DRIVES

Development and Research on Innovative Vocational Education Skills

Automotive Cybersecurity Manager

Job Role Skill Set

Co-funded by the Erasmus+ Programme of the European Union

Development and Research on Innovative Vocational Skills -DRIVES – Project number 591988-EPP-1-2017-1-CZ-EPPKA2-SSA-B

DOCUMENT TITLE

Report Title:	Automotive Cybersecurity Manager Job Role Skill Set		
Author(s):	Dr. Richard Messnarz		
Responsible Project Partner:	ISCN	Contributing Project Partners:	ISCN, TU-Graz

Document data:	Status:	(draft/final)	Dissemination level:	Public
Project title:	Development and Research on Innovative Vocational Educational Skills		GA No.:	2017-3295/001-001.
WP title:	WP3 – Skills Framework		Project No.:	591988-EPP-1-2017-1-CZ-EPPKA2-SSA-B
			Deliverable No:	D3.1
			Submission date:	30/04/2020
Keywords:	automotive sector, skill card, skill set, job roles, ECTS, ECVET			
Reviewed by:	Damjan Ekert (Formal Review)		Review date:	30/04/2020
			Review date:	
Approved by:	Anke Blume Richard Messnarz		Approval date:	30/04/2020

More information about DRIVES project and contact:

www.project-drives.eu

TABLE OF CONTENTS

1 INTRODUCTION

1.1 OBJECTIVE

The objective of this deliverable is to provide an introduction to described Job Role within the applied skills definition model.

1.2 PURPOSE OF THE DELIVERABLE

The purpose of this deliverable is to define skills definitions of the Automotive Cybersecurity 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 Role
- Description of used Skill Sets and skills definitions, coverage of Qualification Schemas

The deliverable does not cover:

- Course development, as this will be done after the skill definitions based on the defined skills which need to be covered by the course.

2 ECQA SKILLS DEFINITION MODEL

A skills definition contains the following items:

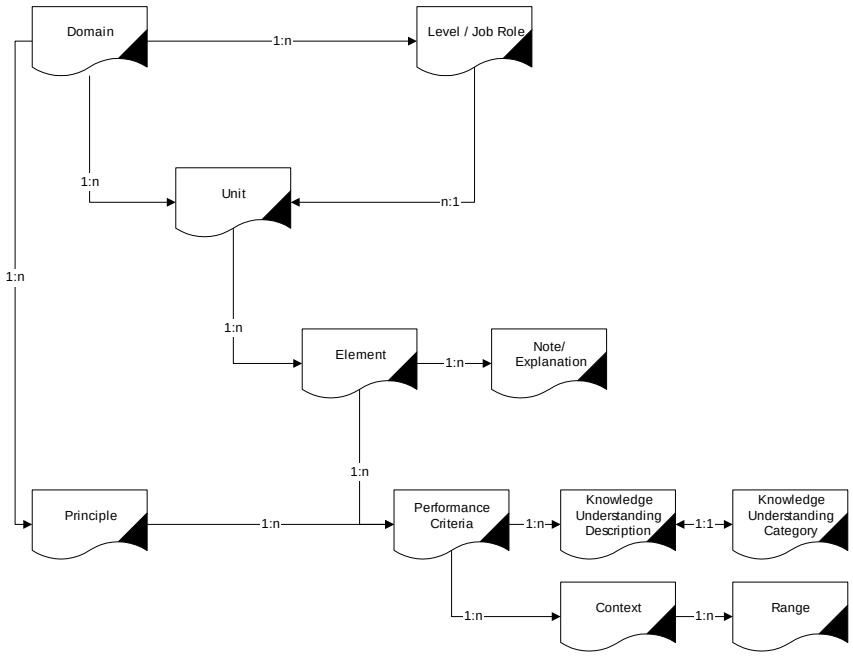

Figure 1 The Skill Definition Model (1:n = one to many relationship)

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

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; it 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 certain 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 a number of 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. These models have been re-used and slightly modified by other countries when they started employing skill cards [1], [2].

ECQA standards are used to describe the skills sets delivered within the DRIVES project (www.project-drives.eu). Further description and rationales are attached in annexes of this document. The ECQA structure was mapped in DRIVES project to DRIVES Reference and Recognition Framework with the links to ESCO[7], EQF[8], ECTS[9] and ECVET[10]. See more in deliverable DRIVES-D4.1.1 Reference and Recognition Framework – Analysis.pdf (www.project-drives.eu).

3 SKILLS DEFINITION FOR THE JOB ROLE AUTOMOTIVE CYBERSECURITY MANAGER

3.1 THE SKILLS HIERARCHY

In the DRIVES project in cooperation with SOQRATES (www.soqrates.de) the new job roles for cybersecurity have been defined.

1. Automotive Cybersecurity Manager
2. Automotive Cybersecurity Engineer
3. Automotive Cybersecurity Tester

The overall set of units and elements for cybersecurity have also been assigned to levels of skills (awareness, practitioner, expert level), see Fig. 2 below.

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

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

In this document we describe the skills set for the cybersecurity manager.

3.2 THE SKILLS DESCRIPTIONS – JOB ROLE AUTOMOTIVE CYBERSCURITY MANAGER

Domain Acronym: Engineering

Domain title: Cybersecurity in Automotive

Domain Description:

Design of modern vehicles requires to consider security related norms (SAE J3061, ISO 21434) and the implementation of security related design patterns. This includes e.g.

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

The DRIVES (EU Blueprint project for Automotive, 2018 – 2021) user analysis outlined that all car makers have a high demnd in the training and certification of cybersecurity related skills of their engineering and testing staff. In the SOQRATES woring group irst a brain storming took place, then a structure of units and elements has been designed and since 2019 the working group elaborates and shares best practices per element of knowledge.

Three job roles have been considered in the analysis:

1. ECQA Certified Cybersecurity Manager
2. ECQA Certified Cybersecurity Engineer
3. ECQA Certified Cybersecurity Tester

In this document we focus on the skills required for the cybersecurity manager.

Job Role Acronym: CYBERMAN

Job Role Title: Automitive Cybersecurity Manager

Description:

The Skill card comprises the following thematic learning units, and learning elements for the job role cybersecurity manager:

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 Hardware Design and Vulnerability Analysis (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 system level (awareness)

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 Planning

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 about the following aspects:

- You know about the legal situation
- You know about cases showing a high business impact
- You know about the issue of complex mechatronic products and safety
- You know the most important norms and their main meaning, required for homologation of cars in case of functional safety.

Performance Criteria:

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U1.E1.PC1	The student knows about data protection laws.
CYBER.U1.E1.PC2	The student knows about hacker paragraphs for allowing the testing.
CYBER.U1.E1.PC3	The student knows about the European regulations and product liability law and the resulting consequences.

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

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

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

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

3.3.3 Unit CYBER.U1 - Element 3: Cybersecurity Planning

Acronym: CYBER.U1.E3

Element Title: Cybersecurity Planning

Element Note:

This element deals with

- How to establish a plan in the project?
- What methods to be selected?
- Considering not only development, also production, or series maintenance – the entire life cycle needs to be considered.

Performance Criteria:

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U1.E3.PC1	The student knows about how to establish and maintain cybersecurity plans in an Automotive project.
CYBER.U1.E3.PC2	The student 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 student knows that work products and tasks need to be planned for the entire life cycle, not only development, also production, or series maintenance.

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

3.4 UNIT CYBER.U2 CYBERSECURITY OPERATION AND MAINTENANCE

Acronym: CYBER.U2

Title: Cybersecurity Operation and Maintenance

Description:

This unit addresses aspects such as

- Cybersecurity related life cycle assessment
- Cybersecurity processes and audits

- Incident response management
- Supply Chain Security

3.4.1 Unit CYBER.U1 - 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 entire life cycle, not just during development.

Performance Criteria:

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U2.E1.PC1	The student is able to analyse threats in all phases of the life cycle.
CYBER.U2.E1.PC2	The student is able assess vulnerabilities in all phases of the life cycle.
CYBER.U2.E1.PC3	The student is able to set appropriate measures to solve vulnerabilities in all phases of the life cycle, e.g. key handling, update of SW, EOL in production, trust provisioning, etc.

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

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 evidences to prepare for a cybersecurity process audit.

Performance Criteria:

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U2.E2.PC1	The student knows the clauses of the ISO 21434 norm and how they can be mapped to processes of an organisation.
CYBER.U2.E2.PC2	The student knows the clauses of the SAE J3061 norm and how they can be mapped to processes of an organisation.
CYBER.U2.E2.PC3	The student knows how an assessment is planned, performed, and documented.

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

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

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

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

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

Acronym: CYBER.U2.E4

Element Title: Supply Chain Security

Element Note:

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

Performance Criteria:

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

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

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

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 Design and Vulnerability Analysis

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
- Drawing a system item picture including the assets that could be attacked
- Threat and Risk Analysis (TARA)
- Cybersecurity goals

Performance Criteria:

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U3.E1.PC1	The student knows the different types of attacks.
CYBER.U3.E1.PC2	The student is able to access the known threat lists.
CYBER.U3.E1.PC3	The student is able to identify and document cybersecurity assets (asset analysis).
CYBER.U3.E1.PC4	The student is able to draw a system item picture showing the system structure and the cybersecurity assets as potential attack targets.
CYBER.U3.E1.PC5	The student is able to perform a TARA (Threat and Risk Analysis) and document it.
CYBER.U3.E1.PC6	The student is able to derive cybersecurity goals from the TARA (Threat and Risk Analysis) and document them.

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

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 looks at the system level related cybersecurity methods.

This includes

- Applying cybersecurity design patterns on system level
- Performing an attack tree analysis
- Performing vulnerability analysis and integrating a proper defence mechanism
- Integrating cybersecurity views into the system architectural design
- Writing cybersecurity requirements

Performance Criteria:

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

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

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

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.

This includes

- Cybersecure Data Analysis
- Cybersecure Functions Analysis
- Writing cybersecurity software requirements
- Integrating cybersecurity views into the software architectural design
- Applying a list of state of the art software related cybersecurity design patterns

Performance Criteria:

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U3.E3.PC1	The student is able to perform a cybersecure critical software functions analysis.
CYBER.U3.E3.PC2	The student is able to perform a cybersecure critical software data analysis.
CYBER.U3.E3.PC3	The student is able to write cybersecurity related software requirements.
CYBER.U3.E3.PC4	The student 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 student is able to integrate cybersecurity views into the software architectural design.
CYBER.U3.E3.PC6	The student knows cybersecurity design patterns on software level and how to apply them.

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

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 looks at the software detailed design level related cybersecurity methods.

This includes

- Cybersecurity related detailed SW design principles
- Cybersecurity critical code inspections and reviews
- Qualification of 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 student must be able to show evidence of competencies for the following performance criteria (PC):

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U3.E4.PC1	The student knows the common weakness enumeration of the community developed list of software weakness types (https://cwe.mitre.org/)
CYBER.U3.E4.PC2	The student knows the guidelines of OWASP (Open Web Application Security Project) and the recommended tools and methods.
CYBER.U3.E4.PC3	The student knows how to perform a cybersecure related code review, and the review checklist applies the OWASP knowledge.
CYBER.U3.E4.PC4	The student knows and applies the MISRA 2012 extension rules for cybersecurity relevant code development.
CYBER.U3.E4.PC5	The student knows the principles of preventive and defensive programming.

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

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

Acronym: CYBER.U3.E5

Element Title: Hardware Design and Vulnerability Analysis

Element Note:

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

This includes

- Integrating HSM (Hardware Security Module) on ECU
- Architecture of a HSM
- Interfacing operating system on main controller and HSM firmware
- Configuration of secure com stack
- List of main diagnostic security services to be provided

Performance Criteria:

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U3.E5.PC1	The student knows how to integrate the HSM (Hardware Security Module) into the ECU.
CYBER.U3.E5.PC2	The student knows the typical architecture of a HSM.
CYBER.U3.E5.PC3	The student knows how the interfaces between the main controller and the HSM controller /(firmware) work.
CYBER.U3.E5.PC4	The student knows the main services provided by a Secure OS Lib in a secure operating environment (list of functions and services).

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

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.

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U4.E1.PC1	General: The student knows about the test methods proposed by the norms SAE J3061, ISO 21434 and the OWASP project.
CYBER.U4.E1.PC2	SW unit test related: The student knows about the MISRA 2012 check using the extension for cybersecurity.

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U4.E1.PC3	SW unit test related: The student knows about cybersecure relevant criteria to be applied informal code reviews (using the available libraries like OWASP).
CYBER.U4.E1.PC4	SW integration test related: The student 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 student knows about the configuration of a secure comm stack and checks the correct configuration.
CYBER.U4.E1.PC6	SW integration test related: The student knows the criticality of the communication between the main controller OS and the firmware in the HSM and extra test cases to assure that communication are applied.
CYBER.U4.E1.PC7	SW function test related: The student knows the 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 student knows how to test all diagnostic services requested by the cybersecurity protocols and that all of them are tested.
CYBER.U4.E1.PC9	SW penetration test related (integration and functional test in SW): The student knows the concept of penetration testing and how to involve such external penetration testing (hacker) teams.
CYBER.U4.E1.PC10	Traceability: The student knows how to link cybersecurity critical SW requirements to test cases and test results.

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

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U4.E2.PC1	The student 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 student knows that OEMs provide SSL/SSA libraries which need to be integrated with the HSM software and that OEM/customer specific test environments/tools need to be used.
CYBER.U4.E2.PC3	The student knows that HW security modules have a specification sheet with services that need to be activated and that the activation of these services needs to be reviewed.
CYBER.U4.E2.PC4	The student knows that the exploit options of the selected HSM module need to have a 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.

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

3.6.3 Unit CYBER.U4 - Element 3: Cybersecurity verification at system 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 student must be able to show evidence of competencies for the following performance criteria (PC):

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

Performance Criterion	Evidence Check: The student can demonstrate
CYBER.U4.E3.PC2	System integration: The student knows what security services at vehicle level in the production at EOL or at vehicle set up when integrating the vehicle.
CYBER.U4.E3.PC3	System test: The student knows what security services at vehicle level in the operation need to be tested and what security data need to reported/observed to assure secure fleet operation.
CYBER.U4.E3.PC4	System test: The student 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 student knows how to interact with external penetration testing teams to assure early detection of weaknesses and issue problem reports before incidents appear.

Table 15 Performance Criteria for the Element CYBER.U4.E1

ANNEXES

The annex provides overview of used skills set, coverage of Qualification Schemas and Legal background for Certification

ANNEX A ECQA DESCRIPTION

ECQA – EUROPEAN CERTIFICATION AND QUALIFICATION ASSOCIATION

ECQA standards are used to describe the skills sets delivered within the DRIVES project (www.project-drives.eu). ECQA is the pilot Certification body, which structure is mapped to DRIVES Reference and Recognition Framework providing the EU-wide overview of training courses and possible certifications, and micro-credentials. DRIVES Reference and Recognition Framework provides links to ESCO[7], EQF[8], ECTS[9] and ECVET[10]. See more in deliverable DRIVES-D4.1.1 Reference and Recognition Framework – Analysis.pdf (www.project-drives.eu).

Europe Wide Certification

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

Through the ECQA it becomes possible that you attend 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 currently supports 27 professions in Europe and with the continuous support until 2012 by the European Commission the pool is growing to 30 certified professions in Europe. 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

ECQA SKILLS DEFINITION MODEL

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

ECQA SKILL SET STRATEGY

Imagine that in the future Europeans will have a skill set like a card with a chip which stores your skill profile to fulfil specific professions, job roles, and tasks. It's working like 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 UK, The Netherlands, and France already have well established open universities which support APL (Accreditation of Prior Learning). In APL the skills of students are assessed, already gained skills are recognised, and only for the skill gaps a learning plan is established. The skill assessment bases on defined skill units and a skill profile displaying how much of the skill units are covered.

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

ECQA SKILLS ASSESSMENT MODEL

Step 1 – Browse a Skills Set: You select a set of skills or competencies, which are required by your profession or job using national standards or your company standards. You browse different skills cards and select a job role you would like to achieve.

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

your company which offers skills assessment services. In case of the Safety Manager Project the registration will automatically assign a predefined service unit.

Step 3 – Receive an Account for Self-Assessment and Evidence Collection : With the registration you automatically received an account to login to the working space in which you can go through the steps of online self assessment and the collection of evidences to prove that you are capable of certain performance criteria.

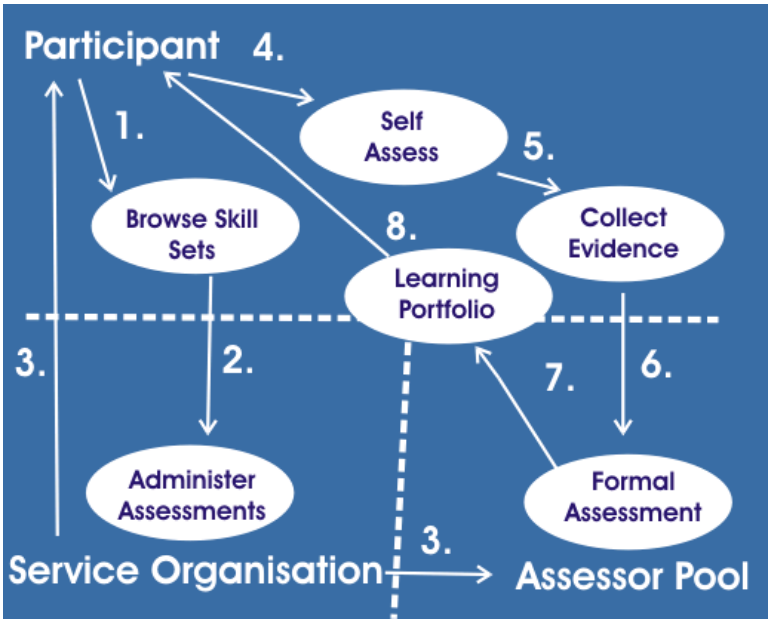

Figure 3 Basic steps of the skills assessment model

Step 4 – Perform Self Assessment: You 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 in which areas your self assessment shows improvement potentials.

Testing of Skills (Addition to Step 4) – The system provides a multiple-choice test for each performance criteria so that you can check your capabilities as realistically as possible.

Step 5 – Collect Evidences: Before you want to enter any formal assessment you need to prove your skills by evidences. Evidences 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). Evidences you can then link 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 they

received a certificate if they pass. This traditional approach however is insufficient when it comes to measuring experience and (soft) skills learned on the job and fails to give recognition to skills gathered on the job. The APL (Accreditation of Prior Learning) approach, by contrast, collects so called evidences. Evidences can be certificates obtained in the traditional way, but also references from previous employers, materials from previous projects in which the person took ownership of results (e.g. a test plan) to prove their capability, as well as 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 evidences 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 Advise 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 advises).

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 student passed the test, all elements shall be covered
  - Generation of certificate

- Professional Certificate
    - Uploading applied experiences for review by assessors
    - Rating by assessors
    - Observation of 2 years

The certificates show credited elements in comparison to all required.

ANNEX B ECQA COVERAGE OF QUALIFICATION SCHEMAS

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 an 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).

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)

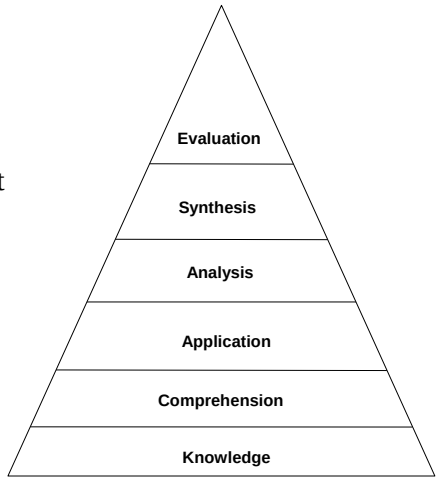

Figure 4 BLOOMS Learning Levels

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
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	Knowledge	Example
Level 8	Knowledge at the most advanced frontier of a field of work or study and at the interface between fields	Six Sigma Master Black Belt

Figure 5 EQF Learning Levels

MAPPING BASED ON ECTS AND ECVET SCHEMA

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

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

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 on different universities in Europe.

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 6 EQF Example Automotive Quality Engineer and Safety Manager

The 2 job roles illustrated in the picture above have been assigned to ECTS and are taught using the same skills set at industry and also universities.

ECVET Mapping

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

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 7 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 8 ECVET Mapping example – Functional Safety Manager / Engineer

ANNEX C ECQA LEGAL BACKGROUND FOR CERTIFICATION

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 to log the exam to keep a record/proof that the examinee passed the exam
- Mapping of processes towards ISO 17024

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 form of a self declaration.

LIASION WITH NATIONAL UNIVERSITIES

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

ANNEX D 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**