Cybersecurity Engineer Training Schedule
5 Days

4 Days Cybersecurity Engineer + 1 Day Cybersecurity Testing Introduction

Background

ISCN is a certified training partner of iNTACS and VDA-QMC for Automotive SPICE.

https://www.intacs.info/index.php/component/weblinks/category/122-training-organisation

ISCN is a certified training body for the EuroSPI/ASA Certified Functional Safety Manager, accredited by EuroSPI/ASA (EuroSPI Certificates & Services GmbH and the ASA Automotive Skills Alliance led by ACEA).

https://conference.eurospi.net/index.php/certification

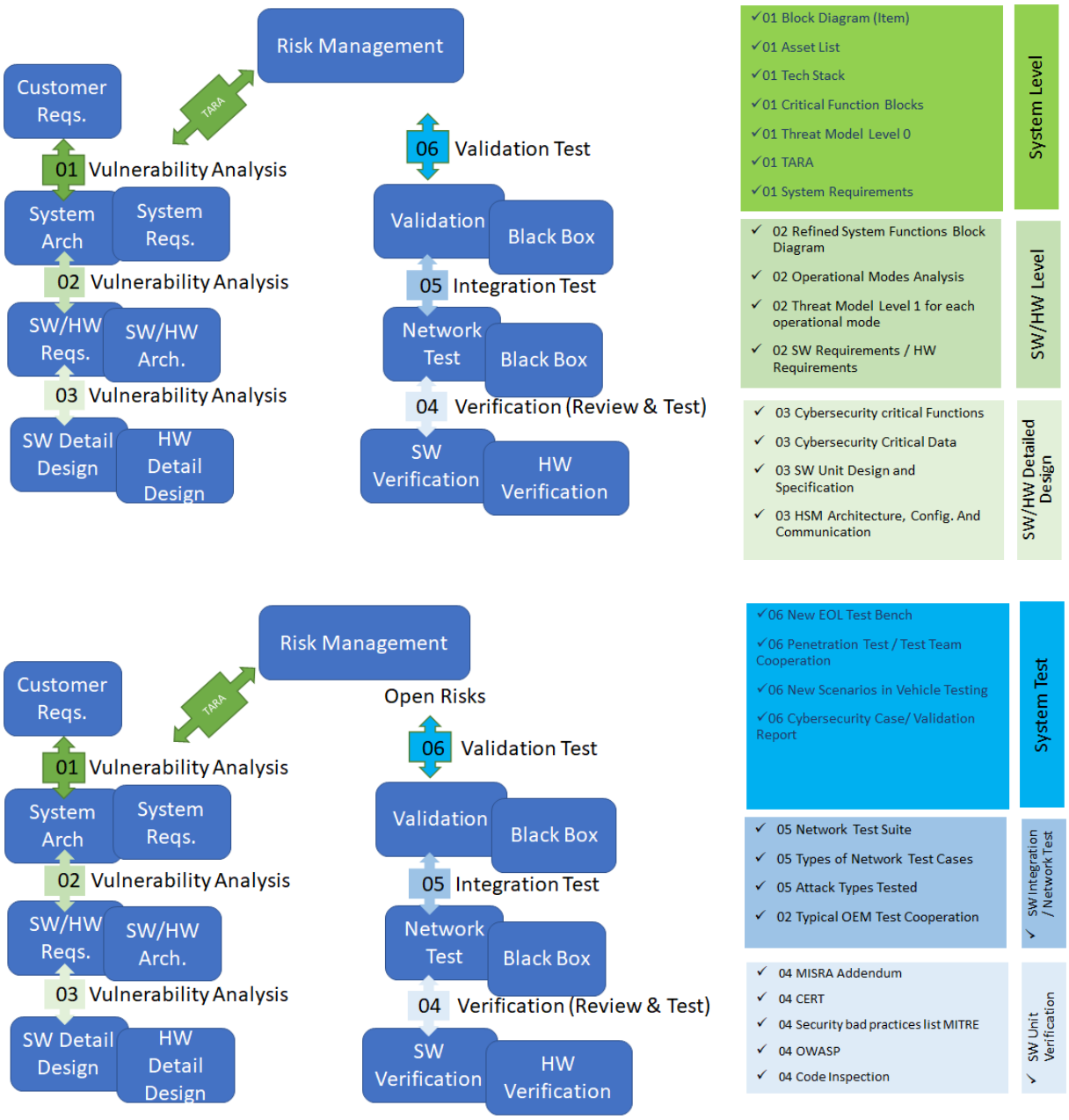
The course is based on a joined development with leading Tier 1 companies in the Soqrates group (www.soqrates.de) such as ZF Friedrichshafen AG, Continental Automotive AG, Hella KG, etc.

Cybersecurity Course

In this 5 days training course the attendees get introduced to SAE J3061 and ISO 21434 based on examples from real cybersecurity classified projects in Automotive. They will participate actively in case studies and elaborate an cybersecurity case based on your own products.

The approach of „Learning by Doing“ is used to elaborate different forms of threat and vulnerability analysis at system, software and hardware level.

See the assignment of threat analysis techniques to the V model. Also, the training material demonstrates the threat analysis of a steering system in a car and in exercises the attendees can take their own system and apply the practices and the shown best practice example on their own system in the course.



The course offers

- Examples and templates for the threat and vulnerability analysis
- A refined tool for TARA analysis (different methods possible, including HEAVENS, SAHARA, etc.)

The course is structured in 5 days as follows.

Day 1: Cybersecurity System Analysis and TARA

U3 Engineering Aspects in Cybersecurity (1 hour presentation)

U3.E1/2 System Threat Analysis and Cybersecurity Goals (1 hours presentation)

Exercise 1 Asset Analysis (0,5 hours example shown, 1 hours exercise, 1 hour discussion)

- Block Diagram (Item) – example provided
- Tech Stack – example provided
- Critical Function Blocks – example provided
- Asset List – template provided

Note: exercises demonstrate the method only on a selected set of examples.

Exercise 2 TARA Analysis (0,5 hours example/ slides shown, 1 hours exercise, 1 hour discussion)

- Threat Model Level 0 – example and template provided
- TARA – tool provided

Note: exercises demonstrate the method only based on a selected set of examples.

Day 2: Cybersecurity System & Software Analysis

Exercise 3 Deriving System Requirements from TARA (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

- System Requirements – template provided
- Refined System Functions Block Diagram – example provided
- Refined Threat Model System Level – emphasize the cyclic improvement (only if time is available)

U3.E3 Cybersecurity SW Design and Vulnerability Analysis (1,5 hours presentation)

Exercise 4 Analysing SW Architecture and Threat Modelling at SW level (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

- Operational Modes Analysis – Example and tool provided
- Threat Model Level 1 based on operational state model
- Threat Model Level 1/2 for each SW operational mode – Example provided
- TARA refined – emphasize the cyclic improvement (only if time is available)

Day 3: Cybersecurity Software Analysis

U3.E3 Cybersecurity SW Design and Vulnerability Analysis Continued (1 hours presentation)

Exercise 4 Analysing SW Threat Models and Deriving Actions and Requirements at SW level (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

- SW Requirements
- Cybersecurity Critical Functions list
- Cybersecurity Critical Data List

U3.E3 Cybersecurity SW Design and Vulnerability Analysis & Counter Actions (1 hours presentation)

- Cybersecurity Critical Data/Signals Identification
  - Encryption (global key limited time)
  - Integrity check (Message Authentication Code MAC) of messages
  - Range check, plausi check, refreshment time, loading CAN with messages …
  - SecOC specific configuration in Autosar 4.3
- Cybersecurity Critical Functions Identification/List
  - Best Practice List from OEMs
  - Attack Flow / Attack Tree Modelling (Cybersecurity Critical Flow)
  - Cybersecurity Defense Layer Model
  - Typical Cybersecurity Related Architectural Components / Layers
- Design Concepts:
  - Cybersecurity Critical Data/Signals Identification
    - Encryption (global key limited time, software variables marked and checked)
  - Cybersecurity Critical Functions Identification/List
    - E.g. secure boot
    - E.g. SOTA – Software-over-the-air
    - E.g. secure storage in Autosar (signed, encrypted …)
    - E.g. secure communication config in an Autosar system
    - E.g. security services functions
    - E.g. signature functions to assure parts were not changed (checksum for memory)
    - E.g. secure diagnosis functions (Security Access – Service 0x27, encrypted, SecOC …)
    - E.g. Secure Debug
    - Quality of keys, key generation, and key management
    - Attack examples

Exercise 5 Analysing SW Threat Models and Deriving Actions and Requirements at SW level (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

- Cybersecurity Critical Functions and Counter Actions
- Cybersecurity Critical Data and Counter Actions
- SW Unit Design and Specification Requirements

Day 4: Cybersecurity Critical Detailed and Unit Design

U3.E4 Cybersecurity Detail Design (1 hours presentation)

- Detailed Design Principles

- Known faults and preventive programming
- Secure coding guidance
- e.g. MISRA 2012 – security extension (amendment 1)
- E.g. guidelines of OWASP https://owasp.org/
- Security bad practices list https://cwe.mitre.org/
- Code inspection
- Listing of qualified tools

Exercise 6 Deriving requirements for SW unit design (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

- SW Unit Design and Specification Requirements
- Use MITRE and OWASP and reflect the current programming guide

U3.E5 Hardware and HSM Chip Architectures Basics (1 hours presentation)

Exercise 7 Deriving requirements for the right hardware and base SW setup – Selection of HSM Chip Exercise (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

- SW Unit Design and Specification Requirements
- Use MITRE and OWASP and reflect the current programming guide

Day 5: Cybersecurity Testing & Validation

U4 Test Aspects in Cybersecurity (2 hours lecture)

- Testing at SW Unit Level
- Network test suites and testing at system integration level (usually provided also by OEM)
- Validation / penetration testing

Exercise 8 Deriving test cases to simulate attacks (0,5 hours example /slides shown, 2 hours exercise, 1 hour discussion)

- Elaborating test case examples applying the presented methods

Outlook to Future Secure Vehicle Design (1 hour)

- What security architectures will come

Certification through ECQA and Wrap Up (1 hour)

Target Group Cybersecurity Engineers / Managers

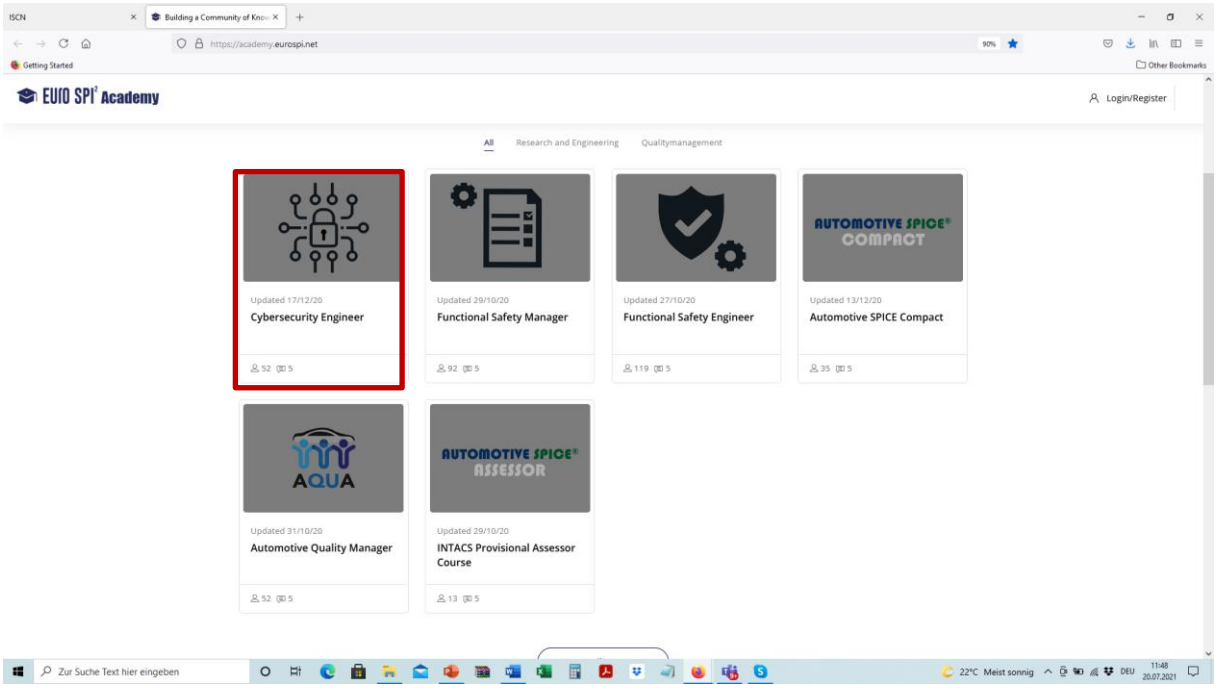
Engineers and managers who want to learn practical examples of applying cybersecurity with best practice tools and methods.

Resources

Cybersecurity Materials

The course materials and lectures are online available on the EuroSPI Academy platform. The materials will be provided latest till 16.12.

https://academy.eurospi.net/



- Select the course Cybersecurity Engineer (is accessible from 16.12.2020)
- Register
- You will receive an email and need to confirm by clicking the link in your email.
- Then you can login
- You need the enrollment key **– will be provided -**

Course Schedule

Day 1: Cybersecurity System Analysis and TARA

Day 1 08.00 - 08.30 Introduction to Safety Manager Strategy Level,
Safety Engineer, and Safety Project Manager Qualification

08.00 – 09.00 U3 Engineering Aspects in Cybersecurity (1 hour presentation))

09.00 – 10.00 U3.E1/2 System Threat Analysis and Cybersecurity Goals (1 hours presentation)

10.15 – 12.45 Exercise 1 Asset Analysis (0,5 hours example shown, 1 hours exercise, 1 hour discussion)

12.45 – 13.30 Lunch Break

13.30 – 16.00 Exercise 2 TARA Analysis (0,5 hours example/ slides shown, 1 hours exercise, 1 hour discussion)

Day 2: Cybersecurity System & Software Analysis

08.00 – 10.30 Exercise 3 Deriving System Requirements from TARA (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

10.45 – 12.30 U3.E3 Cybersecurity SW Design and Vulnerability Analysis (1,5 hours presentation)

12.30 – 13.30 Lunch Break

13.30 – 16.00 Exercise 4 Analysing SW Architecture and Threat Modelling at SW level (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

Day 3: Cybersecurity Software Analysis

08.00 – 09.00 U3.E3 Cybersecurity SW Design and Vulnerability Analysis Continued (1 hours presentation)

09.15 - 11.45 Exercise 4 Analysing SW Threat Models and Deriving Actions and Requirements at SW level (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

11.45 – 12.45 U3.E3 Cybersecurity SW Design and Vulnerability Analysis & Counter Actions (1 hours presentation)

12.45 – 13.30 Lunch Break

13.30 – 16.00 Exercise 5 Analysing SW Threat Models and Deriving Actions and Requirements at SW level (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

Day 4: Cybersecurity Software Analysis

08.00 – 09.00 U3.E4 Cybersecurity Detail Design (1 hours presentation)

09.15 – 11.45 Exercise 6 Deriving requirements for SW unit design (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

11.45 – 12.45 U3.E5 Hardware and HSM Chip Architectures Basics (1 hours presentation)

12.45 – 13.30 Lunch Break

13.30 – 16.00 Exercise 7 Deriving requirements for the right hardware and base SW set up – Selection of HSM Chip Exercise (0,5 hours example /slides shown, 1 hours exercise, 1 hour discussion)

Day 5: Cybersecurity Testing & Validation

08.00 – 11.00 U4 Test Aspects in Cybersecurity (2 hours lecture)

11.00 – 12.30 Exercise 8 Deriving test cases to simulate attacks (0,5 hours example /slides shown, 2 hours exercise, 1 hour discussion)

12.30 – 13.30 Lunch Break

13.30 – 14.30 Continued: Exercise 8 Deriving test cases to simulate attacks (0,5 hours example /slides shown, 2 hours exercise, 1 hour discussion)

14.30 – 15.30 Outlook to Future Secure Vehicle Design (1 hour)

15.30 – 16.00 Certification with ECQA and Wrap Up (1 hour)

MS Teams Links

Will be provided

This course is based on practical Automotive examples from Cybersecurity projects in Ford, DAG and BMW security classified projects. The exercises are based on best practices in cybersecurity projects which were implemented at leading Automotive suppliers and OEMs.