Industrial Automation System Architecture

and OT Cybersecurity

(Training Course #6)



11 Jan 2020

**© TAPS**

Version: 1.1

# Confidentiality, Copyright and Disclaimer

**Confidential and Copyright:**

This document is **Confidential** to TAPS, Ted Angevaare Process Security, a company located at the Guirlande 123, 2496 WP the Hague in The Netherlands and registered at the Kamer van Koophandel under number 68174616. Neither the whole nor any part of this document may be disclosed to any third party without the prior written consent of TAPS, The Netherlands. The copyright of this document is vested in this company. All rights reserved. Neither the whole nor any part of this document may be reproduced, stored in any retrieval system or transmitted in any form or by any means (electronic, mechanical, reprographic, recording or otherwise) without the prior written consent of the copyright owner.

**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](http://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 6 of the TAPS training and is about ‘Industrial Automation System Architecture and OT Cybersecurity’.

Industrial Automation is the technology to automate industrial production processes and over the last two decades this technology has changed from pneumatic systems, via the first electronic systems to 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 has 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. 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 cyber-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 Cyber-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 the first fast step in the process of creating skilful staff to eliminate 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 at a multinational over the last decades.

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 by 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 the participants how to configure an Industrial Firewall or Intrusion Detection Systems, like Forescout.

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. TAPS cannot provide training for Mastery level.

This training course “6. Industrial Automation System Architecture and OT Cybersecurity” consist of the following subjects:

**Day 1:**

* General IT knowledge
* General Industrial Automation knowledge
* Industrial Architecture
* Cybersecurity, what is the threat?

**Day 2:**

* General Cybersecurity knowledge
* The activities before you start an OT-Cybersecurity project
* The OT-Cybersecurity project
* The 3rd Phase: Implement in ‘the maximum possible’
* Typical costs of a Security Program for a large refinery?
* Example of Security Plan and estimated cost

*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, 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*

*Jan. 2020*

# Content of Training Course

**Day 1**

1. **Introduction**
2. **General IT knowledge**
	1. Handshake
	2. OSI Model
	3. Parity bit
	4. TCP/IP and UDP
	5. Token Ring
	6. FTP
	7. URL
	8. HTTP, HTML and XML
	9. Ethernet
	10. Hub
	11. Gateway
	12. Router
	13. Switch
	14. USB
	15. Firewall
	16. DMZ
	17. Domain
	18. IPsec and VPN
	19. DNS
	20. NAT
	21. The Internet
	22. The Cloud
	23. Edge Computing
	24. Deep WEB and Dark WEB

**2. General Industrial Automation knowledge**

* 1. Control Theory
	2. Transmitter and Control Valves
	3. Hazardous Area
	4. Ingress Protection
	5. RS-232, RS-485 and Modbus, the industrial serial protocols
	6. HART™
	7. Profibus
	8. Foundation Fieldbus™
	9. Industrial Ethernet (IE)
	10. Other Fieldbuses
	11. OPC
	12. Smart IO
	13. Wireless
	14. Control Systems, PLC, SCADA and DCS
	15. Virtualisation
	16. Safeguarding Systems (SIF)
	17. Safety Risk Assessment
	18. The PFD of a SIF-loop
	19. SIF Certification (SIL)
	20. 1oo1, 2oo4, XooY voting transmitters
	21. Oreda (Offshore and Onshore Reliability Data)
	22. Engineering Work Station (EWS)
	23. Central Control Room (CCR)
	24. Flow computers and flow measurements
	25. Water Cut measurement
	26. Tank Gauging
	27. Fire and Gas Detection Systems
1. **Industrial Architecture**
	1. Industrial Automation, what makes it so special, robustness and integrity
	2. The difference between OT and IT
	3. Architecture and Purdue Model
	4. O-PAS™ and O-PAF ®
	5. NOA
	6. The pro’s and con’s of O-PAS and NOA
	7. How to design a network
	8. Network separation and segregation
	9. Secure Cell
	10. Zones and Conduits
	11. Workflows as a tool to optimise
	12. Remote Operations
	13. The merging of IT and OT
	14. IIoT and Industry 4.0
	15. IACS Vendors and their services
2. **Cybersecurity, what is the threat?**
	1. What’s happening?
	2. Who and why
	3. How big is the threat?
	4. Trends
	5. Latest news on Cyber Security
	6. Most successful ICS attacks in industry
	7. Successful Attacks
	8. What is the biggest threat?
	9. Cybersecurity Metrics
	10. Standards
	11. IEC 62443 series
	12. Legislation, NIS, BRZO, Csw, Wbni, Wgmc and Wdo

**Day 2**

1. **General Cybersecurity knowledge**
	1. Vulnerabilities
	2. Disclosure of vulnerabilities
	3. Vulnerability Life Cycle
	4. Types of malware
	5. Hackers and Cyber-criminals
	6. Hardening, Passwords and Default Passwords
	7. Anti-virus software
	8. Security Patching and WSUS
	9. Back-up and Restore
	10. Application White Listing (AWL)
	11. IDS
	12. IPS
	13. SOC, SIEM and Monitoring Tools
	14. OT Help Desk
	15. Cybersecurity Risk Assessment and Gap Analysis
	16. Defense in Depth (DiD)
	17. Defense by Design (DbD) and Power Supply
	18. Encryption and Cryptography
	19. Incident Management
2. **The activities before you start an OT-Cybersecurity project**
	1. What do you need to know before you start a project?
	2. 9 steps of ‘prerequisites to success’ before you start an OT Cybersecurity project
	3. Justification of a Security Program
	4. Supporting organisation, budget, knowledge of project members
	5. Planning
3. **The OT-Cybersecurity project**
	1. The Framework and overview of all project steps
	2. The Cheapest solution: Create a Secure Cell
	3. Fine-tuning of the of 12-Basic Steps
	4. **The 1st Phase:** **1a** - The Inventory and Network drawings of existing network
	5. Step 1.1 - Make an inventory of installed base
	6. Step 1.2 - Make Network drawings of existing network (incl. IP-addresses and network equipment)
	7. **The 1st Phase: 1b** - Design, prepare and train staff
	8. Step 1.3 - Check for old dial-up modems in your OT and make a plan to remove and replace the function of the dial-up modem by a network connection.
	9. Step 1.4 - Contact your Control System Vendors to inform them of your program and collect info on Vendor Solutions
	10. Step 1.5 - Separate OT and IT Network by design, e.g. with the help of a Network Designer or major ICS Vendor and create ‘defence in depth’ by segmentation
	11. Step 1.6 - Design SIS only connected to the Control System and EWS
	12. Step 1.7 - Training of Staff
	13. **The 1st Phase: 1c** - Execute the work of the 12-Basic Steps
	14. Step 1.8 - Implement changes to network and install Firewall(s)
	15. Step 1.9 - Install OT Anti-Virus clients and server in the DMZ
	16. Step 1.10 - Install WSUS or similar and patch
	17. Step 1.11 - Execute hardening and overwrite ‘Default Passwords’
	18. **The 1st Phase: 1d** - Create Sustainability and Back-ups
	19. Step 1.12 - Create Sustainability and make Back-ups, etc.
	20. **The 2nd Phase: 2a** - Determination of a ‘Cost & Impact Effective’ Security Program
	21. Step 2.1 - Make a Security Plan (use ISA99 IACS Security Program Model)
	22. Step 2.2 - Determine your ANSSI Class (Class 1-3) and perform a Risk Assessment and Gap Analysis
	23. Step 2.3 - Make 3 scenarios (depending on costs for ALARP) with associated residual risks and costs
	24. Step 2.3.1 - OT Security Plan, Strategy and Policy
	25. Step 2.3.2 - Security Management System, Roles & Responsibilities and Job Descriptions
	26. Step 2.3.3 - Incident Management
	27. Step 2.3.4 - Configuration Management
	28. Step 2.3.5 - Disconnection Procedures
	29. Step 2.3.6 - Security Administration
	30. Step 2.3.7 - Infrastructure Management
	31. Step 2.3.8 - Firewall Management System
	32. Step 2.3.9 - Access Control and Management
	33. Step 2.3.10 - Application and Data Management
	34. Step 2.3.11 - TOGAF in the OT?
	35. Step 2.3.12 - Physical Security
	36. Step 2.3.13 - Advanced Remote Access to OT
	37. Step 2.3.14 - Data Stream Model
	38. Step 2.3.15 - Two-Factor Authentication (2FA) and Single Sign-on
	39. Step 2.3.16 - Disposal / Confidential waste
	40. Step 2.3.17 - Security Dashboards, Helpdesk and SOCs
	41. Step 2.3.18 - Monitoring Tools
	42. Step 2.3.19 - Background checks
	43. Step 2.3.20 - Strong protocols
	44. Step 2.3.21 - Secure Time Synchronisation
	45. Step 2.3.22 - Wireless Security and Protocols
	46. Step 2.3.23 - Security Requirements for Vendors
	47. Step 2.3.24 - Compliance to Legislation
	48. Step 2.3.25 - Life Cycle and Obsolescence Management
	49. Step 2.4 - Create information pack of Security Plan and above results for Stake Holders and Staff involved
	50. Step 2.5 - Prepare Management Presentation, estimate planning and required staff and present 3 scenarios in order to obtain budgets.
	51. **The 2nd Phase: 2b** - Execution of a ‘Cost & Impact Effective’ Security Program
	52. Step 2.6 - Execute comprehensive training programs for own staff (See also step 1.7)
	53. Step 2.7 - Start implementation project, report regular progress reports on costs, planning, progress and staff matters.
	54. Step 2.8 - Create contracts with IACS and Security Vendors, award and execute for Implementation
	55. Step 2.9 - Create contracts with IACS and Security Vendors, award and execute for Security Maintenance, Forensics and Fast Response if required
	56. Step 2.10 - Conduct detailed commissioning, follow-up of punch lists and produce lessons learned
	57. **The 2nd Phase: 2c** - Create sustainability of a ‘Cost & Impact Effective’ Security Program
	58. Step 2.11 - Execute Continual Improvement (CI) and conduct Pen Tests on at least a yearly basis
	59. Step 2.12 - Execute Maintenance (e.g. Patching, keep AV up-to-date, review of FW-rules, keep inventory up-to-date, maintain lists of users and their authorisation, make obsolescence plan as part of life-cycle management, Pen-tests, etc.
4. **The 3rd Phase:** Implement in ‘the maximum possible’
	1. Step 3.1 - Implement Step 1: Simple and Step 2: Cost & Impact Effective first, before starting this phase
	2. Step 3.2 - Advance the Risk Assessment with an OT Attack Vector Analysis and define all Cyber Security Threats to the OT
	3. Step 3.3 - Use the Bow-tie model and implement for each Threat Vector at least three (3) ‘lines of defence’ (3LoD)
	4. Step 3.4 - Implement the best mitigation actors
	5. Step 3.5 - Stop using Shareware or other Non-auditable software
	6. Step 3.6 - Only use certified hardware and software applications
	7. Step 3.7 - Change to Secure Protocols when feasible and move away from open protocols. Apply double or multiple authentication
	8. Step 3.8 - Install DataDiode (e.g. Fox IT or Sectra) to secure segments of highest criticality and security, e.g. SIS and HIPPS. It is assumed that the SIS will only communicate to the ICS and that HIPPS will only communicate to the SIS
	9. Step 3.9 - Check applied Security Applications on the use of secure protocols and the security resilience of the application itself!
	10. Step 3.10 - Implement all administrative requirements
	11. Step 3.11 - Train all staff at required levels and repeat at regular intervals
	12. Step 3.12 - Implement Maintenance Contracts with specialist companies and patch immediately after release
	13. Step 3.13 - Implement a Continual Improvement (CI) plan and implement Sustainability plan, incl. regular Pen-tests.
	14. Step 3.14 - What else…
5. Typical costs of a Security Program for a large refinery?
6. Example of Security Plan and estimated cost

# Appendix A: Example of the subjects of an OT-Cybersecurity plan


# **The Author and Trainer**

**Ted Angevaare**

Independent Consultant Process Security and Owner of TAPS (Ted Angevaare Process Security)

The Hague Area, Netherlands.

As Independent Consultant Ted brings more than 35 years of Shell experience of Process Control and Automation and 3 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 decade and is the godfather and driver of Shell’s DACA for which he has created Shell’s first standard on Process Control Security. 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 Shell 25 experts involved in Process Security/PCD OT-Security), 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 eight years ago the first Industry Standard on PCD Security Requirements for Vendors, which was the basis of the new IEC Standard (IEC 62443-2-4, issued 2015). Ted is a recognized specialist in the world of Process Automation and Industrial Safety and OT-Security.

**Specialties:**

- Management

- Measurement, 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 projects management

***Objective 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) is the hardware and software 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 Italy (1976), Bhopal Gas Tragedy in India (1984), Chernobyl nuclear power plant (1986), 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 accidents when industrial systems are failing, but much can be done to prevent this.*

*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. 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.*

*The information presented has been gained in the last decades of working for a large multi-national and is known to be the best you can receive world-wide.*