financial

Background

- What are the challenges to have ICS security Assurance
  - Awareness level and Business Buy-In
  - The computerized ICS with open protocol and open platform infrastructure
  - Integration between ICS Network and Business Network
  - Risk heritage from the common IT infrastructure that being adopted by ICS
  - Professional capability IT security vs. ICS security
  - Threat and vulnerability vs. Risk -> Safety, Business, Environment -> tangible impact vs. investment

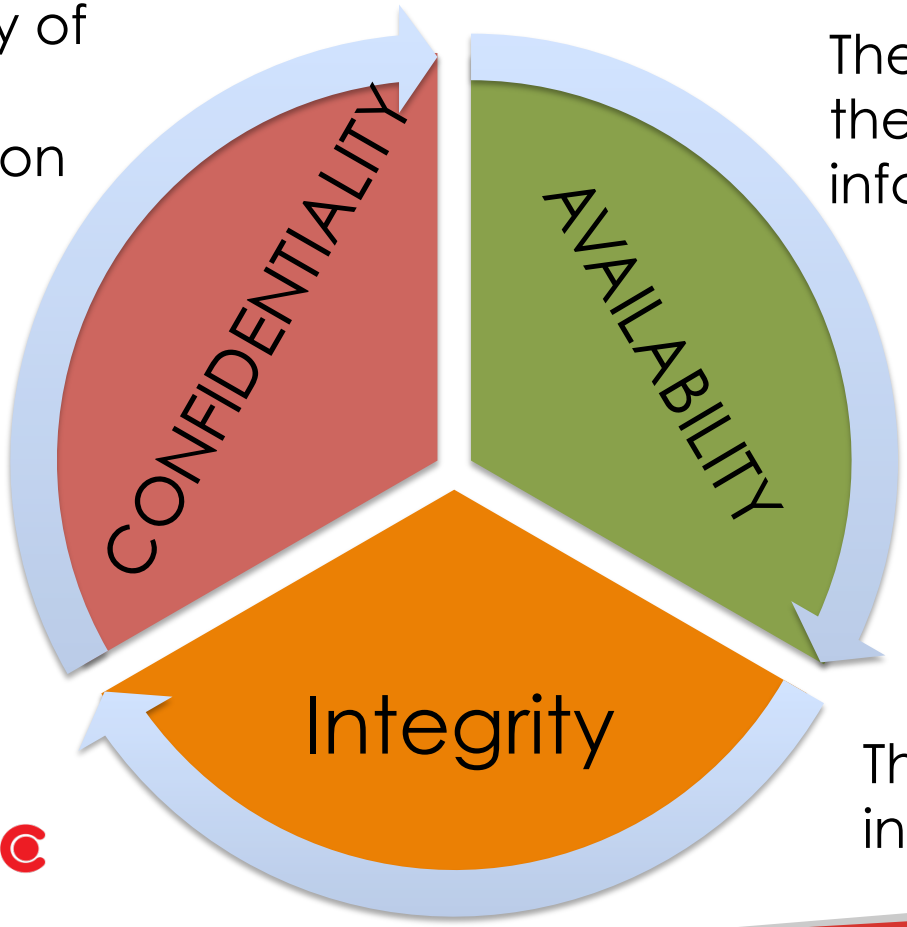
Content

- Background
- IT vs. ICS from Cyber Security Perspective
- VA and Pen Test in IT vs. SCADA ICS
- Recommended Practices
- Summary

IT vs. ICS from Cyber Security Perspective

The Essentials of Cyber Security Assurance

Information confidentiality of data communication



The availability of the required information

The system objective will drive the fulfilment of these three aspects

The validity of information exchange

PECB fedc fedco.co.id

IT vs. ICS from Cyber Security Perspective

IT vs. ICS from CIA Priority

Prioritas	IT	ICS
Confidentiality	1st	3rd
Integrity	2nd	2nd
Availability	3rd	1st

IT vs. ICS from Cyber Security Perspective

Category	Information Technology System	Industrial Control System
Performance Requirements	Non-real-time Response must be consistent High throughput is demanded High delay and jitter may be acceptable	Real-time Response is time-critical Modest throughput is acceptable High delay and/or jitter is not acceptable
Availability Requirements	Responses such as rebooting are acceptable Availability deficiencies can often be tolerated, depending on the system's operational requirements	Responses such as rebooting may not be acceptable because of process availability requirements Availability requirements may necessitate redundant systems Outages must be planned and scheduled days/weeks in advance High availability requires exhaustive pre-deployment testing

Availability is the ULTIMATE PRIORITY

PECB fedc fedco.co.id

IT vs. ICS from Cyber Security Perspective

Category	Information Technology System	Industrial Control System
Risk Management Requirements	Data confidentiality and integrity paramount Fault tolerance / momentary / major risk Major / day of business operation	Human safety is paramount, followed by protection / process Fault to / momentary downtime Major risk impacts are environmental impact / loss of / or production
Architecture Security Focus	Primary focus is protecting the information stored on or among these assets. Central server may require more protection	to protect edge clients (e.g., such as process controllers) Protection of central server is also important
Unintended Consequences	Security solutions are designed around typical IT systems	Security tools must be tested (e.g., off-line on a comparable ICS) to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	Less critical emergency interaction Tightly restricted access control can be implemented to the degree necessary for security	Response to human and other emergency interaction is critical Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction

Financial Concern

Safety Concern

Ultimate RISK Exposure

PECB fedc fedco.co.id

Content

- Background
- IT vs. ICS from Cyber Security Perspective
- VA and Pen Test in IT vs. SCADA ICS
- Recommended Practices
- Summary

VA and Pen Test in IT vs. SCADA ICS

Activity	Corporate IT Environment	SCADA ICS Environment
Identification of networks, hosts and nodes	Ping Sweep (e.g.. NMAP)	Examine CAM Tables Examine Config files Conduct Physical Checks Passive Listening
Identification of services	Port Scan (e.g.. NMAP)	Port verification (netstat) Port scan in a duplicate test environment
Identification of vulnerabilities	Vulnerability Scanning (e.g. Nessus)	Local banner grabbing Scan of a duplicate test environment
Gaining access	Exploits tested (e.g.. password guessing/cracking)	Review of local security configs. Only perform this stage in a test environment.
Elevate Privileges	Undertake further exploits	Only perform in a test environment
Place Backdoors and Cover Tracks	Install programs and delete logs and log files	Only perform in a test environment

Content

- Background
- IT vs. ICS from Cyber Security Perspective
- VA and Pen Test in IT vs. SCADA ICS
- Recommended Practices
- Summary

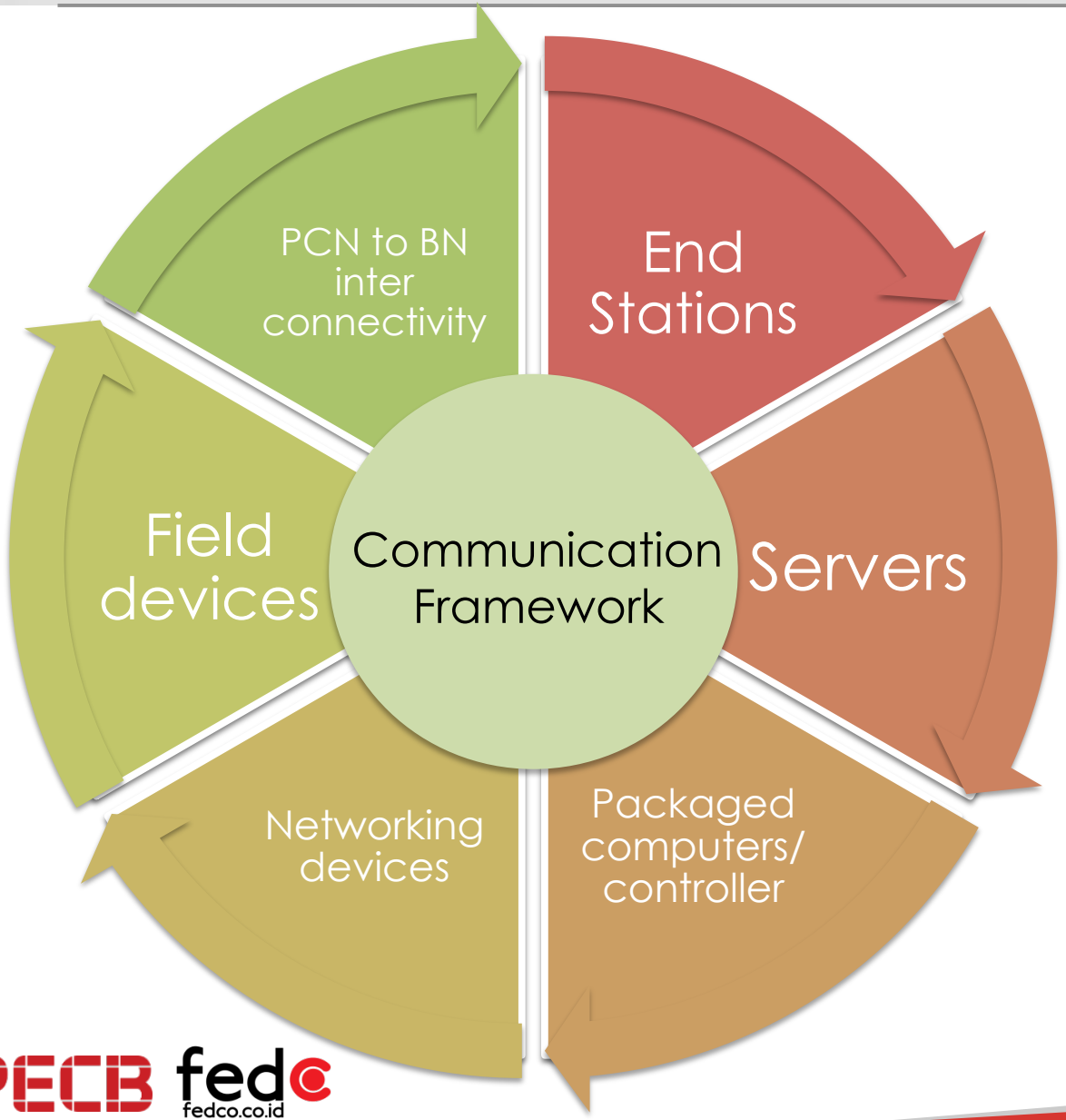
Recommended Practices

The rule of thumbs

- SCADA ICS security is not 100% mapping of IT security
- The safety risk exposure and some consideration drive the approach on doing the VA and Pen Test in SCADA ICS environment
- Using "Non Destructive Testing" approach instead of using automated VA
- Avoid using direct "destructive" Pen Test method that will trigger losses (safety risk as ultimate concern), use the "Non Destructive Testing" approach
- By doing some activities such as reviewing, assessing, passive scanning, sniffing against several items related to SCADA ICS environment

PECB fedc fedco.co.id

Recommended Practices



- ✓ Process Control Network interconnectivity to Business Network
- ✓ Networking and security devices (router, switch, firewall, IDPS)
- ✓ End stations (HMI, Eng. W/S, Operator W/S, SCADA ICS clients, etc.)
- ✓ Servers (DCS, SIS, SCADA , DMC, Historian, etc.)
- ✓ Packaged computer/controller (flow computer, PLC, RTU, turbomachinery PLC, DCS controller, etc.)
- ✓ Field devices (RTU, Hart devices, Fieldbus devices, IED)
- ✓ Communication framework (internal and external)

PECB fedc fedco.co.id

Recommended Practices

Some of the recommended practices for Vulnerability Assessment and Penetration Testing in SCADA ICS Environment

- Reviewing network devices configuration, including network security devices
- Remote access review including its methods, protocols and technique
- Reviewing access control (logical and physical) against the protected system (restricted access to ICS servers, windows logon via domain/local, field access to system, engineering key management, application access and usage, maintenance laptop, etc.

Recommended Practices

Some of the recommended practices for Vulnerability Assessment and Penetration Testing in SCADA ICS Environment

- Backup and restore activities, review the pratice in place
- Assessing SCADA ICS security policy and procedure, including domain and local user policy and implementation
- Management of change coverage against system changes
- Access testing from business network to process control network to ensure one way path

Recommended Practices

Some of the recommended practices for Vulnerability Assessment and Penetration Testing in SCADA ICS Environment

- Update and upgrade management review
- Align the security patches, OS update, anti virus and definition update, application update with OEM recommendation – test before deploy, ensure backup before and after
- Scanning of wireless access to detect unsecure WiFi setup, typically for uncritical field devices that using wireless communication platform
- Any external connection should be risk assessed and reviewed to ensure secure interconnection
- Be aware of obsolescence issue
- …

Recommended Practices

Can we do VA and Pen Test as we have in IT security, being executed in SCADA ICS environment?

Sure, but do it at your own risk, technical capability, understanding of ICS engineering philosophy, partial execution, ensure you have good mitigation plans, proper insurance coverage & legally covered (especially for vendor), and the last thing "no safety risk to be exposed"

Otherwise, test it in offline production system by developing your mimic system to reflect the running environment

OR

*Do the safer way **"the NDT method"***

PECB fedc fedco.co.id

Content

- Background
- IT vs. ICS from Cyber Security Perspective
- VA and Pen Test in IT vs. SCADA ICS
- Recommended Practices
- Summary

Summary

- Safety is the ultimate risk exposure on the SCADA ICS environment
- The ultimate risk exposure drives the different way to do the VA and Pen Test
- The NDT method, ensure the system still running normally while doing the security testing (VA and Pen Test)
- The NDT method can manage the risk exposure on its ALARP level while providing proper security posture and validation against assessed system

Do you want to have more challenging task, then why don't do it in online system?

PECB fedc fedco.co.id

THANK YOU

QUESTIONS

+6282114858766

pedrowirya@fedco.co.id

www.fedco.co.id

linkedin.com/in/pedro-putu-wirya-37491734

pedro.putuwirya