ECQA Certified Cybersecurity Engineer and Manager

Automotive Sector

IO2

Skills set for an ECQA Certified Cybersecurity Engineer and Manager – Automotive Sector based on ECQA skills definition standards

With the support of the Erasmus+ Programme of the European Union

Report Title:	**Skills Set for an ECQA Certified Cybersecurity Engineer and Manager – Automotive Sector Based on ECQA Skills Definition Standards**		
Author(s):	Georg Macher; Eugen Brenner		
Responsible Project Partner:	TUG	**Contributing Project Partners:**	VSB-TUO; REAL-SEC; Elektrobit; ISCN; AIT

Document data:	**File name:**	CYBERENG IO2 Skills Set		
	Pages:	56	**No. of annexes:**	5
	Status:	Final	**Diss. Level:**	PU
Project title:	ECQA Certified Cybersecurity Engineer and Manager – Automotive Sector		**KA No.:**	KA203-FE74E5D7
			Output No:	IO2
Date:	**Due Date:**	31/7/2021	**Submission date:**	05/08/2021
Keywords:	Cybersecurity; engineer; manager; skills; competence; performance criteria			
Review by:	Marek Spanyik, VSB-TUO		**Review date:**	27/07/2021
	Andreas Gasch, EB			04/08/2021
Approved by:	Jakub Stolfa, VSB-TUO		**Approval date:**	04/08/2021

For more information, visit the project website

CYBERENG (project-cybereng.eu)

With the support of the Erasmus+ Programme of the European Union

1. INTRODUCTION

1.1. Objective

The objective of this deliverable is to provide a description of the job role within the applied skills definition model.

The DRIVES (EU Blueprint project for Automotive, 2018 – 2021) skills needs analysis outlined that within the automotive valuechain is a high demand in the training of cybersecurity-related skills of their engineering and testing staff. In the project group, brainstorming took place and structures of units and elements have been designed. These concepts have further been elaborated in cooperation with partners from the SoQrates working group, which elaborates and shares best practices of knowledge since 2019.

Three job roles have been considered in the analysis, while the testing job role was not further elaborated within this project:

1. ECQA Certified Cybersecurity Manager;
2. ECQA Certified Cybersecurity Engineer;
3. ECQA Certified Cybersecurity Tester (out of scope for CYBERENG).

In the continuation of the work, in alignment with the SOQRATES working group, the CYBERENG project has further elaborated this structure and enhanced it based on a survey of domain experts (IO1). This document focuses on the skills required for the cybersecurity manager and engineer.

1.2. Purpose of the Deliverable

This deliverable details the skills definitions of the Automotive Cybersecurity Engineer and Manager job role within the ECQA skills definition model.

1.3. Scope of the Deliverable

The deliverable contains:

- description of the content of the job roles within the automotive domain;
- description of used skill sets and skills definitions;
- description of the coverage of qualification schemas.

With the support of the Erasmus+ Programme of the European Union

The deliverable does not cover course materials (which are part of IO3). These training materials will be developed based on the different job roles' skill definitions. Furthermore, the jobrole of Cybersecurity Tester is out of scope for this project/deliverable.

With the support of the Erasmus+ Programme of the European Union

2. ECQA Skills Definition Model

This chapter provides and overview of the ECQA skills definition model. Figure 1 is giving a general overview and indicating the mutual relations, while in the following the individual terms of a skills definition are explained.

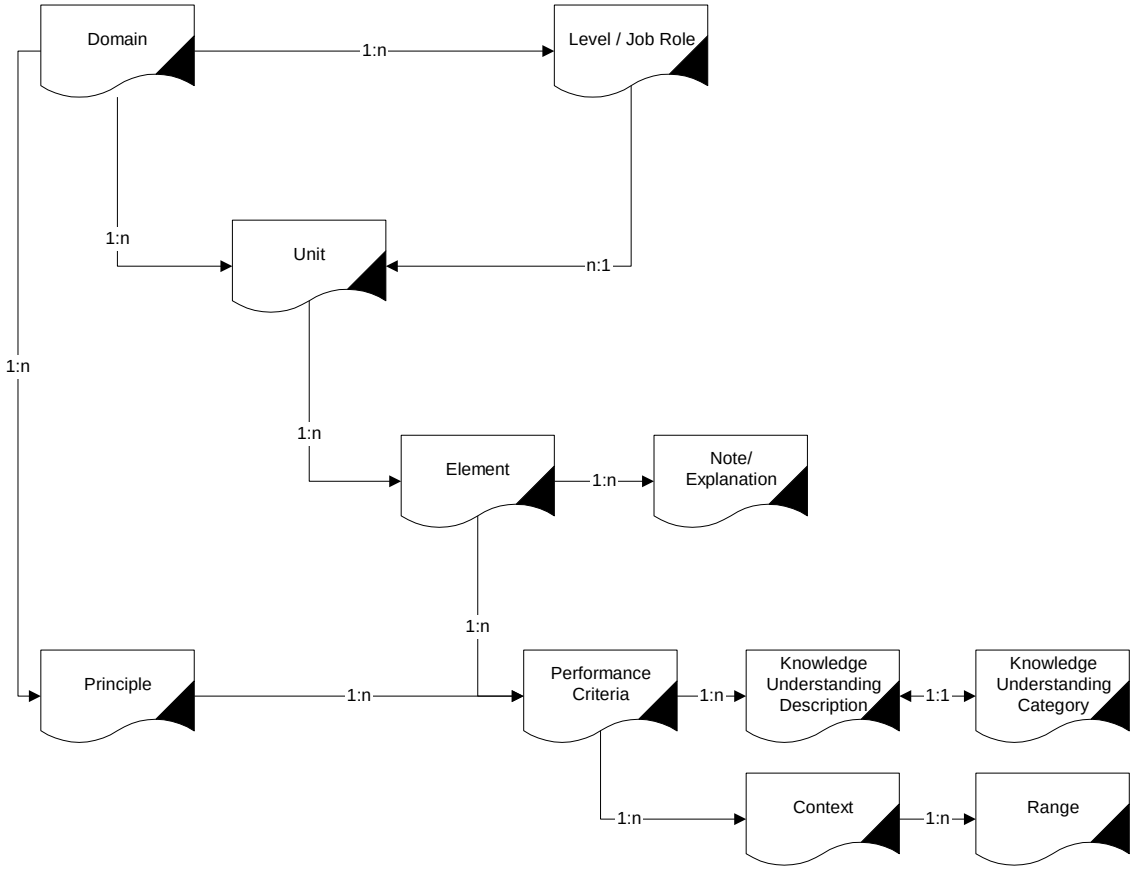

Figure 1 The Skill Definition Model (1:N = one to many relationships)

A skills definition contains the following items:

Context: A category of ranges; it represents some terminology used in a performance criterion that consists of different contexts, conditions or circumstances. A participant must be able to prove competence in all the different cases covered by the context.

Domain: An occupational category, e.g. childcare, first-level management or software engineering.

Element: Description of one distinct aspect of the work performed by a worker, either a specific task that the worker has to do or a specific way of working. Each element consists of several performance criteria.

With the support of the Erasmus+ Programme of the European Union

Evidence: Proof of competence.

Knowledge and understanding category: A category of knowledge and understanding descriptions.

Knowledge and understanding description: A description of certain knowledge and understanding. To be judged competent in a unit, a participant must prove to have and to be able to apply all the knowledge and understanding attached to it.

NVQ (UK based): The National Vocational Qualification standard of England, Wales and N. Ireland.

Performance criterion: Description of the minimum level of performance a participant must demonstrate in order to be assessed as competent. A performance criterion may have relevant contexts.

Principle: A statement of good intentions; underpins all competent domain practice.

Range: Description of a specific circumstance and condition of a performance criterion statement.

Qualification: The requirements for an individual to enter or progress within a specific occupation.

Job Role: A certain profession that covers part of the domain knowledge. E.g. domain = Functional Safety, job role = Functional Safety Manager.

Unit: A list of certain activities that have to be carried out in the workplace. It is the top-level skill in the UK qualification standard hierarchy, and each Unit consists of several elements.

The rationales for developing the ECQA skills definition model is based on the skills definition proposed by the DTI (Department of Trade and Industry) in the UK for the NVQ (National Vocational Qualification) standards. Other countries have re-used and slightly modified these models when they started employing skill cards [1], [2].

ECQA standards are used to describe the skills sets. Further description and rationales are attached in annexes of this document.

With the support of the Erasmus+ Programme of the European Union

3. Skills Definition for the Job Role Automotive Cybersecurity Manager

3.1. The Skills Hierarchy

In the preparation of the CYBERENG project, the project consortium, in cooperation with the SoQrates working group (https://soqrates.eurospi.net/), identified the following job roles for cybersecurity:

1. Automotive Cybersecurity Manager
2. Automotive Cybersecurity Engineer
3. Automotive Cybersecurity Tester (out of scope)

The first two roles were identified as foundational jobs for automotive cybersecurity and the CYBERENG project was therefore set up with the focus on the development of courses for Automotive Cybersecurity Manager and Automotive Cybersecurity Engineer. The Automotive Cybersecurity Tester job role is out of scope of the CYBERENG project. The overall set of units and elements for the CYBERENG project have also been assigned to levels of skills (awareness, practitioner, expert level) as described in [12].

- **Expert:** an expert knowledge or competence/skill inherits the ability to develop and apply procedures and perform activities as an individual and/or provide it's qualified opinion to a team. An expert is a recognised specialist and advisor in the generation of solutions and ideas, including methods, tools, techniques, guiding or leading others in best practice use of the specific knowledge and skill.
- **Practitioner:** has a strong understanding of the knowledge, the experience in the competence/skill required in the field. Practitioners are able to apply knowledge, experience of competence/skill, share with others, including tools and techniques, and define and use the most appropriate solution.
- **Awareness:** Awareness level indicates the understanding of the background of the knowledge, competence/skill, and its implications to understand how it is applied in the environment.

With the support of the Erasmus+ Programme of the European Union

Units (U) and Elements (E) of the skill card	Cybersecurity Engineer	Cybersecurity Manager	Cybersecurity Tester
Unit 1 Cybersecurity Management			
U1.E1 Legal Aspects and Privacy		practitioner	
U1.E2 Organisational Structure		practitioner	
U1.E3 Cybersecurity Planning		practitioner	
Unit 2 Cybersecurity Operation and Maintenance			
U2.E1 Life Cycle Assessment		expert	
U2.E2 Cybersecurity processes and audits		expert	
U2.E3 Incident Response Management		expert	
U2.E4 Supply Chain Security		expert	
Unit 3 Engineering aspects of cybersecurity			
U3.E1 System Threat Analysis and Cybersecurity Goals	expert	awareness	
U3.E2 System Design and Vulnerability Analysis	expert	awareness	
U3.E3 Software Design and Vulnerability Analysis	expert	awareness	
U3.E4 Software Detailed Design and Cybersecurity	expert	awareness	
U3.E5 Cybersecure hardware and firmware design	expert	awareness	
Unit 4 Testing aspects of cybersecurity			
U4.E1 Cybersecurity verification at SW level		awareness	expert
U4.E2 Cybersecurity verification at HW level		awareness	expert
U4.E3 Cybersecurity verification at system level		awareness	expert

Out of Scope for CYBERENG

Figure 2 The Skills Set for ECQA Certified Cybersecurity Related Job Roles

Figure 2 depicts a collection of units and elements of the developed skill card, as well as the classification of cybersecurity engineer/manager skills. The green part shows the scope of the CYBERENG project (i.e., Automotive Cybersecurity Engineer and Manager). However, as indicated in red, the cybersecurity tester is not included in the scope of the project.This document describes the skills set for the cybersecurity manager and engineer.

With the support of the Erasmus+ Programme of the European Union

3.2. THE SKILLS DESCRIPTIONS – JOB ROLE Automotive CYBERSECURITY Manager/Engineer

Domain Acronym: Engineering

Domain title: Cybersecurity in Automotive

Domain Description:

The design of modern vehicles requires considering cybersecurity-related norms and regulations (such as ISO/SAE 21434 / UN Regulation No. 155 - Cybersecurity and cybersecurity management system) and implementing security-related design patterns. This includes but is not limited to

- Consideration of cybersecurity risks early on and at key development stages (mainly those with design decisions)
- Identification and addressing of potential threats and attack scenarious
- Appropriate methods of attack surface reduction
- Layered cybersecurity defenses (defense-in-depth)
- Identification of trust boundaries
- Inclusion of security design reviews in the development process
- Emphasising secure connections
- Limiting of network interactions
- Integrity and security testing methods
- SW-level vulnerability testing strategies
- Validation strategies of security systems at the vehicle level

3.2.1. Cybersecurity Manager

Job Role Acronym: CYBERMAN

Job Role Title: Automotive Cybersecurity Manager

Description:

The Skill card comprises the following thematic learning units and learning elements (which will be detailed in Section 3.3 – 3.6) for the job role cybersecurity manager:

With the support of the Erasmus+ Programme of the European Union

1. **Unit 1 – Cybersecurity Management**
    a. U1.E1 Legal Aspects and Privacy (practitioner)
    b. U1.E2 Organisational Structure (practitioner)
    c. U1.E3 Cybersecurity Planning (practitioner)
2. **Unit 2 – Cybersecurity Operation and Maintenance**
    a. U2.E1 Life Cycle Assessment (expert)
    b. U2.E2 Cybersecurity processes and audits (expert)
    c. U2.E3 Incident Response Management (expert)
    d. U2.E4 Supply Chain Security (expert)
3. **Unit 3 – Engineering aspects of cybersecurity**
    a. U3.E1 System Threat Analysis and Cybersecurity Goals (awareness)
    b. U3.E2 System Design and Vulnerability Analysis (awareness)
    c. U3.E3 Software Design and Vulnerability Analysis (awareness)
    d. U3.E4 Software Detailed Design and Cybersecurity (awareness)
    e. U3.E5 Cybersecurity hardware and firmware design (awareness)
4. **Unit 4 – Testing aspects of cybersecurity**
    a. U4.E1 Cybersecurity Verification at SW level (awareness)
    b. U4.E2 Cybersecurity Verification at HW level (awareness)
    c. U4.E3 Cybersecurity Verification at the System level (awareness)

3.2.2. Cybersecurity Engineer

Job Role Acronym: CYBER

Job Role Title: Automotive Cybersecurity Engineer.

Description:

The skill card for the cybersecurity engineer job role includes the following thematic learning elements in Unit 3 (details for these unit will be provided in Section 3.3).

Unit 3 – Engineering aspects of cybersecurity

a. U3.E1 System Threat Analysis and Cybersecurity Goals (expert)
b. U3.E2 System Design and Vulnerability Analysis (expert)
c. U3.E3 Software Design and Vulnerability Analysis (expert)

With the support of the Erasmus+ Programme of the European Union

d. U3.E4 Software Detailed Design and Cybersecurity (expert)
e. U3.E5 Cybersecurity Hardware and Firmware Design (expert)

3.3. Unit CYBER.U1 Cybersecurity Management

Acronym: CYBER.U1

Title: Cybersecurity Management

Description:

The first Unit introduces the subject of Cybersecurity, with a particular focus on management topics, such as

- Legal Aspects and Privacy
- Organisational Structure
- Cybersecurity Incident Management

3.3.1. Unit CYBER.U1 – Element 1: Legal Aspects and Privacy

Acronym: CYBER.U1.E1

Element Title: Legal Aspects and Privacy

Element Note:

This element gives an overview of the following aspects:

- The trainee knows about the legal situation
- The trainee knows about cases showing a high business impact
- The trainee knows about the issue of complex mechatronic products and dependability relation
- The trainee knows the most important norms and their main meaning required for homologation of cars in context of dependability engieering.

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

With the support of the Erasmus+ Programme of the European Union

Table 1 Performance Criteria for the Element CYBER.U1.E1

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U1.E1.PC1	The trainee knows about data protection laws.
CYBER.U1.E1.PC2	The trainee knows about the general hacker paradigm applicable in the automotive domain for elaborating the testing.
CYBER.U1.E1.PC3	The trainee knows about the international regulations regarding cybersecurity type approval and product liability law and the resulting consequences and requirements.

3.3.2. Unit CYBER.U1 – Element 2: Organisational Structure

Acronym: CYBER.U1.E2

Element Title: Organisational Structure

Element Note:

This element introduces aspects, such as

- Cybersecurity related roles
- Cybersecurity related organisational structures
- Cybersecurity planning

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

With the support of the Erasmus+ Programme of the European Union

Table 2 Performance Criteria for the Element CYBER.U1.E2

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U1.E2.PC1	The trainee knows the roles needed for cybersecurity in the automotive domain.
CYBER.U1.E2.PC2	The trainee knows typical organisational structures supporting the implementation of cybersecurity-related norms and relations to related organisational topics
CYBER.U1.E2.PC3	The trainee knows how to manage and escalate risks in the organisation.

3.3.3. Unit CYBER.U1 – Element 3: Cybersecurity Planning

Acronym: CYBER.U1.E3

Element Title: Cybersecurity Planning

Element Note:

This element deals with

- The trainee knows how to establish a plan for the project
- The trainee knows which methods to select for cybersecurity engineering
- The trainee knows considerations related to development, production, or series maintenance (the entire life cycle needs to be considered).

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

With the support of the Erasmus+ Programme of the European Union

Table 3 Performance Criteria for the Element CYBER.U1.E3

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U1.E3.PC1	The trainee knows about how to establish and maintain cybersecurity plans in an Automotive project.
CYBER.U1.E3.PC2	The trainee knows the method selection for the different process steps (threat analysis methods, test methods and tools, etc.) and knows how to document this in the plan.
CYBER.U1.E3.PC3	The trainee knows that work products and tasks need to be planned for the entire life cycle, not only development, also production or series maintenance.

With the support of the Erasmus+ Programme of the European Union

3.4. Unit CYBER.U2 Cybersecurity Operation and Maintenance

Acronym: CYBER.U2

Title: Cybersecurity Operation and Maintenance

Description:

This Unit addresses

- The trainee knows cybersecurity related life cycle assessment
- The trainee knows cybersecurity processes and audits
- The trainee knows incident response management
- The trainee knows supply chain security aspects

3.4.1. Unit CYBER.U2 – Element 1: Life Cycle Assessment

Acronym: CYBER.U2.E1

Element Title: Life Cycle Assessment

Element Note:

This element includes skills needed to assess threats throughout the automotive life cycle, not just during development.

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 4 Performance Criteria for the Element CYBER.U2.E1

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U2.E1.PC1	The trainee is able to analyse threats in all phases of the automotive life cycle.
CYBER.U2.E1.PC2	The trainee is able to assess vulnerabilities in all phases of the automotive life cycle and is aware of possible threat information sources.

With the support of the Erasmus+ Programme of the European Union

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U2.E1.PC3	The trainee is able to set appropriate measures to solve vulnerabilities in all phases of the automotive life cycle, e.g. key handling, update of SW according to UNECE regulations, EOL in production, trust provisioning, etc.

3.4.2. Unit CYBER.U2 – Element 2: Cybersecurity processes and audits

Acronym: CYBER.U2.E2

Element Title: Cybersecurity processes and audits

Element Note:

This element includes requirements to collect evidence to prepare for a cybersecurity process audit.

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 5 Performance Criteria for the Element CYBER.U2.E2

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U2.E2.PC1	The trainee knows the clauses of the ISO 21434 norm and how they can be mapped to the processes of an organisation.
CYBER.U2.E2.PC2	The trainee knows the clauses of other automotive cybersecurity guidelines (e.g. SAE J3061) and how they can be mapped to the processes of an organisation.
CYBER.U2.E2.PC3	The trainee knows how an organisational audit (e.g. ISO PAS 5112) and a product assessment (e.g. ISO/SAE 21434) is planned, performed, and documented.

With the support of the Erasmus+ Programme of the European Union

3.4.3. Unit CYBER.U2 – Element 3: Incident Response Management

Acronym: CYBER.U2.E3

Element Title: Incident Response Management

Element Note:

This element deals with methods and approaches to handle incidents in the field.

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 6 Performance Criteria for the Element CYBER.U2.E3

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U2.E3.PC1	The trainee knows how to react in case of a public incident in general.
CYBER.U2.E3.PC2	The trainee knows the procedures to alert consumers and the authorities.
CYBER.U2.E3.PC3	The trainee knows how to establish urgent response procedures, including all relevant suppliers.
CYBER.U2.E3.PC4	The trainee knows how to form an urgent response team, including experts from different impacted domains.

3.4.4. Unit CYBER.U2 – Element 4: Supply Chain Security

Acronym: CYBER.U2.E4

Element Title: Supply Chain Security

Element Note:

With the support of the Erasmus+ Programme of the European Union

Supply chain security includes the entire supply chain and necessary controls to keep up a secure environment.

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 7 Performance Criteria for the Element CYBER.U2.E4

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U2.E4.PC1	The trainee is able to set up a Development Interface Agreement based on security requirements with suppliers.
CYBER.U2.E4.PC2	The trainee is able to define secure interfaces between suppliers during development, operation and maintenance.
CYBER.U2.E4.PC3	The trainee is able to plan and prepare for cybersecurity audits at the supplier site.
CYBER.U2.E4.PC4	The trainee knows about potential human risks (e.g. developers/suppliers building holes into the system) and considers strategies to avoid harm.

3.5. Unit CYBER.U3 Engineering aspects of cybersecurity

Acronym: CYBER.U3

Title: Engineering aspects of cybersecurity

Description:

This Unit is about the analysis and design techniques used for cybersecurity during the development. It addresses topics such as

- System Threat Analysis and Cybersecurity Goals
- System Design and Vulnerability Analysis
- Software Design and Vulnerability Analysis
- Software Detailed Design and Cybersecurity
- Hardware and Firmare Design

With the support of the Erasmus+ Programme of the European Union

3.5.1. Unit CYBER.U3 – Element 1: System Threat Analysis and Cybersecurity Goals

Acronym: CYBER.U3.E1

Element Title: System Threat Analysis and Cybersecurity Goals

Element Note:

This element addresses

- Types of attacks
- Known threat lists
- Cybersecurity assets
- Describing system items, including the assets that could be attacked
- Threat and Risk Analysis (TARA)
- Cybersecurity goals
- Threat modelling tools

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 8 Performance Criteria for the Element CYBER.U3.E1

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U3.E1.PC1	The trainee knows different types of attacks.
CYBER.U3.E1.PC2	The trainee is able to work with known threat lists.
CYBER.U3.E1.PC3	The trainee is able to identify and document cybersecurity assets (asset analysis), their cybersecurity properties and impact if the cybersecurity properties are violated.
CYBER.U3.E1.PC4	The trainee is able to describe system items, including the system structure and the cybersecurity assets as potential attack targets.

With the support of the Erasmus+ Programme of the European Union

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U3.E1.PC5	The trainee is able to perform a TARA (Threat and Risk Analysis) and document it.
CYBER.U3.E1.PC6	The trainee is able to derive cybersecurity goals from the TARA (Threat and Risk Analysis) and document them.
CYBER.U3.E1.PC7	The trainee is able to generate a threat model of the automotive system structure.

3.5.2. Unit CYBER.U3 – Element 2: System Design and Vulnerability Analysis

Acronym: CYBER.U3.E2

Element Title: System Design and Vulnerability Analysis

Element Note:

This element addresses at the system level related cybersecurity methods.

This includes

- The trainee knows how to apply cybersecurity design patterns on system level
- The trainee knows how to perform an attack tree analysis
- The trainee knows how to perform vulnerability analysis and integrating a proper defence mechanism
- The trainee can integrate cybersecurity views into the system architectural design
- The trainee knows how to write cybersecurity requirements

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 9 Performance Criteria for the Element CYBER.U3.E2

With the support of the Erasmus+ Programme of the European Union

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U3.E2.PC1	The trainee knows cybersecurity design patterns on the system level and how to apply them.
CYBER.U3.E2.PC2	The trainee is able to perform an attack tree analysis.
CYBER.U3.E2.PC3	The trainee is able to perform vulnerability analysis and implement a proper defence mechanism.
CYBER.U3.E2.PC4	The trainee is able to integrate cybersecurity views into the system architectural design.
CYBER.U3.E2.PC5	The trainee is able to write and trace cybersecurity requirements.

3.5.3. Unit CYBER.U3 – Element 3: Software Design and Vulnerability Analysis

Acronym: CYBER.U3.E3

Element Title: Software Design and Vulnerability Analysis

Element Note:

This element looks at the software level related cybersecurity methods.

- The trainee is able to perform a Cybersecure Data Analysis
- The trainee is able to perform a Cybersecure Functions Analysis
- The trainee is able to write cybersecurity software requirements
- The trainee knows how to integrate cybersecurity views into the software architectural design
- The trainee knows how to apply a list of state of the art software-related cybersecurity design patterns

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

With the support of the Erasmus+ Programme of the European Union

Table 10 Performance Criteria for the Element CYBER.U3.E3

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U3.E3.PC1	The trainee is able to perform a cybersecure critical software functions analysis.
CYBER.U3.E3.PC2	The trainee is able to perform a cybersecure critical software data analysis.
CYBER.U3.E3.PC3	The trainee is able to write cybersecurity-related software requirements.
CYBER.U3.E3.PC4	The trainee is able to link the cybersecure critical software functions and data with cybersecurity relevant software requirements (SW requirements to monitor and avoid harm).
CYBER.U3.E3.PC5	The trainee is able to integrate cybersecurity views into the software architectural design.
CYBER.U3.E3.PC6	The trainee knows to select cybersecurity design patterns on the software level and how to apply them.

3.5.4. Unit CYBER.U3 – Element 4: Software Detailed Design and Cybersecurity

Acronym: CYBER.U3.E4

Element Title: Software Detailed Design and Cybersecurity

Element Note:

This element considers at the software detailed design level related cybersecurity methods.

- The trainee knows cybersecurity related detailed SW design principles
- The trainee knows cybersecurity critical code inspections and reviews

With the support of the Erasmus+ Programme of the European Union

- The trainee is able to select development tools and SW development environments, e.g. secure session key generation by random generator, encryption of signals, secure key store etc.

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 11 Performance Criteria for the Element CYBER.U3.E4

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U3.E4.PC1	The trainee knows the common weakness enumeration of the community-developed list of software weakness types.
CYBER.U3.E4.PC2	The trainee knows guidelines, knowledge bases, recommended tools, and methods supporting cybersecure design approaches.
CYBER.U3.E4.PC3	The trainee knows how to perform a cybersecure related code review and the review checklist (applying available knowledge data sources).
CYBER.U3.E4.PC4	The trainee knows and applies the MISRA extension rules for cybersecurity relevant code development.
CYBER.U3.E4.PC5	The trainee knows the principles of preventive and defensive programming.

3.5.5. Unit CYBER.U3 – Element 5: Cybersecure hardware and firmware design

Acronym: CYBER.U3.E5

Element Title: Hardware Design and Firmware Design

Element Note:

This element looks at the hardware detailed design level related cybersecurity methods.

With the support of the Erasmus+ Programme of the European Union

- The trainee knows how to integrate HSM (Hardware Security Module) on ECU
- The trainee understands the architecture of a HSM
- The trainee knows the operating system on the controller and HSM firmware interfaces
- The trainee knows how to configure secure com stack
- The trainee knows the list of main diagnostic security services to be provided

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 12 Performance Criteria for the Element CYBER.U3.E5

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U3.E5.PC1	The trainee knows how to use the HSM (Hardware Security Module) of the ECU.
CYBER.U3.E5.PC2	The trainee knows the typical architecture of a HSM.
CYBER.U3.E5.PC3	The trainee knows how the interfaces between the main controller and the HSM controller/firmware works.
CYBER.U3.E5.PC4	The trainee knows the secure OS Lib's main services in a secure operating environment (list of functions and services).

With the support of the Erasmus+ Programme of the European Union

3.6. Unit CYBER.U4 Testing aspects of cybersecurity

Acronym: CYBER.U4

Title: Testing aspects of cybersecurity

Description:

The Unit addresses the different test levels and test methods to be applied in cybersecurity development.

- The trainee knows of testing aspects of cybersecurity
- The trainee knows of different testing types and methods for cybersecurity
- The trainee knows test methods proposed by automotive norms

3.6.1. Unit CYBER.U4 – Element 1: Cybersecurity verification at SW level

Acronym: CYBER.U4.E1

Element Title: Cybersecurity verification at SW level

Element Note:

This element includes aspects of what is required in SW testing to cover the cybersecure relevant SW requirements.

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 13 Performance Criteria for the Element CYBER.U4.E1

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U4.E1.PC1	General: The trainee knows about the test methods proposed by the automotive norms and guidebooks (e.g. ISO/SAE 21434, SAE J3061, UNECE regulations, and other available knowledge sources such as the OWASP project).
CYBER.U4.E1.PC2	SW unit test related: The trainee knows about the MISRA check using the extension for cybersecurity.

With the support of the Erasmus+ Programme of the European Union

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U4.E1.PC3	SW unit verification related: The trainee knows about cybersecure relevant criteria to be applied informal code reviews (using the available libraries, knowledge databases like OWASP and guidelines).
CYBER.U4.E1.PC4	SW integration test-related: The trainee knows the cybersecure critical software data and develops test cases to attack the data and assure that the preventive mechanisms are working.
CYBER.U4.E1.PC5	SW integration test-related: The trainee knows about the configuration of a secure communication stack and checks the configuration.
CYBER.U4.E1.PC6	SW integration test-related: The trainee knows the criticality of the communication between the main controller OS and the firmware in the HSM and extra test cases to verify their sufficient integration.
CYBER.U4.E1.PC7	SW function test-related: The trainee knows the significance cybersecure critical software functions and develops test cases to attack the software function (e.g. calling it with an unauthorised session ID) and assure that the preventive mechanisms are working.
CYBER.U4.E1.PC8	SW function test-related: The trainee knows how to test different diagnostic services requested by the cybersecurity protocols and their impact on cybersecurity.
CYBER.U4.E1.PC9	SW penetration test-related (integration and functional test in SW): The trainee knows the concept of penetration testing and how to involve such external penetration testing (hacker) teams.

With the support of the Erasmus+ Programme of the European Union

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U4.E1.PC10	Traceability: The trainee knows how to link cybersecurity critical SW requirements to test cases and test results.

3.6.2. Unit CYBER.U4 – Element 2: Cybersecurity verification at HW level

Acronym: CYBER.U4.E2

Element Title: Cybersecurity verification at HW level

Element Note:

This element includes aspects of what is required in HW testing to cover the cybersecure relevant HW requirements.

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 14 Performance Criteria for the Element CYBER.U4.E2

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U4.E2.PC1	The trainee knows about automotive certified HSM architectures and can verify that the HSM hardware module is qualified for the Automotive project.
CYBER.U4.E2.PC2	The trainee knows that customer possibly provide SSL/SSA libraries that need to be integrated with the HSM software and that customer-specific test environments/tools need to be used.
CYBER.U4.E2.PC3	The trainee knows that HW security modules have a specification sheet with services that need to be activated

With the support of the Erasmus+ Programme of the European Union

Performance Criterion	Evidence Check: The trainee can demonstrate
	and that the activation of these services needs to be reviewed.
CYBER.U4.E2.PC4	The trainee knows that the exploit options of the selected HSM module need to have protection by the HSM supplier and thus will have review meetings with the supplier (or request data) about the hardware tests done at the HSM supplier site.

3.6.3. Unit CYBER.U4 – Element 3: Cybersecurity verification at the system level

Acronym: CYBER.U4.E3

Element Title: Cybersecurity verification at the system level

Element Note:

This element includes aspects of what is required in system testing to cover the cybersecure relevant system requirements.

Performance Criteria:

The trainee must be able to show evidence of competencies for the following performance criteria (PC):

Table 15 Performance Criteria for the Element CYBER.U4.E3

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U4.E3.PC1	General: The trainee knows about the test methods proposed by the norms and guidebooks (e.g. ISO/SAE 21434, SAE J3061, and the OWASP project), which can be applied at the system/vehicle level

With the support of the Erasmus+ Programme of the European Union

Performance Criterion	Evidence Check: The trainee can demonstrate
CYBER.U4.E3.PC2	System integration: The trainee knows what security services at vehicle level in the production, at end-of-line, or at vehicle set up are required for integration.
CYBER.U4.E3.PC3	System test: The trainee knows which security services at the vehicle level in operation need to be tested and which security data must be reported/observed to ensure a secure vehicle operation.
CYBER.U4.E3.PC4	System test: The trainee knows what security services at vehicle level in the vehicle testing (or test bench testing) need to be tested.
CYBER.U4.E3.PC5	Penetration testing: The trainee knows how to interact with external penetration testing teams to undertake penetration testing on vehicle level.

3.7. Mapping to ESCO and other frameworks

Described skills set and developed roles of cybersecurity engineer and manager will be throughout the project mapped to frameworks such as ESCO and DRIVES framework and others if applicable. In case of changes during the project duration minor adjustments or updates of the framework to which the roles are mapped might be possible. Further mapping or recognition of the developed training will be done in the future development of the project.

3.7.1. ESCO

ESCO classification or taxonomy is a collection of skills, occupations and qualification concepts in multiple languages. The main vision is to enhance the functional and integrated labour market and support bridging communication gaps between the industry and education, and thus develop a shared understanding of occupations, skills, competencies, and qualifications.

With the support of the Erasmus+ Programme of the European Union

CYBERENG skills for both roles were compared to the existing concepts in the ESCO database. Although multiple skills related to information security, general cybersecurity, data protection, or ICT related security and standards is available, there are no specifics for cybersecurity in the automotive field.

The same applies when it comes to occupations. When comparing CYBERENG developed skills set for cybersecurity managers and engineers, only general ICT related occupations are present, such as ICT security consultant, administrator, manager, technician, resilience manager or disaster recovery analyst.

Project CYBERENG will propose possible update of ESCO by providing the concepts based on the findings of the CYBERENG project. Initial mapping to ESCO with new concepts proposed is seen in Annex V. ESCO Mapping.

3.7.2. DRIVES Framework

DRIVES framework is a reference and recognition framework with a focus on the EU automotive mobility ecosystem. The framework and its online platform establishes and maintains a database of training courses advertised by training providers. The DRIVES Framework and its structure maps skills/competence and knowledge concepts onto training and job roles. Both, skills/competences and knowledge can be matched against each other and the related maturity levels or EQF can be specified. The DRIVES Framework offers micro-credentials in the form of digital badges – issued for skills/competence and knowledge on different levels.

Project CYBERENG will provide advanced skillsets as reference job roles in the DRIVES Framework and the link to the developed training. By this, the recognition of the work done in the CYBERENG project will be supported.

With the support of the Erasmus+ Programme of the European Union

Annexes

The annexe provides an overview of used skills set, coverage of Qualification Schemas, Legal background for Certification, and mappings to other frameworks.

With the support of the Erasmus+ Programme of the European Union

4. Annex I. - ECQA Description

4.1. ECQA – European Certification and Qualification Association

ECQA standards are used to describe the skills sets delivered within the project. ECQA is the selected certification body for the project outcome.

Europe Wide Certification

The ECQA is the result of a number of EU supported initiatives in the last ten years. In the European Union Life Long Learning Programme, different educational developments decided to follow a collaborative process for the certification of persons in the industry.

Through the ECQA, it becomes possible that one attends courses for a specific profession in, e.g. Spain and perform a Europe wide agreed test at the end of the course.

Access to a Vast Pool of Knowledge

ECQA started as a European Commission funded endeavour and continued since 2012 autonomously to supports more than 45 professions in Europe. The pool of knowledge is continuously growing and ECQA offers certification for professions like IT Security Manager, Innovation Manager, EU project manager, E-security Manager, E-Business Manager, E-Strategy Manager, SW Architect, SW Project Manager, IT Consultant for COTS selection, Internal Financial Control Assessor (COSO/COBIT based), Interpersonal Skills, Scope Manager (Estimation Processes), Configuration Manager, Safety Manager, and so forth.

The ECQA guide can be downloaded at www.ecqa.org -> Guidelines.

Defined procedures are applied for:

- Self-assessment and learning http://www.ecqa.org/fileadmin/documents/Self_Assessment/eucert-users-self-assessment-learning-guide-v5-doc.pdf
- Exam performance http://www.ecqa.org/fileadmin/documents/ECQA_Exam_Guide_Participant_v2.pdf

4.1.1. ECQA Skills Definition Model

With the support of the Erasmus+ Programme of the European Union

The ECQA skills definition model, used for Job Role definition, is described in section 2 of this document.

4.1.2. ECQA Skill Set Strategy

The goal of European endeavours, like DRIVES project, is to have a skill set like a card with a chip that stores once skill profile to fulfil specific professions, job roles, and tasks in the future. It's working as an ID card. This future scenario requires -

- A standard way to describe a skill set for a profession, job, or specific task.
- A standard procedure to assess the skill and to calculate and display skill profiles.

Such a common set of skill sets in Europe is needed due to the free mobility of workers. European countries such as the UK, the Netherlands, and France already have well established open universities which support APL (Accreditation of Prior Learning). In APL, trainees'/students' skills are assessed, already gained skills are recognised, and a learning plan is established only for the skill gaps. The skill assessment is based on defined skill units and a skill profile that displays how much of the Unit is covered.

In a previous project, CREDIT (Accreditation of Skills via the Internet) [1], some of the project partners were involved, such an Internet-based skills assessment system was built. Therefore, another possible future scenario is that representative educational bodies per country in Europe maintain skill profiles in databases that can be accessed via defined ID codes for people.

4.1.3. ECQA Skills Assessment Model

Step 1 – Browse a Skills Set: One select a set of skills or competencies required by ones profession or job using national or company standards. Further, one browse different skills cards and select a job role one would like to achieve.

Step 2 – Register for Self Assessment with a Service Unit: This can be a service unit inside the own company (e.g. a personnel development department) or a skills card and assessment provider outside your company that offers skills assessment services.

Step 3 – Receive an Account for Self-Assessment and Evidence Collection: One automatically received an account to log in to the working space with the registration.

With the support of the Erasmus+ Programme of the European Union

There one can go through the steps of online self-assessment and collect evidence to prove the capabilities of specific performance criteria.

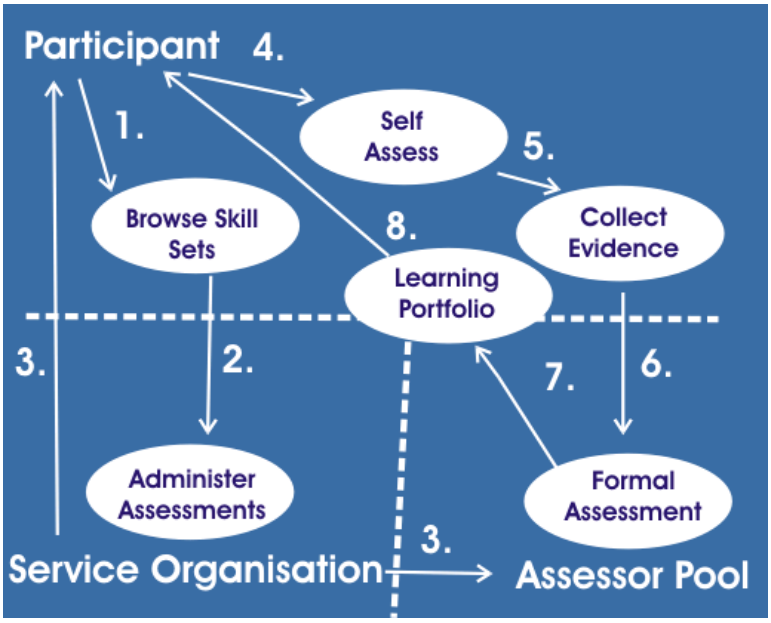

Figure 3 Basic steps of the skills assessment model

Step 4 – Perform Self Assessment: Log into the system, browse through the skills required and self assess performance criteria, whole elements or whole units with a standard evaluation scale of non-applicable, not adequate, partially adequate, largely adequate, and fully adequate. A skills gaps profile can be generated and printed, illustrating which areas the self-assessment shows improvement potentials.

Testing of Skills (Addition to Step 4) – The system provides a multiple-choice test for each performance criteria to check that the required capabilities are gained.

Step 5 – Collect pieces of evidence: Before entering any formal assessment, one needs to prove its skills by evidence. Pieces of evidence can be any electronic files (sample documents, sample graphics, results of some analysis, etc.) or any references with details (e.g. a certificate received from a certain institution). Pieces of evidence can then be linked to specific performance criteria or whole elements of skills units.

Testing of Skills (Addition to Step 5) – In traditional learning schemes, people have always needed to go to a learning institution (university, accreditation body, professional body, etc.) to take exams and receive a certificate if they pass. However, this traditional approach is insufficient when measuring experience and (soft) skills learned on the job and fails to recognise skills gathered on the job. The APL (Accreditation of Prior Learning) approach, by contrast, collects so-called evidences. Evidences can be certificates

With the support of the Erasmus+ Programme of the European Union

obtained in the traditional way, references from previous employers, materials from earlier projects in which the person took ownership of results (e.g. a test plan) to prove their capability, and any kind of proof of competence gathered on the job. The assessors will then evaluate the evidences provided and not only rely on certificates and exams.

Step 6 – Receive Formal Assessment: Formal assessors are assigned by the service unit to the skills assessment. Once formal assessors log into the system, they automatically see all assigned assessments. They select the corresponding one and can see the uploaded evidences. They then formally assess the pieces of evidence and assess the formal fulfilment of performance criteria, whole elements or whole units with a standard evaluation scale of non-applicable, not adequate, partially adequate, largely adequate, and fully adequate. In case of missing competencies, they enter improvement recommendations, a well as learning options.

Step 7 – Receive Advice on Learning / Improvement Options: After the formal assessment, the participants log into the system and can see the formal assessment results from the assessors, can print skills gaps profiles based on the assessor results, and can receive and print the improvement recommendations and learning options. If required, the generation of learning options can also be automated through the system (independent from assessor advice).

4.1.4. ECQA Certificate Types

In the standard test and examination procedures for levels of certificates are offered:

- Course Attendance Certificate
  - Received after course attendance
  - Modular per Element
- Course / Test Certificate
  - Test in a test system (European pool of test questions)
  - 67% satisfaction per element
- Summary Certificate
  - Overview of covered elements where the trainee passed the test, all elements shall be covered
  - Generation of certificate
- Professional Certificate
  - Uploading applied experiences for review by assessors

With the support of the Erasmus+ Programme of the European Union

- Rating by assessors
- Observation of 2 years

The certificates show credited elements in comparison to all required.

With the support of the Erasmus+ Programme of the European Union

5. Annex II. - ECQA Coverage of Qualification Schemas

5.1. Mapping based on NVQ Qualification Levels

Qualification/training levels: Five levels of qualification/training are defined by European legislation and this structure can be used for comparability of vocational qualifications from the different European countries.

- Level 1: semi-skilled assistant performing simple work
- Level 2: basic employee performing complex routines and standard procedures
- Level 3: skilled professional with responsibility for others and performing independent implementation of procedures
- Level 4: middle management & specialist performing tactical and strategic thinking
- Level 5: professional / university level

In most cases, the same job role can be offered on different levels. e.g. IT Security Manager Basic Level (NVQ level 2), IT Security Manager Advanced level (NVQ Level 3), and IT Security Manager Expert Level (NVQ Levels 4 and 5).

With the support of the Erasmus+ Programme of the European Union

5.2. Mapping based on European Qualification Framework (EQF) Learning Levels

- Six level taxonomy:

  Level 0: I never heard of it

  1. Knowledge (I can define it):
  2. Comprehension (I can explain how it works)
  3. Application (I have limited experience using it in simple situations)
  4. Analysis (I have extensive experience using it in complex situations)
  5. Synthesis (I can adapt it to other uses)
  6. Evaluation (I am recognized as an expert by my peers)

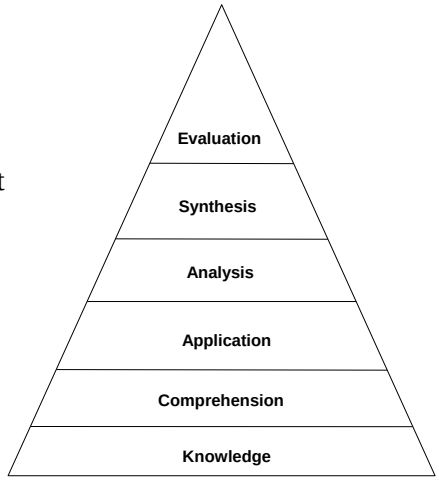

Figure 4 BLOOMS Learning Levels

Table 16 EQF Learning Levels

Level	Knowledge	Example
Level 1	Basic general knowledge	
Level 2	Basic factual knowledge of a field of work or study	
Level 3	Knowledge of facts, principles, processes and general concepts in a field of work or study	Six Sigma Yellow Belt
Level 4	Factual and theoretical knowledge in broad contexts within a field of work or study	
Level 5	Comprehensive, specialised, factual and theoretical knowledge within a field of work or study and an awareness of the boundaries of that knowledge	
Level 6	Advanced knowledge of a field of work or study, involving a critical understanding of theories and principles	Six Sigma Green Belt

With the support of the Erasmus+ Programme of the European Union

Level	Knowledge	Example
Level 7	Highly specialised knowledge, some of which is at the forefront of knowledge in a field of work or study, as the basis for original thinking and/or research Critical awareness of knowledge issues in a field and at the interface between different fields	Six Sigma Black Belt
Level 8	Knowledge at the most advanced frontier of a field of work or study and the interface between fields	Six Sigma Master Black Belt

5.3. Mapping based on ECTS and ECVET Schema

In addition, ECQA has established a procedure to map ECQA skills sets onto the ECTS (European Credit Transfer System) and the ECVET framework in the European Union.

A job role is assigned ECTS and ECVET points using a defined framework.

5.3.1. ECTS Mapping

Each element of the skills set is assigned hours of lecturing and exercises. These hours determine the ECTS points, which are then agreed among a cluster of different universities in Europe.

With the support of the Erasmus+ Programme of the European Union

Level	Knowledge	AQUA	ECTS	Safety Manager	ECTS
Level 1	Basic general knowledge	-		-	
Level 2	Basic factual knowledge of a field of work or study	-		-	
Level 3	Knowledge of facts, principles, processes and general concepts, in a field of work or study				
Level 4	Factual and theoretical knowledge in broad contexts within a field of work or study				
Level 5	Comprehensive, specialized, factual and theoretical knowledge within a field of work or study and an awareness of the boundaries of that knowledge				
Level 6	Advanced knowledge of a field of work or study, involving a critical understanding of theories and principles	AQUA - Automotive Quality Integrated Skills - presentations / theory	3	AQUA - Automotive Quality Integrated Skills - presentations / theory	3
Level 7	- Highly specialized knowledge, some of which is at the forefront of knowledge in a field of work or study, as the basis for original thinking and/or research - Critical awareness of knowledge issues in a field and at the interface between different fields	AQUA - Automotive Quality Integrated Skills - with exercises to apply on nan example (e.g. ESCL)	4	AQUA - Automotive Quality Integrated Skills - with exercises to apply on nan example (e.g. ESCL)	4
Level 8	Knowledge at the most advanced frontier of a field of work or study and at the interface between fields	AQUA - Automotive Quality Integrated Skills - implementation in a research at PhD level / with link to a real project	5	AQUA - Automotive Quality Integrated Skills - implementation in a research at PhD level / with link to a real project	5

Figure 5 EQF Example Automotive Quality Engineer and Safety Manager

The two job roles illustrated in Figure 6 have been assigned to ECTS and are taught using the same skills set at industry and universities. Such a mapping is also intended for the trainings established in CYBERENG project.

5.3.2. ECVET Mapping

Also, ECQA provides a framework to assign ECVET points onto elements of the skills set. The ECQA guidance recommends offering the ECQA course (which is delivered as a lecture at university) as a short course (2 weeks with exercises) in the industry to retrain for a job role. The recommended size is 30 ECVET points in total. The lecturing time and exercise per element determine how many ECVET points are assigned to an element of the skills set.

With the support of the Erasmus+ Programme of the European Union

Automotive Quality Engineer			
			ECVET L7&8
U1	4	U1.E1: Introduction	2
		U1.E2: Organisational Readiness	2
U2	32	U2.E1 Life Cycle	8
		U2.E2 Requirements	8
		U2.E3 Design	8
		U2.E4 Test and Integration	8
U3	12	U3.E1: Capability	2
		U3.E2: Hazard and Risk Management	8
		U3.E3 Assessment and Audit	2
U4	12	U4.E1: Measurement	6
		U4.E2: Reliability	6
		ECVET Points Total	60

Figure 6 ECVET Mapping example - Automotive Quality Engineer

Functional Safety Manager / Engineer			
			ECVET L7&8
U1	2	U1.E1 International Standards	1
		U1.E2 Product Life Cycle	1
		U1.E3 Terminology	
U2	4	Safety management on organisational	1
		Safety Case Definition	1
		Overview of Required Engineering an	1
		Establish and Maintain Safety Plannin	1
U3	16	System Hazard Analysis and Safety Co	4
		Integrating Safety in System Design &	4
		Integrating Safety in Hardware Design	4
		Integrating Safety in Software Design	4
U4	4	Integration of Reliability in Design to I	2
		Safety in the Production,Operation an	2
U5	4	Legal aspects and Liabilities	2
		Regulatory & Qualification Requireme	2
		ECVET Points Total	30

Figure 7 ECVET Mapping example – Functional Safety Manager / Engineer

With the support of the Erasmus+ Programme of the European Union

6. Annex III.- ECQA Legal Background For Certification

6.1. ISO/IEC 17024 standard for personnel certification programmes

The ISO/IEC 17024 standard describes standard processes for the examination and certification of people. Some of the basic principles described include:

- Standard exam procedure
- Standard certification procedure
- Identification of persons receiving the certificate
- Independence of examiner and trainer
- Certification system that allows logging the exam to keep a record/proof that the examinee passed the exam
- Mapping of processes towards ISO 17024

6.2. ECQA and ISO/IEC 17024 standard

- ECQA defined standard exam processes
- ECQA defined standard certification processes
- ECQA developed an exam system that generates random exams and corrects exams.
- ECQA developed a certification database to identify persons and map them to exam results
- ECQA established a mapping onto the ISO 17024 norm and published that in the form of a self-declaration.

6.3. LIASION with National Universities

ECQA established cooperation with national universities that teach job roles with ECTS. The same job roles are offered with ECVET on the market by training bodies.

With the support of the Erasmus+ Programme of the European Union

7. Annex IV. - Further reading regarding standards and regulations

While ISO/SAE 21434 "road vehicles – cybersecurity engineering" is the predominant standard regarding automotive cybersecurity, there are further standards that refer to specific topics (privacy, certificate handling) or bridge to additional disciplines (software update, V2X). This list here is not intended as a complete and concluding list but as an option for further reading and information.

Standards and Regulations for Mobility

Operational Environment		On-Road		Off-Road				Aerospace	Infrastructure
				Industrial automation, machinery	Construction	Mining	Agriculture		
Taxonomy Standards		SAE J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles							
		ISO/TR 21718:2019 Spatio-temporal data dictionary for cooperative ITS and automated driving systems 2.0							
		J3216_202005 Taxonomy and Definitions for Terms Related to Cooperative Driving Automation for On-Road Motor Vehicles							
		PAS 1883 Operational design domain (ODD) taxonomy for an automated driving system (ADS). Specification							
Regulations	Global	1949 UN Convention on road traffic in Geneva							
		1968 UN Convention on road traffic in Vienna							
	US		US DOT Automated vehicles comprehensive plan (non-binding)						
		California	SB-1298 Vehicles: autonomous vehicles: safety and performance requirements						
			AD-2866 Autonomous vehicles						
		Other States	Autonomous vehicles state bill tracking database						
	Europe / ECE	UN/ECE Resolution on the deployment of highly and fully automated vehicles in road traffic		EU Machine directive 2006/42/EC				EU Unmanned aircraft	

With the support of the Erasmus+ Programme of the European Union

								systems 2019/945	
		UN/ECE 79 Uniform provisions concerning the approval of vehicles with regard to steering equipment							
		UN/ECE provisions concerning Lane Keeping Systems							
Standards	Functional Safety	E/E system, HW/SW components	ISO 26262 - Functional Safety	IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems				DO-178C Software considerations in airborne systems and equipment certification	
				ISO 13489 Safety of machinery					
		Functional performance	ISO PAS 21448 Safety of the intended functionality						
			ISO DIS 21448 Safety of the intended functionality						
		Verification & Validation	ISO/TR 4804 Safety and cybersecurity for automated driving systems - Design, verification and validation						
			ISO/AWI TS 5083 Safety for automated driving systems – Design, verification and validation						
			BSI PAS 1880 Guidelines for developing and assessing control systems for automated vehicles						
		Safety case framework	ANSI/UL 4600 Standard for safety for the evaluation of autonomous products						
	Testing	PAS 1881:2020 Assuring safety for autonomous vehicle trials and testing							
		SAE J3018 Guidelines for safe on-road testing of SAE level 3,4 and 5 prototype automated driving systems							
		CEN ISO/TS 21189 Cooperative ITS – Test requirements and protocol implementation conformance statement (PICS)							
		ISO 19206 Test devices for target vehicles, vulnerable road users and other objects for assessment of active safety functions							
	Interfaces	ISO 23150 Data communication between sensors and data fusion unit for automated driving functions							
	Performance requirements and testing procedures	Positioning	ETSI EN 302 895 V1.1.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM)						
		Lane-keeping	ISO 17361 Lane departure warning systems						
			ISO 11270 Lane-keeping assistance systems						
			ISO 19638 Road boundary departure prevention systems						
			ISO 21202 Partially automated lane change systems						

With the support of the Erasmus+ Programme of the European Union

			ISO 21717 Partially Automated In-Lane Driving Systems (PADS) – Performance requirements and test procedures						
			SAE J3045 Truck & bus lane departure warning systems test procedure						
		Cruise Control	ISO 15622 Adaptive cruise control systems						
			ISO 20035 Cooperative adaptive cruise control systems						
		Driving	ISO 23792 Motorway chauffeur systems						
			ISO 22737 Low-speed automated driving systems for predefined routes						
		Parking	ISO 20900 Parking Partially automated parking systems						
			ISO 23374 Automated valet parking systems						
			ISO 16787 Assisted Parking System (APS) – Performance requirements and test procedure						
		Safety	ISO 19237 Pedestrian detection and collision mitigation systems						
			ISO 22078 Bicyclist detection and collision mitigation systems						
			ISO 23375 Collision evasive lateral manoeuvre systems						
			ISO 20901 Emergency electronic brake light systems						
			ISO 19206 Road vehicles – Test devices for target vehicles, vulnerable road users and other objects for assessment of active safety functions						
			ETSI TS 103 300-2 V2.2.1 Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 2: Functional Architecture and Requirements definition; Release 2						
			ETSI TS 103 300-3 V2.1.2 Intelligent Transport Systems (ITS); Vulnerable Road Users (VRU) awareness; Part 3: Specification of VRU awareness basic service; Release 2						
			IETSI TS 101 539-2 V1.1.1 Intelligent Transport Systems (ITS); V2X Applications; Part 2: Intersection Collision Risk Warning (ICRW) application requirements specification						
	Security	ISO 21434 Cybersecurity of road vehicles						National Aerospace Standard 9933	ISO 27001 Information security management systems

With the support of the Erasmus+ Programme of the European Union

		ISO PAS 5112 Guidelines for auditing cybersecurity engineering						ISO 27002 Code of practice for information security controls
		BSI PAS 1885 Fundamental principles of automotive cybersecurity						BSI-Standard 200-1
		BSI PAS 11281 Connected automotive ecosystems. Impact of security on safety. Code of practice.						BSI-Standard 200-2
		SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems						ISO/IEC 15408 / Common Criteria for Information Technology Security Evaluation
		European Commission: Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)						
		European Commission: Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)						
		ETSI TR 103 460 Intelligent Transport Systems (ITS); Security; Pre-standardization study on Misbehaviour Detection; Release 2						
		ETSI TS 102 731 V1.1.1 Intelligent Transport Systems (ITS); Security; Security Services and Architecture						
		ETSI TS 102 940 V1.3.1 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management						
		ETSI TS 102 941 V1.4.1 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management						
		ETSI TS 102 942 V1.1.1 Intelligent Transport Systems (ITS); Security; Access Control						
		ETSI TS 102 943 V1.1.1 Intelligent Transport Systems (ITS); Security; Confidentiality services						
		ETSI TS 103 097 V1.4.1 Intelligent Transport Systems (ITS); Security; Security header and certificate formats						
		SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organisations						
	Software Updates	ISO 24089 Software update engineering						
	Connectivity	CEN ISO/TS 19468 Intelligent transport systems – Data interfaces between centres for transport information and control system						NEMA TS 10 Connected vehicle infrastructure-roadside equipment

With the support of the Erasmus+ Programme of the European Union

		IEEE 1609.12 IEEE standard for wireless access in vehicular environments (WAVE) – Identifiers						• European Commission: Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)
		CEN ISO/TS 19091 Intelligent transport systems – Cooperative ITS – Using V2I and I2V communications for application related to signalised intersections						
		IEEE 1609.2b IEEE standard for wireless access to the vehicular environment						
		CEN/TR 17297-1 Intelligent transport systems – Location referencing harmonisation for urban ITS – Part 1: State of the art and guidelines						
		ISO 20078 Extended vehicle (ExVe) web services						
		ISO 20080 Information for remote diagnostic support						
		SAE J2945/2 DSRC performance requirements for V2V safety awareness						
		ETSI TS 138 522 5G; NR; User equipment conformance specification						
		ISO 20077 Extended vehicle (ExVe) methodology						
		ETSI GR IP6 030 IPv6-based Vehicular Networking (V2X)						
		ETSI TR 103 496 Intelligent Transport Systems (ITS); Cooperative ITS (C-ITS) support for transport pollution management applications; Use cases and standardisation study						
		ETSI EN 302 890-1 V1.2.1 Intelligent Transport Systems (ITS); Facilities layer function; Part 1: Services Announcement (SA) specification						
		ETSI EN 302 890-2 V2.1.1 Intelligent Transport Systems (ITS); Facilities Layer function; Part 2: Position and Time management (PoTi); Release 2						
		ETSI TS 102 637-1 V1.1.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 1: Functional Requirements						
		ETSI EN 302 637-2 V1.4.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service						

With the support of the Erasmus+ Programme of the European Union

		ETSI EN 302 637-3 V1.3.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service						
		ETSI TS 103 301 V2.1.1 Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Facilities layer protocols and communication requirements for infrastructure services; Release 2						
		ETSI EN 302 665 V1.1.1 Intelligent Transport Systems (ITS); Communications Architecture						
		ETSI EN 302 636-1 V1.2.1 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 1: Requirements						
		ETSI EN 302 636-3 V1.2.1 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network Architecture						
		ETSI EN 302 636-5-1 V2.2.1 Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol						
		ISO 23132 Extended Vehicle (ExVe) time-critical applications						
	Human Factors	ISO/TR 21959 Human performance and state in the context of automated driving						
		ISO/TR 23049 Ergonomic aspects of external visual communication from automated vehicles to other road users						

With the support of the Erasmus+ Programme of the European Union

8. Annex V. ESCO Mapping

8.1. Cybersecurity Manager Mapping to established ESCO Entries

This annex contains the mapping to ESCO – information about CYBERENG proposed occupation concepts (Cybersecutiry Manager and Engineer) in the table 17 and 19; optional and essential skills/knowledge that are composing the profiles in tables 18 and 20 (new proposed skill/knowledge concepts are based on the pool in 8.3, additionally existing concepts in the ESCO are mapped as well – links are provided within the cell with blue font)

Table 17 ESCO Mapping – Cybersecurity Manager

Concept Name:	Automotive Cybersecurity Manager
Description of the Occupation:	Automotive Cybersecurity Manager focuses on the process level, standards, regulatory compliance and on the management of automotive cybersecurity in distributed processes.
Alternative Lables:	automotive cybersecurity director; automotive cybersecurity executive
Scope Note:	targeting more specific areas within automotive cybersecurity, existing ICT security roles not applicable due to their generic context
Regulated Profession:	no
ISCO Hierarchy:	2529 Database and network professionals not elsewhere classified

With the support of the Erasmus+ Programme of the European Union

Table 18 Skills Mapping to ESCO – Cybersecurity Manager

Essential skills	Essential knowledge	Optional skills	Optional knowledge
perform risk analysis	cybersecurity roles	manage system security	cyber attack counter-measures
respect data protection principles	organisational structure	satisfy technical requirements	automotive cyber attacks
establish and maintain cybersecurity plans in automotive	data protection	conduct ICT code review	cybersecurity design patterns
analyse cybersecurity threats and vulnerabilities throughout the automotive life cycle	hacker paradigm in automotive domain	access known automotive cyber threat list	common software wakness types
solve cybersecurity vulnerabilities throughout the automotive life cycle	EU cybersecurity regulations	perform cybersecurity asset analysis	guidelines, knowledge bases, tools and methods supporting cybersecure design approach
manage audit and product assessment	cybersecurity project life cycle	depict system architecture	cybersecurity related code review and review checklist
handle incidents	automotive cybersecurity standards, norms and guidelines	outline potential cybersecurity attack targets	MISRA extension rules for cybersecurity code development
manage emergency procedures	ingredient threats	perform and document TARA (threat and risk analysis)	principles of preventive and defensive programming
manage and establish urgent response procedures	supplier management	derive and document cybersecurity goals	HSM (Hardware Security Module) integration into ECU (Electronic Control Unit)

With the support of the Erasmus+ Programme of the European Union

form an urgent response team		perform cyber attack tree analysis	HSM architecture
arrange audit		perform a vulnerability analysis	main controller and HSM controller interface
negotiate terms with supplier		integrate cybersecurity defence mechanism	secure OS Lib's main services and functions
negotiate supplier arrangements		integrate cybersecurity views into system architecture design	ICT security legislation
maintain relationship with supplier		write and trace cybersecurity requirements	ICT security standards
		perform a cybersecure critical software functions analysis	automotive test methods
		perform a cybersecure critical software data analysis	levels of software testing
		write cybersecurity related software requirements	penetration testing tool
		link cybersecurity requirements to critical sw functions and data	requirement traceability
		integrate cybersecurity views into the software	certified HSM architectures verification and analysis
		adjust priorities	
		develop information security strategy	
		integrate system components	
		manage system testing	

* concepts with links (blue font color) are already existing within the ESCO

With the support of the Erasmus+ Programme of the European Union

8.2. Cybersecurity Engineer Mapping to established ESCO Entries

Table 19 ESCO Mapping – Cybersecurity Engineer

Concept Name:	Automotive Cybersecurity Engineer
Description of the Occupation:	Automotive Cybersecurity Engineer possesses the basic skills for active technical work regarding the achievement of automotive cybersecurity for a product throughout the complete lifecycle
Alternative Lables:	-
Scope Note:	targeting more specific areas within automotive cybersecurity, existing ICT security roles not applicable due to their generic context
Regulated Profession:	no
ISCO Hierarchy:	2529 Database and network professionals not elsewhere classified

Table 20 Skills Mapping to ESCO – Cybersecurity Engineer

Essential skills	Essential knowledge	Optional skills	Optional knowledge
access known automotive cyber threat list	automotive cyber attacks	perform risk analysis	cyber attack counter-measures
perform cybersecurity asset analysis	cybersecurity design patterns	manage system security	
depict system architecture	common software wakness types	satisfy technical requirements	
outline potential cybersecurity attack targets	guidelines, knowledge bases, tools and methods supporting cybersecure design approach	conduct ICT code review	

With the support of the Erasmus+ Programme of the European Union

perform and document TARA (threat and risk analysis)	cybersecurity related code review and review checklist		
derive and document cybersecurity goals	MISRA extension rules for cybersecurity code development		
perform cyber attack tree analysis	principles of preventive and defensive programming		
perform a vulnerability analysis	HSM (Hardware Security Module) integration into ECU (Electronic Control Unit)		
integrate cybersecurity defence mechanism	HSM architecture		
integrate cybersecurity views into system architecture design	main controller and HSM controller interface		
write and trace cybersecurity requirements	secure OS Lib's main services and functions		
perform a cybersecure critical software functions analysis			
perform a cybersecure critical software data analysis			
write cybersecurity related software requirements			
link cybersecurity requirements to critical sw functions and data			
integrate cybersecurity views into the software			

* concepts with links (blue font color) are already existing within the ESCO

With the support of the Erasmus+ Programme of the European Union

8.3. New Concept Suggestions for ECSO Entries

Table 20 New Proposed Concepts – Overall

Concept name
access known automotive cyber threat list
perform cybersecurity asset analysis
depict system architecture
outline potential cybersecurity attack targets
perform and document TARA (threat and risk analysis)
derive and document cybersecurity goals
perform cyber attack tree analysis
perform a vulnerability analysis
integrate cybersecurity defence mechanism
integrate cybersecurity views into system architecture design
write and trace cybersecurity requirements
perform a cybersecure critical software functions analysis
perform a cybersecure critical software data analysis
write cybersecurity related software requirements
link cybersecurity requirements to critical sw functions and data
integrate cybersecurity views into the software
automotive cyber attacks
cybersecurity design patterns
common software wakness types
guidelines, knowledge bases, tools and methods supporting cybersecure design approach
cybersecurity related code review and review checklist
MISRA extension rules for cybersecurity code development
principles of preventive and defensive programming
HSM (Hardware Security Module) integration into ECU (Electronic Control Unit)
HSM architecture
main controller and HSM controller interface
secure OS Lib's main services and functions
establish and maintain cybersecurity plans in automotive
analyse cybersecurity threats and vulnerabilities throughout the automotive life cycle
solve cybersecurity vulnerabilities throughout the automotive life cycle
manage audit and product assessment
manage and establish urgent response procedures
form an urgent response team
hacker paradigm in automotive domain
EU cybersecurity regulations
cybersecurity project life cycle
automotive cybersecurity standards, norms and guidelines
automotive test methods
requirement traceability
certified HSM architectures verification and analysis

With the support of the Erasmus+ Programme of the European Union

References

[1] *CREDIT Project*, **Accreditation Model Definition, MM 1032 Project CREDIT**, Version 2.0, University of Amsterdam, 15.2.99

[2] DTI - Department of Trade and Industry UK, **British Standards for Occupational Qualification**, *National Vocational Qualification Standards and Levels*

[3] R. Messnarz, et al., ***Assessment Based Learning centers***, in Proceedings of the EuroSPI 2006 Conference, Joensuu, Finland, Oct 2006, also published in Wiley SPIP Proceeding in June 2007

[4] Richard Messnarz, Damjan Ekert, Michael Reiner, Gearoid O'Suilleabhain, ***Human resources based improvement strategies - the learning factor* (p 355-362)**, Volume 13 Issue 4, Pages 297 - 382 (July/August 2008), Wiley SPIP Journal, 2008

[5] European Certification and Qualification Association, ***ECQA Guide***, Version 3, 2009, www.ecqa.org, Guidelines

[6] Richard Messnarz, Damjan Ekert, Michael Reiner, **Europe wide Industry Certification Using Standard Procedures based on ISO 17024**, in Proceedings of the TAEE 2012 Conference, IEEE Computer Society Press, June 2012

[7] The European Skills/Competences, Qualifications and Occupations (ESCO), https://ec.europa.eu/esco/portal/home

[8] The European Qualifications Framework (EQF), https://www.cedefop.europa.eu/en/events-and-projects/projects/european-qualifications-framework-eqf

[9] European Credit Transfer and Accumulation System (ECTS), https://ec.europa.eu/education/resources-and-tools/european-credit-transfer-and-accumulation-system-ects_en

[10] The European Credit system for Vocational Education and Training (ECVET), https://ec.europa.eu/education/resources-and-tools/the-european-credit-system-for-vocational-education-and-training-ecvet_en

[11] Messnarz R., Georg Macher, Florian Stahl, Stefan Wachter, Damjan Ekert, Jakub Stolfa, and Svatopluk Stolfa (2020) **Automotive Cybersecurity Engineering Job Roles and Best Practices – Developed for the EU Blueprint Project DRIVES.** In:

Yilmaz M., Niemann J., Clarke P., Messnarz R. (eds) Systems, Software and Services Process Improvement. **EuroSPI 2020. Communications in Computer and Information Science, vol 1251. Springer, Cham.** https://doi.org/10.1007/978-3-030-56441-4_37

[12] Development and Research on Innovative Vocational Educational Skills. (2020). (rep.). Reference and Recognition Framework – Analysis. Retrieved from https://www.projectdrives.eu/Media/Publications/25/Publications_25_20200604_132039.pdf

With the support of the Erasmus+ Programme of the European Union