Summary and Content of the Training Course 4

General Knowledge of OT-Cybersecurity

7th of February 2024
Version: 1.0

Confidentiality, Copyright, TAPS and Disclaimer

Confidential and Copyright:

Disclaimer:

Every effort is made to provide accurate information in this document. However, TAPS makes any warranty of any kind about the quality or correctness of the information included in this document. TAPS will not be liable for any damages of any kind arising from the use of this document.

Comments sent by E-mail:

You are invited to provide TAPS with your personal comments or questions in an E-mail, directed to TAPS@TedAngevaare.nl. TAPS will use this information to improve the content of this document.

TAPS:

Ted Angevaare
Independent Consultant Process Security
Mail and Visit address : Guirlande 123, 2496 WP, The Hague (ZH), The Netherlands.
Telephone : +31 6 207 177 75
E-mail : TAPS@TedAngevaare.nl
Website : www.TedAngevaare.nl
Registered at the KvK : 68174616

The TAPS Documents and Training:

This Training is one in a series and the documents are:

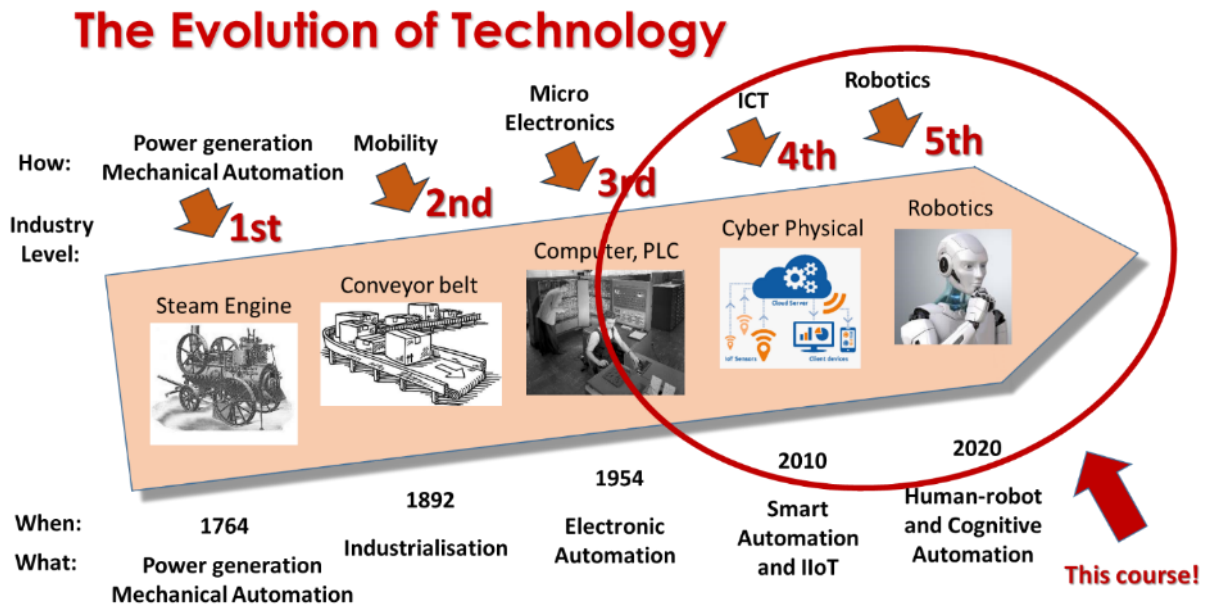
1. Industrial Security Project Justification
2. How to realise an Industrial Security Project
3. Sustainability of OT-Cybersecurity
4. **General Knowledge of OT-Cybersecurity**
5. The Past, the Present and the Future of Process Automation and OT-Cybersecurity
6. Industrial Automation System Architecture and OT Cybersecurity

Management Summary

This training course is number 4 of the TAPS training and is a 4-day course to provide knowledge of 'Industrial Automation System Architecture and OT Cybersecurity, basics and implementation'.

Industrial Automation is the technology to automate industrial production processes and over the last 20-30 years this technology has changed from pneumatic systems, and the first electronic systems into Windows-based computer systems. The Control and Automation discipline has evolved tremendously and entered the era of applied computer science. This has helped the industry into the next generation of smartness in process control and the cost per measurement has come down by a factor of 3-5. This opened the doors to production optimisation, modelling and artificial intelligence (also called Industry 4.0).

Robots have been introduced already to go to places where humans cannot survive (e.g. toxic gasses, extreme weather conditions, noisy environments) and the next generation robots are being developed as we speak (called Industry 5.0). These robots will be connected via wireless links with the control systems and will perform the eyes, ears and hands of the field operator of today.

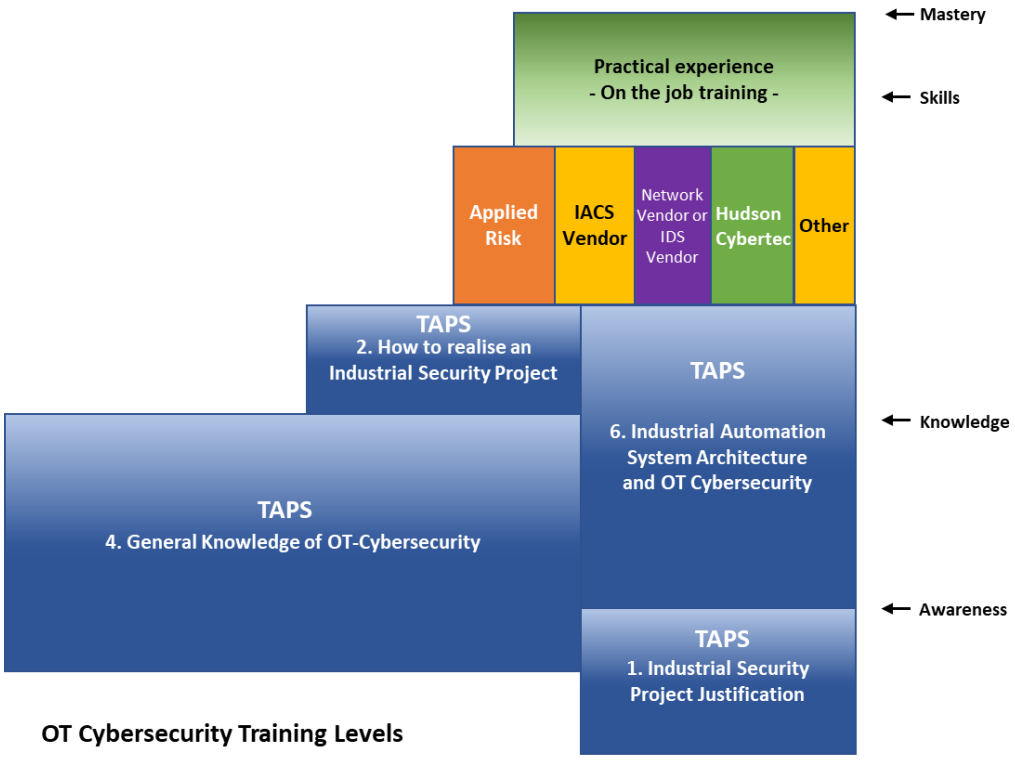


This new technology has brought us more optimised and reliable operations of our production plants, however another threat has been introduced and that is the threat of malware and hackers, the Cybersecurity threat. A hacker can sit safely at home behind his screen and can create a lot of damage, sometimes unintentionally, but most of the time with a specific focus and purpose. Hackers say: "when it has two wires, we can hack it, take over control and sometimes we crack it (destroy it)." We are facing a new form of crime called Cybersecurity crime and with Ransomware these criminals can paralyse an entire company and when the attack is successful, it's too late to do anything about it.

But before it's too late a company can train its staff and this training course (6. Industrial Automation System Architecture and OT Cybersecurity) could be a step in the process of creating skilful staff to manage and mitigate this threat.

TAPS can provide training that is not only broad and covers the entire spectrum of industrial Automation and OT-Cybersecurity, but also provide knowledge that is unique and based on the experiences gained over the last decades at one of the largest multinationals.

Most Vendors provide training of their products and how to configure these, but the TAPS training will handle all aspects that will form the new discipline OT-Cybersecurity.



The Training is split in 4 levels:

1. Awareness
2. Knowledge
3. Skills
4. Mastery

The first two levels, i.e. Awareness and Knowledge can be followed as Classroom Training.
The Knowledge level will be finalised with a test and when successfully passed with a certificate.

Level 3. Skills can only be completed when demonstrated in practise. TAPS can provide this service but will bring in experts on various subjects, e.g. a 'White hat hacker' to show how to do this in real live or a Firewall specialist to learn how to configure an Industrial Firewall or Intrusion Detection Systems, like ForeScout with its product 'SilentDefense'.

Level 4. Mastery means that the candidate is an expert on the subject. Not many Masters in OT Cybersecurity do exist globally that master the whole range of OT Cybersecurity. Often only a part of the OT Cybersecurity is for a master, e.g. a Firewall expert, or a Network Designer, or a person who masters Risk Assessments and Gap Analysis.

This training course "4. General Knowledge of OT Cybersecurity" consist of the following subjects:

1. Introduction to OT Cybersecurity
2. Digital theory
3. A computer system
4. Information Computing Technology, Networking and Protocols
5. Industrial Automation (Part 1, 2, and 3)
6. Cybersecurity, what is the threat?

7. Cyber Security Metrics
8. Cyber Security Standards and Legislation
9. General Cybersecurity knowledge
10. The activities before you start an OT-Cybersecurity project
11. The 12-Basic Steps of a Security Program
12. The 'Cost & Impact Effective' Security Program (Part 1 and 2)
13. Implement in 'the maximum possible'
14. Typical costs of a Security Program

Above subjects are handled in a class room with the students for 4 days. The last day, day 5, it's strongly recommended to complete training course #2, How to realise an Industrial Security Project. This is a workshop that will take each student through the theory and bring it in practise. Each student will make a plan what to do when back at work, start or continue with a OT-Cybersecurity program. All material in Training course #4 will be reviewed and it will be determined to bring this in practise and how. The student will complete the training course #4 and #2 fully equipped with knowledge and a plan on what to do!

With this training "General Knowledge of OT-Cybersecurity" you will be able to:

- Lead a Team of OT-Cybersecurity Engineers and have a good understanding of what's required to make an End-User resilient and robust to Cyber-attacks.
- Participate in a Team of OT-Cybersecurity Engineers and have a good understanding of what's required to make an End-User resilient and robust to Cyber-attacks.
- When you're a Process Automation Engineer, you will receive basic IT- and Cybersecurity knowledge
- When you're an IT Engineer, you will receive basic Process Control and Automation knowledge
- This training will bridge the gap between the two disciplines (IT & Automation) with a focus on OT-Cybersecurity.
- A high-level program will be shown of an OT-Cybersecurity program for an Industrial End-User.
- The training is broad and will touch upon all aspects that require attention to make an End-User robust against a Cyber Attack!

The biggest threat of OT Cybersecurity are people and is not the technology used. 30% of the threat is because of vulnerabilities, patching and anti-virus software not up-to-date, insecure architecture, etc., but 70% is all about human behaviour, Roles & Responsibilities, Tasks & Targets, supporting organisation, Senior Management commitment and Support, available budget, training of staff, i.e. awareness, knowledge, skills and mastery of OT Cybersecurity.

Ted Angevaare
Dec. 2023

1. Introduction

Industrial Automation is the art of running an industrial process fully automatic. The need for automation started during the first industrial revolution. One of the first closed loop control systems were mechanical systems, such as the steam engine governor invented by James Watt in 1788. Its purpose was to control the speed using two metal balls rotating. If the machine went faster the balls went further apart by centrifugal force and this was coupled to a steam control valve that would reduce the speed of the engine, such that the speed of the engine was constant.

This was a great example of what humans can do and soon the pneumatic controller was invented and many applications were engineered to use this type of technology.

After the invention of the transistor the electronic controller was born in the early 1960ties and this was a start of a fast evaluating technology that grew via analog, digital via microprocessors into the computer world.

Industrial Automation now is 'Applied IT' (Information Technology), however the priorities of Industrial Automation of, what is most critical and important, is 100% mirrored when compared to Office IT and Home IT.

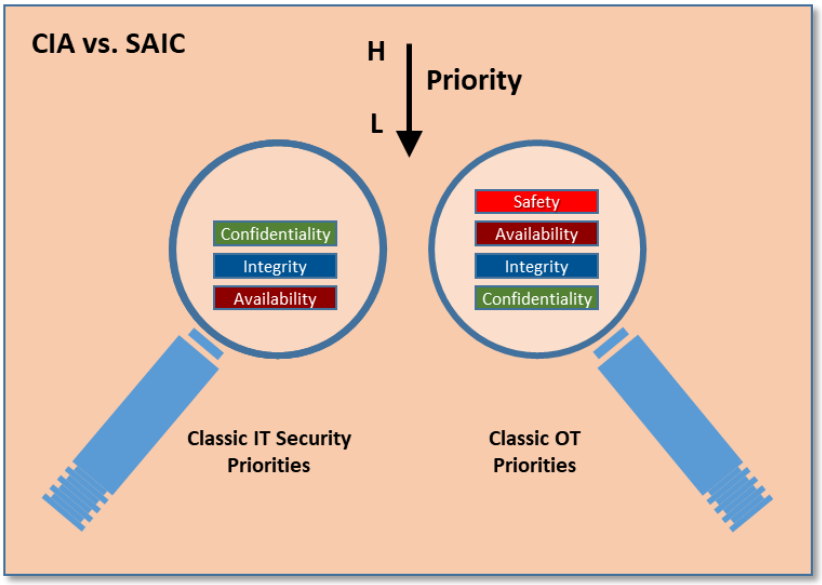


Figure 1: Priority Difference between OT and IT is often

This document is a summary of the TAPS Training Course number 4: General Knowledge of OT Cybersecurity. The subjects handled in the course are detailed in a course handout and can be used as 'after course reading material' for later use.

This report describes the important steps starting with control theory up to the industrial computer world we live in today. Industrial processes are now heavily relying on these modern computer systems. It's expected that soon Artificial Intelligence, Self-learning and Modelling will take over the importance of the 'old type' of control theory. The use of neural networks to control the industrial processes and IIoT will introduce a completely new level and era of Control Technology. Industry 4.0 has been born and the expectations of this technology, Edge-computing and The Cloud are very high.

Most industries think that they are ready to take this new technology onboard, but are they ready? What about Cybersecurity? This report describes the important steps in Industrial Automation that brought us here and more importantly what will the future bring us? Industry 4.0, The Cloud and Industry 5.0, Robots will dominate the industry in the next 25-50 years. What do we need to do to have a smooth transition to this new technology, so that when it is ready to be applied, the investments made prior to this, gently move us in this direction without replacing the entire infrastructure and systems that have been installed in a secure and safe manner?

In the meantime Cybersecurity will evolve as well and new technologies, such as SIEMs, SOCs, OT Helpdesks equipped with Artificial Intelligence, Self-learning and Modelling, like the control theory, but then applied to Cybersecurity, will push us in a world that is fast and very sensitive to technical failures. Murphy's Law will remain relevant and 'robustness, environmental impact and safety' will push back the implementation of new fast-evolving technology which may momentarily impede the rapid progression, but in the long term the robots and artificial Intelligence will win this race after it has been proven to be reliable.

But before new technology can be applied the industry has to embrace the implementation of mitigation actions to stop the Cyberthreats. All the steps described in this report and handled in the course are important to reach the goal of future Industrial Automation.

The course will offer you a view of OT-Cybersecurity from a distance and it will also immerse you right in the heart of the subject. Covering all pertinent topics, it equips you to safeguard your organization against malicious attacks.

2. The Content of the training course:

Digital theory – the subjects of this session:

- Digital theory
- Boolean Algebra
- Binary, Octal and Hexadecimal counting
- Example of Binary, Octal and Hexadecimal
- Conversion of Binary, Octal and Hexadecimal
- The ‘AND-gate’
- The ‘OR-gate’
- NOT-, NAND- and NOR-gate
- The 'Exclusive-OR' gate
- The ‘XOR’-gate equivalent with ‘NOT’, ‘AND’ and ‘OR’-gates
- Example of 2oo3 (two-out-of-three) Voting Logic with 'AND'- and 'OR'-gates
- ANSI and IEC Symbols of logic
- Example of 2oo3 voting system – HIPPS
- The rules of Boolean algebra
- Example of Integrated circuit
- Example of 2 Double HIPPS Valves
- Example of the SIS (Safety Instrumented System)
- Questions Digital theory

A computer system – the subjects:

- The hardware – CPU and Motherboard
- Moore’s Laws
- Transistor density 1971 – 2030
- The latest in Chip technology
- YouTube movie: The Extreme Physics Pushing Moore’s Law to the Next Level #01
- Nielsen's Law of Internet Bandwidth
- 42 Years of Microprocessor Trend data
- The function of the CPU
- Computer memories
- The evolution and cost per GB of Data Storage (Logscale)
- The Cloud Storage
- Binary to ASCII
- The ASCII-code
- Application Processor
- Internal Computer Network
- The Hardware – Motherboard
- BIOS, UEFI and Firmware
- BIOS Setup Utility
- The Unified Extensible Firmware Interface (UEFI)
- YouTube movie: BIOS, CMOS, UEFI - What's the difference? #02
- The types of Software and Abbreviations
- What are API, MIB, OPC and Log-files?
- The types of Computers
- The fastest computers
- The smallest and cheapest computer

- Questions about a Computer System

'Information Computing Technology, Networking and Protocols' – the subjects:

- Computer to computer connection using the handshake
- Sending ASCII 'b' to another computer
- The OSI Stack or OSI Model
- Example of Data comms using the OSI Model
- What is TCP and UDP?
- What is a Parity bit?
- What is IP and an IP Address?
- What is a subnetwork?
- Parts of the OSI-model and TCP/IP Protocol Suite
- Token Ring Data Communication
- FTP (File Transfer Protocol)
- DNS (Domain Name System)
- URL (Uniform Resource Locator)
- HTTP, HTML and XML
- Software Communication Port
- Some Assigned and Registered Ports
- Fiber Optic Cable record
- Fiber Optic Cable
- Coax Cables
- Cable vs DSL vs Fiber- YouTube movie #03
- Wireless Networks, 4G and 5G
- What is Ethernet - YouTube movie #04
- Hub
- Switch
- Router
- Gateway
- OSI-Model of HUB, Switch, Router & Gateway
- HUBs, Switches and Routers - YouTube movie #05
- Port forwarding in more detail - YouTube movie #06
- Default Gateway in more detail - YouTube movie #07
- USB (Universal Serial Bus)
- This USB can destroy your computer! - YouTube movie #08
- How the Internet works - YouTube movie #09
- Dial-up Modems and wired Modems
- Wi-Fi (Wireless Fidelity)
- Wireless Modems (WiFi)
- Bluetooth vs WiFi - YouTube movie #10
- What is the Internet - YouTube movie #11
- Movie: Dawn of the Net - How the Internet works #12
- Deep Web and Dark Web - YouTube movie #13
- VLAN (Virtual Local Area Network)
- VLAN in more detail - YouTube movie #14
- How to set up a VLAN on Cisco?
- What is POP3?
- IMAP (Internet Message Access Protocol)

- What is the difference POP3 vs IMAP?
- SMTP (Simple Mail Transfer Protocol)
- What is a Firewall?
- Different types of Firewalls
- The DPI Firewall
- YouTube movie: DMZ – Demilitarised Zone #15
- The SPAN-port and port mirroring
- IPsec and VPN
- HTTPS, SSL and TLS - YouTube movie #16
- DNS (Domain Name System)
- VPN in more detail YouTube movie #17
- DNS Records in more detail YouTube movie #18
- NAT (Network Address Translation)
- Network Ping, Traceroute and Telnet
- How to 'Ping' a network
- How to 'Traceroute' a network
- How to 'MRT' a network
- What can you do with 'NSLOOKUP'? YouTube movie #19
- Port Scanning
- Network Discovery and Port Scanners

Industrial Automation Part 1 – the subjects:

- Industrial Automation (IA)
- Control Theory
- Control Theory – PID Controller
- PID Controller explained – YouTube movie #22
- Control Theory – How to tune a PID Controller
- Control Theory – using Ziegler-Nichols
- How to Tune a PID Controller - YouTube movie #23
- Transmitters and Control Valves
- Valve Positioner
- Examples of Valve Positioners
- Hazardous Area
- Hazardous Area (Legislation)
- Hazardous Area – Group en Temperature Class
- Hazardous Area – Zones
- Hazardous Area Movie Dust – YouTube movie #24
- Hazardous Area – Zone identification
- Hazardous Area – Application Zones
- Hazardous Area – Temperature Class
- Hazardous Area – Certification selection
- Hazardous Area – Safety Barrier
- Hazardous Area Movie – YouTube movie #25
- Instrument Loop Diagrams
- Marshalling Cabinet
- Field Cables and Instrument Earthing
- Ingress Protection

Industrial Automation Part 2 – the subjects:

- Control Systems, PLC, SCADA and DCS
- PLC
- SCADA (Supervisory Control and Data Acquisition)
- DCS (Distributed Control Systems)
- The cost of embedded hardware
- The computing power per chip
- RS-232 Serial Interface
- RS-232: DTE and DCE
- RS-232, RS-485 and Modbus, the industrial serial protocols
- RS-232 in more detail - YouTube movie #26
- RS-485 in more detail - YouTube movie #27
- Analog signals
- HART™ (Highway Addressable Remote Transducer)
- What is the HART protocol? – YouTube movie #28
- Profibus (Process Field Bus)
- Foundation Fieldbus™
- Industrial Ethernet (IE) comparison
- Other Fieldbuses used in industry
- What is Fieldbus? - YouTube movie #29
- OPC (OLE for Process Control and .NET)
- Wireless Industrial Sensors
- ISA100, Wireless Systems for Automation
- WirelessHART (IEC 62591)
- Wireless Protocol comparison
- ISA100 vs WirelessHART comparison
- LoRaTM and LoRaWAN®
- LoRaWAN® - YouTube movie #30
- LoRaWAN® in practice
- Rechargeable Batteries
- Latest in Process Automation
- Smart IO – Yokogawa
- Smart IO – Honeywell
- Smart IO – CHARM Emerson
- Smart IO – others
- Project time advantage using Smart IO
- Flow computers and flow measurements
- Ultrasonic Flow Meters
- Ultrasonic Flow Meters – YouTube movie #31
- Flow computers
- Continues Water Cut measurement
- Standard and Normal Conditions
- Tank Gauging System
- Process Control and Optimisation
- Multi-variable control
- Advanced Process Control
- Neural Networks – YouTube movie #32

- Vendor's Industrial Solutions
- Example of Vendor's Solution Sand Control

Industrial Automation Part 3 – the subjects:

- Industrial Architecture
- Architecture and Purdue Model
- TOGAF ® and SABSA®
- How to Design a Network?
- Network Separation and Segregation
- Example of a Reference Architecture
- Example of a Yokogawa Architecture
- Apply Secure Zones and Conduits
- Zones and Conduits – YouTube movie #33
- Safeguarding Systems (SIF)
- Secure SIS connections – not recommended
- Secure SIS connections – recommended
- Safety Instrumented Function (SIF) – YouTube movie #34
- Fire and Gas Detection System
- Fire and Gas Detection by Dräger – YouTube movie #35
- Safety Risk Assessment (SRA)
- The PDO (Risk Assessment Matrix)
- Typical outcome of an SRA
- SIL certification
- The PFD of a SIF-loop
- 1oo1, 2oo4, XooY voting transmitters
- Oreda (Offshore and Onshore Reliability Data)
- Example of a Reference Architecture
- Engineering Work Station (EWS)
- Central Control Room (CCR)
- Control Room Building
- Edge Computing
- What is Edge computing? – YouTube movie #36
- The Cloud, IIoT and Industry 4.0/5.0
- Latest in Process Automation - Virtualisation
- O-PAS™ and O-PAF®
- NOA (Namur Open Architecture)
- The difference between O-PAS/NOA and ISA95
- What is Open Process Automation™ and O-PAS™ - YouTube movie #37
- SaaS, PaaS, IaaS, NaaS, PtaaS, RaaS, etc.
- Cloud computing in more detail – YouTube movie

Cybersecurity, what is the threat, trends and attacks? – the subjects:

- What is happening?
- What is happening in Industrial Automation?
- Warning by EU !
- Warning by UK Government !
- The war zone in the media
- Dutch government presents Cybersecurity strategy 2022-2028

- Warning by Anonymous, a global hacktivist group
- What is happening? According to the World Economic Forum – 2023 report
- Simple question: Are you?
- How big do you think is the issue globally in Dollar$?
- Cybercrime Expected To Skyrocket in Coming Years
- McAfee report on Cybercrime in Dollar$
- What is the trend of Malware?
- What is the trend of Cyber Attacks?
- What is the trend of Ransomware?
- What is the Industry Distribution of attacks?
- Different type of Cybersecurity activities?
- Cybersecurity Threats and Types – YouTube movie #39
- Cybersecurity Trends 2023 by IBM – YouTube movie #40
- Some successful attacks on the Industry
- The impact of Triton (2017)
- How the Triton-malware works (2017)
- The impact of NotPetya Ransomware (2017)
- Comparison of the Ukraine Grid Attacks: 2015 vs. 2016
- Most known hacker-groups at this moment
- 7 all of time famous hacker group #41
- Cybersecurity for Industrial Control Systems – YouTube movie #42
- Summary of Cyber-attacks

Cyber Security Metrics – the subjects:

- Cyber Security Metrics
- The Global Cybersecurity Index (GCI)
- Possible improvements of Cyber Security Metrics
- Cyber Security Metrics and Dashboard
- Metrics of Patching and Vulnerabilities
- Vulnerabilities vs. Malware
- Malware vs. Exploits – YouTube movie #43

Cyber Security Standards and Legislation – the subjects:

- Cyber Security Standards
- IEC 62443 Series by WIB, ISA99 and IEC TC65
- IEC 62443-2-4
- IEC 62443-2-4 Maturity Levels and Profile
- Certification against IEC 62443
- Conclusions on International Standards
- What are Governments doing?
- New Cybersecurity Legislation to comply to
- GDPR (General Data Protection Regulation)
- NIS Directive (Network and Information Directive)
- NIS2 - Network and Information Security 2
- NIS2 effective on 17th of Oct 2024 - YouTube movie #44
- Seveso-III - European Directive
- Legislation in the Netherlands on one page
- Cybersecurity regulation in the US

- Legislation in United Kingdom
- UK Cybersecurity Legislation – YouTube movie #45
- Legislation in Belgium
- Legislation in Germany
- Summary Cybersecurity Legislation
- European Cybercrime Centre (EC3)

General Cybersecurity knowledge – the subjects:

- General Cyber Security knowledge
- What are vulnerabilities?
- Vulnerability or Malware detection?
- Who discloses vulnerabilities?
- Vulnerabilities
- The Triconex Safety System attack disclosure
- The Rockwell Safety PLC attack disclosure
- Vulnerability Life Cycle in Industrial Automation
- What kind of cybersecurity attacks are possible?
- Ransomware attacks
- Ransomware evolvements
- Example of Userid and Password hacking movie
- What is a PLC worm?
- DDos Attack
- What is Hacking and Types of Hackers
- How to hack? Just Google it!
- How to hack? LINUX is not the answer!
- How does a hacker work?
- How to Hack a Password?
- How to Hack or Crack a Password?
- How does a hacker work? Maintaining Access
- How does a hacker work? Covering Tracks
- What is the chance that you are impacted by Malware or a Cyber Attack?
- Hardening and Default Passwords
- Secure and Strong Passwords
- Default Passwords can be found on Internet
- OT Anti-Virus clients and server in the DMZ
- Install WSUS or similar and patch
- Backup and Restore
- Application White-Listing (AWL)
- Cyber Security Monitoring Tools for IACS
- IDS and IPS, the difference
- Security Dashboards, Helpdesk and SOCs
- Risk Assessment and Gap Analysis
- What is Defense-in-Depth?
- Defense in Depth (DiD)
- Defense by Design (DbD) and Power Supply
- What is Cryptography?
- Time required to crack encryption
- Tools to encrypt files to keep data safe

- Key Management
- KMaaS (Key Management as a Service)
- Incident Management

The activities before you start an OT-Cybersecurity project – the subjects:

- Check expectations before you start
- Do I have a Cyber Security problem?
- Other Problems?
- Shell Brent Bravo
- Before you start a Security Program
- Justification of a Security Program
- Why is it difficult to start a Security Program
- Create Senior Management commitment
- The difference between OT and IT
- End-Users require a new organisation
- A possible organisation
- Good Contractors required

The 12-Basic Steps of a Security Program – the subjects:

- 12-Basic Requirement Steps to a Simple Approach to Secure your Process Control Domain (OT)
- Step 1.1 - Make an Inventory
- Step 1.2 - Make a Network drawing
- Step 1.3 - Check for dial-up modems
- Step 1.4 - Contact your Control System Vendors for Vendor Solutions
- Step 1.5 - Separate OT and IT Network by design
- Step 1.5 - How to Design a Network
- Step 1.5 - Network Separation and Segregation
- Step 1.5 - Cheapest way to protect Process Automation
- Step 1.5 - Apply Secure Zones and Conduits
- Step 1.6 - Design SIS only connected to the Control System and EWS
- Step 1.6 - SIS Network Design
- Step 1.6 - Secure SIS connections – not recommended!
- Step 1.6 - Example: Emerson DeltaV SIS secure IPS connection
- Step 1.7 - Training of Staff
- Step 1.8 - Execution of network changes
- Step 1.8 - How to implement a Firewall
- Step 1.9 - Install OT Anti-Virus clients and server in the DMZ
- Step 1.9 - Update all OT systems with the latest AV Definition files
- Step 1.9 - How successful is Anti-Virus Software?
- Step 1.10 - Install WSUS or similar and patch
- Step 1.10 - Microsoft WSUS
- Step 1.10 - WSUS to be installed in the DMZ of your L3/L4 F/W
- Step 1.10 - Patch all OT Systems
- Step 1.10 - The Risk of Patching OT Systems
- Step 1.10 - Example of a Vendor's Patch List
- Step 1.11 - Execute Hardening
- Step 1.12 - Create Sustainability Plan

- Step 1.12 - Backup and Restore

The 'Cost & Impact Effective' Security Program – the subjects (Part 1):

- Step 2.1 - Security Plan
- Step 2.2 - Perform Risk Assessment and Gap Analysis
- Step 2.2 - SIS Risk Assessment
- Step 2.2 - Map Gaps in Cost vs Risk diagram
- Step 2.3 - Security Plan
- Step 2.3.1 - OT Security Plan, Strategy and Policy
- Step 2.3.2 - Security Management System, Roles & Responsibilities and Job Descriptions
- Step 2.3.2 - Roles & Responsibilities
- Step 2.3.2 - Job Descriptions
- Step 2.3.3: Incident Management
- Step 2.3.4: Configuration Management
- Step 2.3.5: Disconnection Procedures
- Step 2.3.6: OT Cyber Security Administration
- Step 2.3.7: Infrastructure Management
- Step 2.3.8: Firewall Management System
- Step 2.3.9: Remote Access
- Step 2.3.9: Access Control and Management
- Step 2.3.9: Possible Solutions - Secure OT Solutions for Access and Management
- Step 2.3.9: NextNine Industrial Cybersecurity Solution
- Step 2.3.9: TDi Technologies - Console Works
- Step 2.3.9: Hirschmann Secure Remote Access Solution
- Step 2.3.9: Leidos (past SAIC)
- Step 2.3.10: Application and Data Management
- Step 2.3.11: TOGAF in the OT
- Step 2.3.12: Physical Security
- Step 2.3.13: Advanced Remote Access to OT
- Step 2.3.13: SecurePlant TM
- Step 2.3.13: CISCO Industrial Networking
- Step 2.3.13: Yokogawa Plant Security
- Step 2.3.14: Create plan to ensure that Data Streams will continue to work
- Step 2.3.14: Data Stream Model
- Step 2.3.14: Make a Data Stream model
- Step 2.3.14: Example of a Data Stream model (Alarm Data in PI)
- Step 2.3.15: Two-Factor Authentication (2FA) and Single Sign-on
- Step 2.3.15 - Two-Factor Authentication (2FA)
- Step 2.3.15 - Multi-Factor Authentication (MFA)
- Step 2.3.16: Disposal / Confidential waste
- Step 2.3.17: Security Dashboards, Helpdesk and SOCs
- Step 2.3.17: Gartner's Magic Quadrant for Security Information and Event Management (SIEM)
- Step 2.3.17: CISCO Secure Ops Solution
- Step 2.3.17: Rockwell - Verve Security Center
- Step 2.3.17: Splunk Enterprise Security (ES)

The 'Cost & Impact Effective' Security Program – the subjects (Part 2):

- Step 2.3.18: Cyber Security Monitoring Tools for IACS
- Step 2.3.18: Monitoring Tools
- Step 2.3.18: ForeScout SecurityMatters - SilentDefenseTM
- Step 2.3.18: ForeScout CounterACT
- Step 2.3.18: Ipswitch's WhatsUp Gold®
- Step 2.3.18: WhatsUp Gold Network scanning and monitoring
- Step 2.3.18: CyberX Xsense Security Monitoring Tool
- Step 2.3.18: Claroty (Israel – USA)
- Step 2.3.18: Nozomi Networks (Switzerland – USA)
- Step 2.3.19: Disgruntled Employees
- Step 2.3.19: Background checks
- Step 2.3.20: Change to strong protocols
- Step 2.3.21: Network Design - Time Synchronisation of Automation Solutions
- Step 2.3.21: Some options possible to apply Time Synchronisation:
- Step 2.3.22: Wireless Security and Protocols
- Step 2.3.23: Security Requirements for Vendors
- Step 2.3.24: Compliance to Legislation
- Step 2.3.25: Sustainability Plan & Life Cycle
- Step 2.3.25: Life Cycle and Obsolescence Management
- Step 2.3.25: Regular audits and reviews
- Step 2.3.25: Penetration Testing
- Step 2.4 and Step 2.5: Create information pack
- Step 2.4: Checklist for OT-Security Engineers
- Step 2.5: Checklist for End-User Senior Management
- Step 2.6: Execute training programs for own staff (See also step 1.7)
- Step 2.7: Start Security Project
- Step 2.8 and Step 2.9: Create contracts with IACS and Security Vendors
- Step 2.10: detailed commissioning
- Step 2.11: Continual Improvement (CI)
- Step 2.12: Maintenance

The 3rd Phase: Implement in 'the maximum possible' – the subjects:

- The Quarantine method
- How to implement 'the maximum possible'
- Use the Bow-tie model for defense in depth
- Moving from Reactive to Proactive
- The Swiss Cheese Model
- OT Attack Vector Analysis
- DataDiode
- DataDiode (Fox IT)
- Unidirectional Gateways

Typical costs of a Security Program:

- The costs of Step 2.3: Security Plan (Based on RA and could vary per End-User)
- Typical costs of a Security Program for a large refinery?
- Conclusions status 2023:

3. Summaries and conclusions of Training Sessions:

Some of the questions we try to answer with this training course:

- Why are Governments warning us? Is it that serious?
- Do you know of the successful attacks on the industry and what happened?
- How are the trends of Cybersecurity and attacks?
- How is it possible that these attacks had an impact?
- What is the chance that you are impacted?
- Is my organisation capable of handling this new threat?
- What can we do to protect ourselves?
- What are the projects steps?
- How expensive is it to become more robust and resilient?

Summary of the session - Warning by Governments:

- The US Government and the European Governments are extremely concerned about the impact of OT-Cybersecurity and state that the issue is under-estimated.
- The UK Government warns about a new way of war!
- The Dutch Government stated that the Netherlands are not ready for a major Cyber Attack and is calling for action now, not to become a victim.
- The World Economic Forum in Geneva ranks Cyber Security as Risk number 8 globally for doing business, when compared to global climate changes and other subjects, such as natural disasters and extreme weather events

Questions Digital theory:

- What is the Output of an AND-gate, provide a truth table and what is the symbol?
- What is Boolean Algebra and provide one of the calculation rules, e.g. A + AB = A + B
- What is the meaning of a small line on top of a letter in Boolean Algebra?
- Provide at least 5 types of logic gates
- What is the function of a HIPPS and is this upstream or downstream?
- Why is a HIPPS better than a Relief Valve?
- Convert 42 Octal into Decimal

Questions about a Computer System:

- What is Moore's law?
- What is Transistor Density?
- What is a CPU?
- What is an ALU?
- What is a RAM?
- What is the present most expensive data storage?
- What is the cheapest data storage and what are the disadvantages?
- What is ASCII?
- List 2 internal bus systems
- What is the function of the BIOS?
- What is firmware?
- What is an API?
- OPC UA is based on what?
- What is a MIB-file?

- What is a Log-file?
- Mention 3 of the 6 type of computers?
- How is the speed measured of Super computers?
- What is the name of the smallest and cheapest computer?

Questions about 'Information Computing Technology, Networking and Protocols':

- What is a handshake?
- How many layers are in the OSI-Model and mention 4, use (All People Seem To Need Data Processing)?
- Which levels are used by a Router (nb)?
- What is a Parity bit?
- At which level in the OSI Model is TCP
- At which level in the OSI Model is IP and what is IPv4 and IPv6
- What is a Subnetwork?
- What is a Token Ring?
- What is an URL and a DNS Server?
- What is HTML and XML?
- What is Ethernet and what are the speeds possible?
- What is data collision detection and prevention?
- What is the latest USB version?
- What is a header in a data package and what is a footer?
- What is a Network Ping?
- What is TraceRoute?
- Who owns Internet Tier 1 networks?
- What is an ISP?

Questions part 1 of 'Industrial Automation':

- What does the abbreviation PID mean?
- What are the inputs into a control loop?
- What is the contribution of the I-action?
- What is the contribution of the D-action?
- What is required in practise to tune a controller?
- What is required when the Ziegler-Nichols method is used?
- What is the function of the Valve Positioner?
- How does the symbol of Explosion Proof look like and in what legislation is this embedded?
- What are the two groups in Explosion Proof and also in Ingress Protection and what is typical in an oil & gas plant?
- What is allowed when the equipment is certified according 'Ex ia' when doing maintenance?
- What is required in a safe zone to make signals suitable for the area classification?
- What is typical for instruments installed in a plant w.r.t. power supply and earthing?
- What is the difference between plant earth and signal earth and where are the two connected?
- What is the purpose of a Marshalling Cabinet?

Questions Industrial Automation (Part 2):

- What is the difference between DCS/PLC and SCADA in Europe?
- What is the minimum number of wires for a RS-232 connection?

- What is the max. distance of RS-232?
- What is the max. distance of Modbus?
- What is one disadvantage of using HART?
- What is the difference between Profibus (PB) and Foundation Fieldbus H1 (FF H1)?
- What is one advantage of FF H1 over Hart?
- Why was CoTS introduced in the Process Automation world?
- Would you use OPC to communicate across a firewall, why or why not?
- What are the three most used standards for wireless sensors in the field?
- Is it possible to encrypt data with ISA100?
- What is the advantage of LoRaWAN®?
- What is the major advantage of using Smart IO?
- What is the name of Emerson's Smart IO, Yokogawa's Smart IO and Honeywell's Smart IO?
- With what type of flow meter can you measure mass flow and density?
- What can be used as well for custody transfer, besides flow measurements?
- What is Multi-variable control?
- What are Neural networks?
- Mention one example of Production Optimisation?

Questions Industrial Automation (Part 3):

- What is virtualisation?
- Why is it more attractive than the conventional systems and architecture? (mention at least 3 advantages)
- What is the function of a Safeguarding System?
- What is the abbreviation of SIF and SIS?
- Mention the classes of SIF and how are these established?
- What is $MTBF_{FTD}$?
- What is Ti?
- What is PFD_{AVR}?
- What is the function of a Keyswitch between the ICS and SIS?
- Mention at least 2 International Standards that describe SIF and the related Risk Assessment.
- Where is the Failure Rate data coming from?
- Mention at least 2 International Standards that describe SIF and the related Risk Assessment.
- Where is the Failure Rate data coming from?
- Mention one good database that can be used to determine the design of each SIF.
- How can you improve the PFD of a SIF Function?
- What happens to the Ti when the PFDAVR of the loop is much higher than required?
- What is an EWS?
- What is the difference between an EWS and CCR?
- What is the advantage of virtualisation?
- Which ISA-95 levels are merged with O-PAS?
- What is a big advantage of O-PAS?
- Mention of few *AAS

Summary of Cyber-attacks:

- Many successful attacks on the industry since 2010
- All countries are doing this, but mostly China (stealing) and Russia (destruction)
- Some attacks cause serious damage (Stuxnet, Triton,..)

- Attacks become more automated, less knowledge is required by the attacker (only by the developer)
- It's possible to buy malware on the Darkweb (BlackCat)
- Payment of Ransomware is mostly in Bitcoins
- The key to unlock is often not provided
- A well-managed Firewall, up-to-date Anti-virus Definition files (AV) and applying the latest patches is not good enough
- Some hacker groups are protected in their country or are sometimes sponsored by that government.
- The trends of malware is going up….

Conclusions on Cyber Security threats, trends and attacks:

- Hacking (that we know of) is stabilising over the last years, but is more focussed.
- The number of new malware is increasing over the last years and anti-virus cannot keep-up…
- Cyber Attacks are evolving to more complex attacks, often sleeping until activated
- Ransomware is the biggest threat at this moment and causing most damage financially
- Cyber Attacks are more focussing to warfare, espionage and criminal activities.
- The impact of Cyber Attacks is under-estimated by our Captains of Industry and non-specialists
- The industry only wants to make use of cheaper hardware and software (COTS), but doesn't want to invest much in protection against Malware and Cyber Attacks.
- The industry is not adjusting fast enough to the new Cyber Threats…..

Conclusion on Cyber Security Metrics:

- If you cannot measure it, you cannot improve it.
- Difficult to measure what you don't know!
- Cyber Security Metrics is difficult
- Cyber Security cannot be measured like Safety (MTBF)
- Cyber Security can be positioned on a RAM (Risk Assessment Matrix)
- There are many Cyber Security Metric programs available worldwide
- Good Security Metrics methodologies are:
- NIST Cybersecurity Framework vs 1.1 (April 2018)
- The CIS V7 Security Metrics 2010 and 2018
- Patching and Anti-Virus is not enough to fully protect you, but should be high on the agenda to be updated.
- Using a Security Dashboard can help management to better manage the subject

Conclusions on Cyber Security Standards:

- Office IT Standards (ISO 27000-series) are not suitable for OT (Industrial Automation) [<50% applicable]
- IEC 62443-series (is specifically for OT) is still under development and only half of the standards have been issued officially
- Certification against IEC 62443-2-4 is expensive and is feasible
- Most Vendors/Automation Solution Providers are not compliant against IEC 62443-2-4 and will need to be forced by End-Users (tried before by Shell)
- Most Projects in Industry don't specify compliancy against any Security Standards

Conclusions on Legislation:

- Governments are aware of the threats and are creating new laws, e.g. NIS-Directive and NIS2-Directive for Europe.
- As response to the NIS-directive the Dutch Government has adopted the Wbni that came into force on 9-11-2018.
- GDPR (General Data Protection Regulation) is not part of Industrial Automation, but will need to be addressed by all
- End-Users, where BRZO is applicable, have to prove that they manage Security.
- Security Incidents must be reported (Wgmc) and when not reported a significant penalty could be applicable, being part of Wbni (Wet Beveiliging Netwerk- en Informatiesystemen).
- The Netherlands and some European countries have issued a Framework to motivate, stimulate and to protect the national critical infrastructures and strategic assets and stakeholders.
- More laws will be applicable in the near future, such as NIS2….

Conclusions on General Cybersecurity:

- New vulnerabilities (resulting in Zero-Day Attacks) are being discovered every day.
- Millions of malware have been launched and the trends are still going up, based on these vulnerabilities.
- Vulnerabilities are disclosed, but is that wise?
- Even the most advanced firewalls cannot guarantee 100% protection against malware or hackers. While excellent DPI (Deep Packet Inspection) firewalls are available, their effectiveness relies on well-crafted firewall rules, and they also have vulnerabilities.
- More is required, such as 'Whitelisting (AWL)', IDS (Intrusion Detection System) and IPS (Intrusion Protection System), System Hardening, Patching, etc.
- Hacking tools are available online, just 'Google' it!
- Default passwords should be removed from your systems
- Defense in Depth (ISA95) and Defense by Design (ISA99) shall be applied!
- A Risk Assessment and Gap Analysis will show where the pain is and helps with the justification to do something about it!

Questions on General Cybersecurity:

- What is one of the most important activities you should make sure before you start an OT-Cybersecurity project?
- How did you verify that your management understands the issues with OT-Cybersecurity?
- Do you have a justification for a Security Program and is the budget available?
- Is the justification supported by Senior Management?
- What is a CTR?
- Why is it so difficult to start a Security Program?
- Do you have OT-Cybersecurity knowledge in your company and a supporting organisation?
- What is the major difference between OT-Cybersecurity and IT-Cybersecurity?
- Mention another difference between OT-Cybersecurity and IT-Cybersecurity?
- What is an OCO?
- Where would you place an OCO in your organisation and why?

The activities before you start an OT-Cybersecurity project – Summary:

- There may be a difference between Management expectations and the OT-Cybersecurity Team that needs to be managed
- Some companies have a huge knowledge gap and don't know how to handle the issues. As a result, they are waiting….
- In some companies there is a 'Turf War' going on and only Senior Management can stop this.
- There is need for a blended team of OT and IT-Engineers in each company that can manage and execute all related activities. The team members should be dedicated to the project and maintenance of the programme.
- It is difficult to create Senior Management commitment, because people have difficulty justifying the required budgets.
- Ensure that there are sufficient budgets and that all stakeholders and team members know what to do!

Questions - The 12-Basic Steps:

- What is the first step when implementing the 12-Basic Steps?
- What is the difference between a Physical network diagram and a Logical network diagram and why are both required?
- Why is it that you cannot disconnect all dial-up modems in your network, just like that?
- Do you know what your IACS Vendor can do to make your plant more secure? Did you discuss this, and do you plan this?
- How do you know that your OT and IT Network are properly separated, and did you create secure zones & conduits?
- Is your SIS only connected to the control system and EWS, and do you have a keyswitch to allow for changes to your SIS?
- What is a black channel, and can you avoid this?
- What is a disadvantage of applying HART to your SIF transmitters and what can you do to protect your transmitter from changing settings?
- What is a WSUS and AV-server and where would you install such a server?
- How would you create a Sustainability Plan?

The 12-Basic Steps – Summary:

- Don't wait with the 12-Basic Steps and do this first and fast! The 12-basic requirement steps will provide you with some protection, but not all your doors and windows are closed yet!
- A disaster recovery plan and sufficient backups are the most important steps. You should be able to rebuild your systems
- The installation of Firewalls, Removing Dial-up modems, Patching and AV is the next important step to implement. Most End-users are in the middle of this stage!
- Hardening, Secure network design and Maintaining an up-to-date Inventory are also important steps to implement.
- Your staff should know what to do when under attack or when a successful attack has taken place. Just installing a back-up (restore) is certainly not the first step to take!
- Cyber Incidents must be reported to the Government!

Questions on 'Cost & Impact Effective' Security Program (Part 1):

- What is the major difference between the 12-Basic Steps and the 'Cost & Impact Effective' Security Program?
- What Class (1, 2 or 3) does your company score, according to the ANSSI Classification standard?
- Does your company apply a company approved RAM?
- What is ALARP?
- Did you complete a Risk Assessment and Gap Analysis for OT-Cybersecurity?
- Do you have an OT Security Plan, Strategy and Policy?
- Who is responsible in your company to report Cyber incidents to the Government? And is this in R&R and a Job description?
- What is Configuration Management?
- Do you have Physical Security in place and is this tested?
- Do you allow for Remote Access of your OT systems?
- What is a Security Dashboard and for who is this important?
- What is a SIEM and what is a SOC?
- What is 2FA and MFA?

'Cost & Impact Effective' Security Program (Part 1) – Summary:

- First the 12-Basic Steps should be implemented!
- This approach of initiating the activities of a Security Program is based on a Risk Assessment and Gap Analysis!
- After completing the RA & GA, the subjects of the Security Program shall be based on Costs and Risk (Severity x Likelihood) and available budget
- 75% mitigation of the 100% possible can be realised by 15 of the 37 subjects. That doesn't mean that the other could be a threat to you OT, such as Access Control, Strong Protocols, Firewall Management, etc.
- Other subject that rank out first, could be in the program later when new budgets are made available.
- It's important that people know their Roles & Responsibilities and that OT Cybersecurity is included in their Job Descriptions.
- OT-Cyber Incidents must be reported to the Government.

Questions on 'Cost & Impact Effective' Security Program (Part 2):

- Why are Monitoring Tools, such as ForeScout Silent Defense important?
- What is a big disadvantage of Security Tools in the OT?
- What did Palo Alto announce w.r.t. Disgruntled Employees?
- Mention three weak protocols…
- Why is Time Synchronisation a cyber threat?
- Mention at least three dependencies of Obsolescence and LifeCycle Management…
- Do you have an up-to-date inventory and how do you keep this as-built?
- What are the three phases of software w.r.t. life-time?
- What is a pen test?
- Do you cover OT-Cybersecurity in your commissioning (FAT/SAT/Post)?
- What is CI and what is so special about it?
- Mention at least 5 activities that should be done during maintenance at regular intervals

'Cost & Impact Effective' Security Program (Part 2) – Summary:

- This session is the continuation of the implementation of the OT-Cybersecurity project: 12-Cost Effective Steps and 25 Sub-steps
- In this session a risk-based approach is described of many activities, depending on the outcome of the Risk Assessment. So not all the activities will be implemented.
- Some activities will score low on priority, because it could be that it is expensive and the effect is minimal, such as Data Stream models.
- It is recommended that only the most important Data Streams are described.
- Important activities, such as Remote Access, removal of default passwords, disaster recovery and network design should be handled, but the Risk Assessment should justify this.
- Finally, systems to maintain and continual Improvement (CI) should always be implemented.

Summary – Implement the maximum possible:

- Implement all that is possible or totally disconnect!
- When you implement all that is possible, you can make use of Industry 4.0 and IIoT. Optimisation of your production process is a great business case to invest in Cybersecurity.
- The Quarantine method (total disconnection from the outside world) will not allow you to transfer data to optimisers or to management tools, unless installed in the OT.
- The weakest link is now shifted to your Power Supplies and to your invoicing system. Your IT domain is still subject to malware and hacking and this can paralyse your organisation as well.
- New technology is helping to secure your systems, such as the Data Diode.
- Most important subject in the battle against malware and hacking are still human behaviour and training.

Conclusions status 2023:

- Cyber threats are new and has grown to significant heights over the last years. 70% of the threat can be successful because of ignorance of people.
- The threat is growing faster than the industry can handle.
- The impact of Cyber Security is underestimated by most (not by all).
- Governments are warning and are enforcing new legislation, e.g. NIS2.
- Most companies have installed the minimum, e.g. a weak Firewall and some Anti-Virus software on End-Points.
- Only a few companies have a sophisticated Security Programs and trained staff.
- The problem will grow fast with the present evolvement in the Automation world, e.g. IIoT and more connected Windows-based systems.
- Most companies don't know what to do and don't act.
- It's not a matter if you will be hit, but when! And when you are hit the impact should be limited when you have a proper disaster recovery plan in place.
- It is wise to move your company from reactive to proactive, e.g. by installing IDS and IPS (Intrusion Detection Systems and Intrusion Protection Systems) and to install a SIEM, etc. Avoiding is better than the cure!

Managing the OT-Cybersecurity threat is mostly managing your staff and its behaviour, as such laid down in a Strategy, Policy, Procedures, Roles and Responsibilities, creation of a supporting organisation, training of staff, reporting cyber incidents, and many more activities by people. 60-70% of all security mitigation activities are people's behaviour and 30% is about technology.

Ted Angevaare
Feb. 2024

ENGINEERING
TRAINER

The Author and your Trainer

Ted Angevaare

Independent Consultant Process Security and Owner of TAPS (Ted Angevaare Process Security)
The Hague Area, The Netherlands.

As Independent Consultant Ted brings more than 35 years of Shell experience of Process Control and Automation and 6 years as Independent Consultant. Ted has worked in all aspects of the Process Control and Automation world in Shell, with postings in Syria, Brunei, Tunisia, Morocco, Argentina, the Netherlands and other countries where Shell is active. His experience varies from Operations & Maintenance, through Engineering & Project Management to Standardisation and Leadership. As formal Shell's Global Manager of Process Control Security and Architecture (DACA) he has been active in Process Control Security and Architecture over the past decades and is the godfather and driver of Shell's DACA for which he has created Shell's first standard on Process Control Security in 2005. Shell's DACA has created a big change in Shell and has lead Shell Control & Automation discipline into a new world of Information Technology. Ted holds a degree in 'Measurement & Control' and was leading a team of more than 25 Shell experts involved in Process Security/OT-Cybersecurity), C&A Projects, Remote Operations, SIF, Process Control Architecture and Automation. Ted was also Chairman of the Control Systems Working Group of the WIB, an international group of Instrument and Control & Automation Engineers, who launched the first Industry Standard on PCD Security Requirements for Vendors and Suppliers, which was the basis of the new IEC Standard (IEC 62443-2-4, first issued in 2015 and recently in 2023). Ted is a recognized specialist in the world of Process Automation and Industrial Safety and OT-Security.

Specialties:
- Management
- Measurement, Custody Transfer, Process Control & Automation
- Process Automation Strategy and Policy
- Process Control IT-Security (OT-Cybersecurity)
- SIS (Safety Instrumented Systems) and SIF (Safety Instrumented Functions)
- Large and small project management

Objectives of this training course:
This training course is specifically designed to train Automation Engineers and IT Engineers to be merged into a new discipline Industrial Cybersecurity Engineer, also called OT-Cybersecurity Engineer.
The OT (Operational technology) are systems dedicated to control, manage, safeguard and optimise the production process of the industry. Industrial applications are known to be more reliable and robust when compared to other applications, such as office automation (IT), building automation, and home applications, because often there is a safety aspect that has an impact on the environment and could, when it fails, endanger human lives. In extreme cases failing systems in industrial applications could cause the live of multiple people and examples are the Seveso toxic gas release in Italy (1976), Bhopal Gas Tragedy in India (1984), Texas City Refinery explosion (2005), and many more, all costing the lives of thousands of people, animals and a major disruption to our environment, beside the huge financial loses. Industrial Cybersecurity could create such incidents when industrial systems fail, but much can be done to prevent this. Today, with hostile countries and hackers looking for opportunities to disrupt our world, the threat is growing beyond expectations. In this training course a structured approach is provided to create not only a robust and secure system architecture and OT, but also it will train people to a cost effective approach using a Risk Assessment and Gap Analyses as a basis to work from. This training course is broad and unique and suitable for small and large companies. Small companies could implement the minimum (12-basic steps) and when budget and time allows could implement the next phase and that is the 'Cost Effective' approach. Some industries cannot allow any compromise and have to implement the maximum to protect themselves, people and the environment and prevent huge financial loses and a damaged reputation. The training course #4 is a 4-day course.