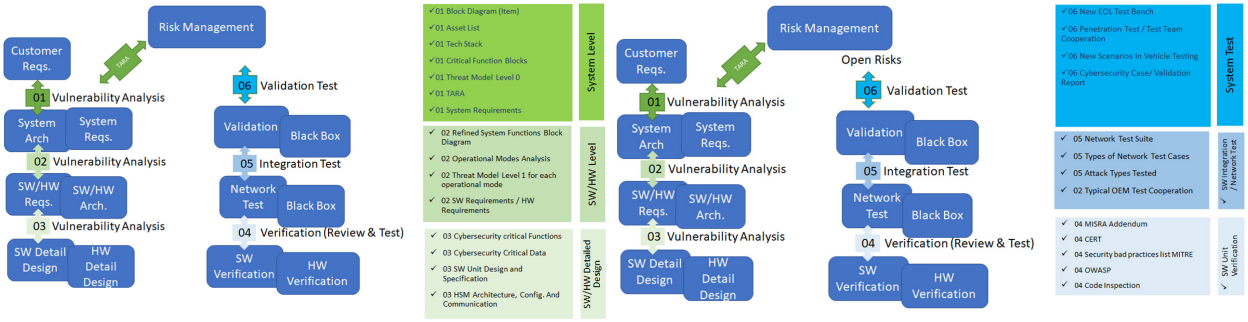
EuroSPI / ASA Certified Cybersecurity Engineer - Expert Level

Goal

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 ISO 21434 Appendix F-H, HEAVENS, SAHARA, etc.)

Content

The course is based on a joined development with leading Tier 1 companies in the Soqrates group (https://soqrates.eurospi.net) such as ZF Friedrichshafen AG, Continental Automotive AG, BOSCH Engineering, MAGNA, Elektrobit, Hella KG, etc.
The course is based on a skills set developed ion the EU Blueprint project DRIVES which led to the foundation of the ASA (Automotive Skills Alliance). EuroSPI is a member of ASA and certifies these courses. ASA members include ACEA, CLEPA, ETREMA, and many more European automotive associations. See ASA Learning Platform (skills-framework.eu)

The course focuses on the following skills elements of that cybersecurity engineer skills set:

Unit 3 – Element 1: System Threat Analysis and Cybersecurity Goals
Unit 3 – Element 2: System Design and Vulnerability Analysis
Unit 3 – Element 3: Software Design and Vulnerability Analysis
Unit 3 – Element 4: Software Detailed Design and Cybersecurity
Unit 3 – Element 5: Hardware Design and Vulnerability Analysis
Unit 4 – Element 1: Cybersecurity verification at SW level
Unit 4 – Element 2: Cybersecurity verification at HW level
Unit 4 – Element 3: Cybersecurity verification at SW level

The course is structured in 5 days as follows.

Schedule

Day 1: Cybersecurity System Analysis and TARA

Time	Activity
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 presenta tion)
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

Time	Activity
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

Time	Activity
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

Time	Activity
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 presen tation)
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

Time	Activity
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)

Training Materials

The training materials include slides, templates for Functional Safety Concept, Technical Safety Concept, Safety Analysis and Dependency Analysis, Diagnose Matrix, HIS – Hardware Software Interface, FIT rates, FMEDA, FTA, etc.
Also tools for FIT rate calculation and methods to calculate an FNEDA are provided. A pool of best practice and state of the art publications from the working group SOQRATES are provided. Additionally the training is supported by an online teaching environment set up on the online EuroSPI academy platform.

Target Group and Prerequisites

Cybersecurity manager, cybersecurity engineer, system architect, software architect, quality engineer, quality manager, project leaders, experienced engineers who are confronted with cybersecurity design. Cybersecurity decisions and design require a background in hardware/electronics and/or software engineering. Also a basic understanding of modelling techniques is helpful. Usually attendees require some minimum 5 years work experience in automotive software or hardware to easily manage the course exercises.

Cancellation

Cancellation is not possible. You may determine a substitute or attend the course at a later date.

Examination and Certification

Exams are organised by the EuroSPI / ASA certification organisation. In case of safety engineers the exam is based on a set of mandatory exercises to be performed in the course under the observation of the trainers. The EuroSPI / ASA system allows to register with a job role, upload the exercises and have an assessor in the system assessing the student performance in the practical exercises. The EuroSPI / ASA system generates a unique certification ID and certificate for the attendee. Every 2 years the certificate will later need to be renewed by attending a short update training of 1 day to learn about the new state of the art developments in functional safety.

The EuroSPI Academy

The training is held in the EuroSPI academy in cooperation with ISCN. The company ISCN is a certified training partner of VDA-QMC and Intacs® for Automotive SPICE (https://www.iscn.com/ressources/PDFs/ISO330xx-intacs-cert-iscn.pdf, https://www.intacs.info/training-center).

The EuroSPI Academy (https://academy.eurospi.net) was founded in 2021 in cooperation with the ASA (Automotive Skills Alliance) and offers an advanced online training environment with materials, templates and exercises. EuroSPI and ISCN are full partners of the ASA (https://automotives-kills-alliance.eu/#partners). In cooperation with ASA WG 3.6 (IT in Automotive) and the EU project FLAMENCO this training platform will be further developed in the next years.

Join our community of knowledge.