ECQA Certified Cybersecurity Engineer and Manager

Automotive Sector

IO1

Study about the requirements for an ECQA Certified Cybersecurity Engineer and Manager – Automotive Sector

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

Report Title:	**Study about the requirements for an ECQA Certified Cybersecurity Engineer and Manager – Automotive Sector**		
Author(s):	Abdelkader Shaaban, Christoph Schmittner et al.		
Responsible Project Partner:	AIT	**Contributing Project Partners:**	VSB-TUO; REAL-SEC; Elektrobit; ISCN; TUG

Document data:	**File name:**	CYBERENG IO1 Study About Requirements		
	Pages:	28	**No. of annexes:**	2
	Status:	Final	**Diss. Level:**	PU
Project title:	ECQA Certified Cybersecurity Engineer and Manager – Automotive Sector		**KA No.:**	KA203-FE74E5D7
			Output No:	IO1
Date:	**Due Date:**	30/4/2021	**Submission date:**	30/4/2021
Keywords:	Cybersecurity; engineer; manager; survey; analysis; skills; competence			
Review by:	Marek Spanyik, VSB-TUO		**Review date:**	29/4/2021
	Jan Plucar, VSB-TUO			29/4/2021
Approved by:	Jakub Stolfa, VSB-TUO		**Approval date:**	30/4/2021

For more information visit project website

CYBERENG (project-cybereng.eu)

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

Table of Contents

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

Abbreviations

CCAM	...	Cooperative, Connected and Automated Mobility
CYBERENG	...	ECQA Certified Cybersecurity Engineer and Manager – Automotive Sector
DRIVES	...	Development and Research on Innovative Vocational Educational Skills
ECU	...	Electronic Control Unit
ERASMUS+	...	EU Programme for Education, Training, Youth and Sport in Europe
ESCO	...	European Skills/Competences, qualifications and Occupations
ICT	...	Information and Communications Technology
IoT	...	Internet of Things
IT	...	Information Technology
ITS	...	Intelligent Transport System
NICE	...	Workforce Framework for Cybersecurity
US	...	United States

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

Executive Summary

The automotive domain is moving towards connected and automated vehicles [1] with a high degree of dynamic and adaptive behavior, driven by software. Due to this connectivity and interaction, cybersecurity is an increasingly important topic. In the future automotive cybersecurity will also play an important role in the type of approval. Due to this challenge, it is necessary to supply the automotive industry with the necessary expertise. For this the ERASMUS+ project CYBERENG was started to develop a skill set, training material, online training campus and certification framework and exams for automotive cybersecurity engineering and manager job roles.

We present here the first results of a European Erasmus+ project, aiming at the development of training for automotive cybersecurity.

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

1. Introduction

The automotive domain is experiencing a transformation from mechanical systems, augmented with embedded control systems towards complex and automated cyber-physical systems with an extended reliance on software.

Modern vehicles have over 100 million lines of code [2], distributed on more than 150 ECUs [3]. Also, there is a transformation from isolated vehicles towards cooperative and connected vehicles [4], integrated into a complex ITS [5]. Vehicles become complex IoT systems, composed of the underlying transport, energy, and infotainment IoT. This new form of mobility is called CCAM [6]. With this increasing reliance on software, connectivity, coordination, and automation there is also a rising need for new skills and expertise in the automotive domain.

1.1. Goal

While there is ongoing work regarding cybersecurity training and expertise in IT and IoT systems, there is still ongoing research on how to address them in the context of the automotive domain. Automotive systems pose particular challenges, ranging from the widespread usage of legacy technologies [7] to the overlap between cybersecurity with safety and also regulatory aspects [8]–[10]. In [11] cybersecurity training was identified as a critical investment, with the right combination of people, processes, and technology as key to success. In [12] training was even identified as the 6th layer of defense in a successful defense in-depth strategy for the automotive domain.

To tackle this challenge there is a need for ongoing training and education in automotive cybersecurity expertise.

To give an insight into the demand, the US Bureau of Labor Statistics expects a rise in the number of cybersecurity jobs by 31% through 2029, compared with an average job growth of 4% [13].

Due to this the CYBERENG project was started as a European Union Erasmus+ project to develop training for automotive cybersecurity. The project is coordinated by the Technical University of Ostrava and the project consortium includes Real security, ISCN, TU Graz, Elektrobit and AIT Austrian Institute of Technology. The project will focus on training for the two fundamental roles:

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

- An **automotive cybersecurity engineer** possesses the basic skills for active technical work regarding the achievement of automotive cybersecurity for a product throughout the complete lifecycle.
- In comparison, an **automotive cybersecurity manager** focuses more on the process level and standard and regulatory compliance and on the management of automotive cybersecurity in a distributed process.

While the generic description of engineer and manager roles can be taken from established disciplines like automotive safety, details, skills, and training are undefined for the automotive domain. The European Skills, Competences, Qualifications and Occupations (ESCO) portal does define ICT related roles like ICT security manager, admin, consultant or technician but does not define a security related role for automotive [14]. Therefore, the CYBERENG project developed, as a first step, set of skill statements for both roles. A survey, based on these skill statements, was distributed to the expert network of the participating organizations to get feedback regarding these skill statements. We will give here an overview of the survey results and present the next steps.

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

2. Development of the Survey

With a lack of proper cyber training, many employees may be more vulnerable to external cybersecurity threats and less able to prevent security breaches inside their organization. This is because of the rising use of the Internet and online services that require higher levels of cyber protection [15]. Furthermore, cybersecurity knowledge and training are essential where cyber-attacks occur daily [16]. As discussed in [15], organizations need to spend money and time on cybersecurity training and awareness to create an effective risk management process with highly skilled personnel. This will lead to an organization providing a better understanding of resisting various cyber-attacks.

To identify which skills are required in the automotive domain the CYBERENG project researched existing skill descriptions and developed the first set of skill statements. Inputs were collected from publications, national and international expert groups and related projects such as the project DRIVES [17], [18].

Besides input from the project DRIVES additional material was brought in from partner experienced in automotive and cybersecurity and from discussions in standardization committees.

To facilitate responses to the survey it was decided to go for a set of skill statements to which the respondents simply agreed or disagreed. Other approaches like a Likert scale [19] were discussed, but this would increase the time needed to fill in the survey and could therefore lead to fewer feedbacks. Therefore, it was also decided to not ask for the level of required expertise, but to add this to the skill statement.

Overall, three iterations of the survey were built until the consortium considered the balance between meaningful results and ease of filling to be achieved.

Based on the collected inputs a set of 18 skill statements for **automotive cybersecurity engineer** and 16 skill statements for **automotive cybersecurity manager** were formulated and distributed to known automotive and cybersecurity experts and interested groups in the public.

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

2.1. Survey Structure

As mentioned previously, two questionnaires were developed and distributed based on the identified target groups: (1) known automotive and cybersecurity experts; and (2) interested groups in the public. Questionnaire structure is the same for both target groups:

1) self-assessment of the respondent;
2) skills rating for cybersecurity engineer role;
3) skills rating for the cybersecurity manager role;
4) conclusions.

After Section one: Self-assessment of the respondent, the questionnaire branches either into Section Two: Automotive Cybersecurity Engineer Skills or Section Three: Automotive Cybersecurity Manager Skills based on the respondents' indication in the Section One where it is possible to specify the interest in cybersecurity engineer or cybersecurity manager role. Detailed information on the questions is provided in Annex I. – Survey on Skills – Public and Annex II. – Survey on Skills – Not Public.

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

3. Survey Skills Statements Analysis

As already mentioned, the final questionnaire for the survey went through several rounds of discussions and changes. The final form of the questionnaire presents the respondent with a role using a simple descriptive model of no more than twenty expressions. Nevertheless, it can be difficult to simply imagine the main competencies of the roles from the questionnaire. This subchapter shows an alternative view of the questions from the questionnaire, which were visualized in the form of Word Cloud. Word clouds or tag clouds are graphical representations of word frequency that give greater prominence to words that appear more frequently in a source text. The larger the word in the visual the more common the word was in the document(s). The visualization considers the first 40 most frequently represented words (Figure 1: Word Cloud, Cyber Security Engineer, Figure 2: Word Cloud, Cyber Security Manager). Although it is a relatively simple method of text analysis, for the purposes of validation and verification of the correct design of questions in the questionnaire, in our case it will suffice.

3.1. Automotive Cybersecurity Engineer vs Manager

By comparing Figures 1 and Figure 2, clear differences between the descriptive models can be identified.

- An **automotive cybersecurity engineer** is defined by words such as cybersecurity, system design, design pattern, cybersecurity requirements, hardware level.
- In comparison, an **automotive cybersecurity manager** is defined by words such as customer, suppliers, supply chain, cybersecurity risk, data protection, organizational process, software update, etc.

Figure 1: Word Cloud, Cyber Security Engineer

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

Figure 2: Word Cloud, Cyber Security Manager

3.2. General Cybersecurity Standards

When creating the two basic automotive roles (automotive cybersecurity engineer and manager), the currently used standards in the field of general computer security were also considered. This chapter presents a possible mapping of the proposed roles to the basic categories and areas of the NICE framework [21], which is one of the most widely used standards for describing roles in the field of computer security.

It is worth noting that the established standards are very complex and define roles at a very low level. However, the aim of this project is to define the basic roles that may break down into specialized roles in the future.

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

Table 1: NICE Framework Mapping

E*	M*	Categories	Descriptions
X		Securely Provision	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
X	X	Operate and Maintain	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
	X	Oversee and Govern	Provides leadership, management, direction, and/or development and advocacy so the organization may effectively conduct cybersecurity work.
X	X	Protect and Defend	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
X		Analyze	Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
X	X	Collect and Operate	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
		Investigate	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

*E = Engineer

*M = Manager

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

4. Results

The complete list of skill statements and responses can be found in the Annexes, Annex I. – Survey on Skills – Public and Annex II. – Survey on Skills – Not Public.

The survey has 39 questions. Four main sections are defined in this questionnaire. This aims to provide a series of questions covering a wide range of points relevant to automotive cybersecurity. Answers to these questions will be collected to provide a comprehensive technical landscape of skills that automotive cybersecurity managers and engineers should be familiar with. Overall, we received 92 responses.

4.1. Section one: Self-assessment of the respondent

The questionnaire asked a few questions to establish the degree of experience in cybersecurity and automotive. It begins by inquiring about respondents' experience with cybersecurity, followed by checking their expertise regarding automotive expertise. Figure 3 and Figure 4 gives an overview of the responses. According to the collected data, more than half of the participants have more than three years of automotive expertise (see figure 4). Regarding security expertise (see figure 3), there is almost an inversion comparing automotive and other domains.

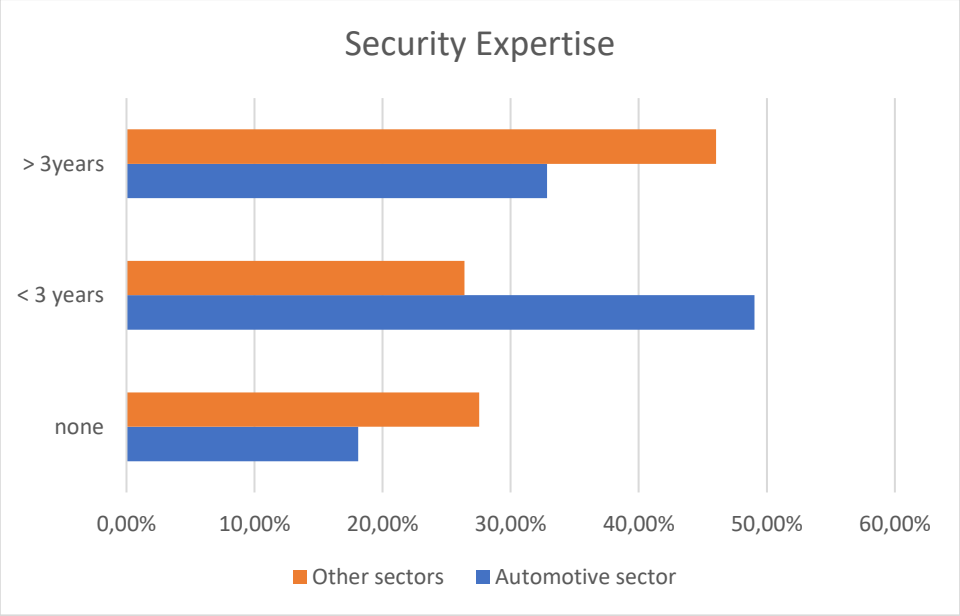

Figure 3: Security Expertise

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

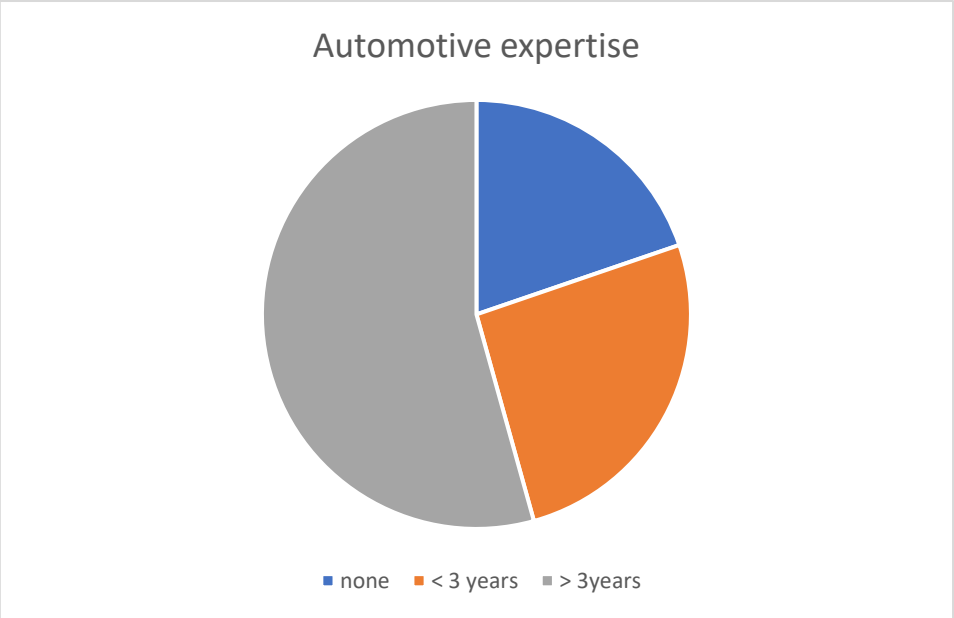

Figure 4: Automotive Expertise

Only 32.85% have more than 3 years of automotive cybersecurity expertise, compared with 46.95% which have more than 3 years of cybersecurity expertise in other domains.

For the next section, the survey participants could decide between taking the **automotive cybersecurity engineer** or the **automotive cybersecurity manager** skill statements. Figure 5 shows the decision from the participants. An unexpected behavior was that if a participant moved on to the next set of questions without selecting a option he could give feedback to both sets of skill statements.

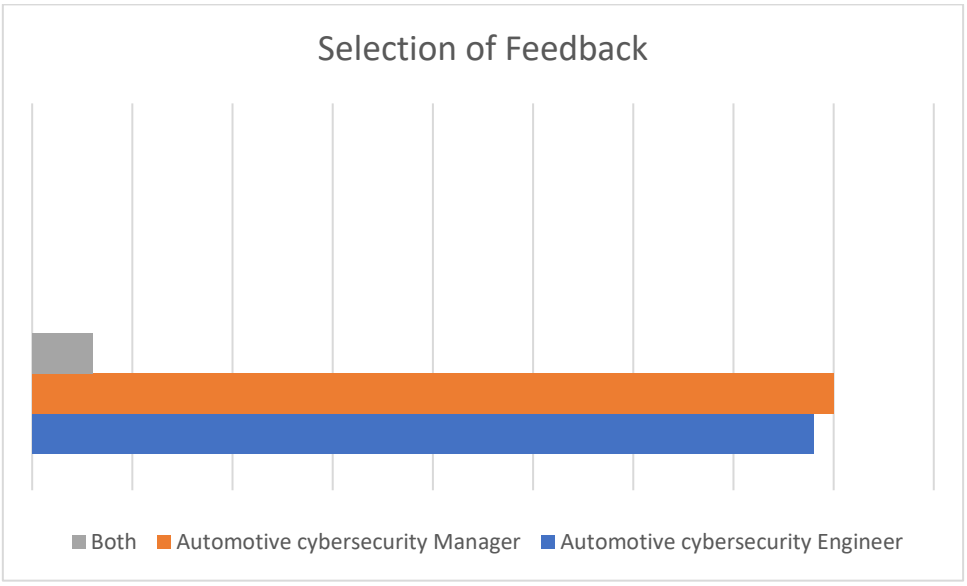

Figure 5: Feedback to Manager or Engineer

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

4.2. Section Two: Automotive Cybersecurity Engineer Skills

This section includes a collection of "agree" and "disagree" questions that estimate respondents' opinions on certain skills and experiences an automotive cybersecurity engineer should have. These questions cover a wide range of cybersecurity necessities that automotive cybersecurity may be aware of all or part of them.

All questions were optional to answer, e.g. if a survey participant had no opinion to a skill statement there was the option to continue without answering the question. The rate of the agree answers is 88.99%, where 10.12% disagree on some skills and experiences that should not be a part of automotive cybersecurity engineers. Considered all questions and responses, 0.89% were not answered.

While in general, the rate of agreement was very high, there were two questions with a substantial rate of disagreement. The first one was related to the topic of asset identification (28.57% disagreement). Here survey participants used the option to give additional comments and thought these skills were more related to the Automotive Cybersecurity Manager role. Regarding cybersecurity assessment (30.95% disagreement), survey participants were not sure if this would not overload the role of the Automotive Cybersecurity Engineer skill set. Proposed solutions were the definition of additional roles for assessment.

4.3. Section Three: Automotive Cybersecurity Manager Skills

Like section two, this section provides a set of "agree" and "disagree" questions to check the knowledge that should be available for the automotive cybersecurity manager.

Annex gives the rate of agreeing and disagree answers about skills that the automotive cybersecurity manager should provide.

Overall, there was 87.18% agreement and 12.65% disagreement to the survey. Here three skill statements received a higher level of disagreement.

The first skill statement was regarding the development interface agreement [20] which was seen as mixing topics from cybersecurity engineer and manager. Also, there were issues that this topic might not be relevant for Automotive Cybersecurity Manager in all organizations.

The second skill statement which was disputed was regarding threat lists. While knowledge of the existence of these threat lists was considered relevant, it was also felt

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

that in-depth knowledge was more relevant to a specific role. In a similar direction question, 14 was considered as more related to other roles.

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

5. Conclusions

Overall, we received a high number of agreements to the formulated skill statements and will take them as starting points for the next steps in the project. With this said, there were also several comments and points raised which will be taken into consideration for the further work of the project.

5.1. Need for additional and subsequent specialized courses

One point raised from multiple respondents was that these two roles do not cover everything, and hints were given for additional roles. Here we completely agree and see the automotive cybersecurity engineer and manager simply as starting steps and trainings on which specialized trainings can be built upon. With this said we identify the requirement to define and develop fundamental courses.

5.2. Level of Knowledge is Required

We received the feedback that for some skill statements a role must know the subject, but not necessarily be able to apply it. While we tried to formulate this in the skill statements themselves it will be important to make this distinction transparent and decide which topics we need to present as an overview and for which topics a practical application is needed for the training. Here we have the requirement to identify the level of knowledge needed for each skill and build the training accordingly.

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

References

[1] Richard Messnarz, Georg Macher, Jakub Stolfa, and Svatopluk Stolfa, "Highly Autonomous Vehicle (System) Design Patterns – Achieving Fail Operational and High Level of Safety and Security," presented at the 26th European Conference on Systems, Software and Services Process Improvement: EuroSPI 2019, Edinburgh, Jan. 2019.

[2] Yanja Dajsuren and Mark van den Brand, Eds., *Automotive Systems and Software Engineering - State of the Art and Future Trends*. Springer, 2019.

[3] IHS Markit AutoTechInsight, "ADAS & Electric Vehicles accelerate demand of automotive electronic control units," AutoTechInsight, May 2019.

[4] Jakub Stolfa *et al.*, "DRIVES – EU blueprint project for the automotive sector – a literature review of drivers of change in automotive industry," Nov. 2019.

[5] Wolfgang Kerber and Daniel Möller, "Access to Data in Connected Cars and the Recent Reform of the Motor Vehicle Type Approval Regulation," *Joint Discussion Paper Series in Economics*, Jul. 07, 2019.

[6] European Commission, "Intelligent transport systems: Cooperative, connected and automated mobility (CCAM)." Apr. 26, 2021. Accessed: May 14, 2021. [Online]. Available: https://ec.europa.eu/transport/themes/its/c-its

[7] Georg Macher, Harald Sporer, Eugen Brenner, and Christian Kreiner, "Supporting cyber-security based on hardware-software interface definition," presented at the European Conference on Software Process Improvement, 2016.

[8] G. Macher, A. Much, A. Riel, R. Messnarz, and C. Kreiner, "Automotive SPICE, Safety and Cybersecurity Integration," in *Computer Safety, Reliability, and Security*, vol. 10489, S. Tonetta, E. Schoitsch, and F. Bitsch, Eds. Cham: Springer International Publishing, 2017, pp. 273–285. doi: 10.1007/978-3-319-66284-8_23.

[9] A. Much, "Automotive Security: Challenges, Standards, and Solutions," *Software Quality Professional Magazine*, 2016.

[10] G. Macher, R. Messnarz, E. Armengaud, A. Riel, E. Brenner, and C. Kreiner, "Integrated Safety and Security Development in the Automotive Domain,"

presented at the WCX™ 17: SAE World Congress Experience, Mar. 2017. doi: 10.4271/2017-01-1661.

[11] D. J. Francois Charbonneau Mohamed Slim Ben Mahmoud, *Securing the Modern Vehicle: A Study of Automotive Industry Cybersecurity Practices*. 2019.

[12] P. Institute, *Cybersecurity in Automotive - How to stay ahead of Cyber Threats?* 2018.

[13] S. I. STAFF, *Cybersecurity: A career that will stay in-demand for decades to come*. 2021. [Online]. Available: https://www.studyinternational.com/news/cybersecurity-career-in-demand/

[14] European Commission, *European Skills, Competences, Qualifications and Occupations*. 2021. [Online]. Available: https://ec.europa.eu/esco/portal/occupation

[15] Clare Naden, *THE CYBERSECURITY SKILLS GAP*. 2021. [Online]. Available: https://www.iso.org/news/ref2655.html

[16] R. Beuran, C. Pham, D. Tang, K. Chinen, Y. Tan, and Y. Shinoda, *Cytrone: An integrated cybersecurity training framework*. SCITEPRESS–Science and Technology Publications, 2017.

[17] J. Stolfa *et al.*, "Automotive Engineering Skills and Job Roles of the Future?," in *European Conference on Software Process Improvement*, 2020, pp. 352–369.

[18] R. Messnarz *et al.*, "Automotive Cybersecurity Engineering Job Roles and Best Practices–Developed for the EU Blueprint Project DRIVES," in *European Conference on Software Process Improvement*, 2020, pp. 499–510.

[19] D. Bertram, "Likert scales," *Retrieved November*, vol. 2, no. 10, 2007.

[20] C. Schmittner, J. Dobaj, G. Macher, and E. Brenner, "A preliminary view on automotive cyber security management systems," in *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2020, pp. 1634–1639.

[21] Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). https://doi.org/10.6028/nist.sp.800-181r1

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

6. Annex I. – Survey on Skills – Public

This annex contains the results of the public survey.

6.1. Self-assessment of the Respondent

Security expertise		Automotive expertise	Would you like to give feedback to the automotive cybersecurity engineer or manager skillset?
Automotive sector	Other sectors		
less than 3 years	less than 3 years	less than 3 years	Automotive cybersecurity Manager
less than 3 years		less than 3 years	Automotive cybersecurity Engineer
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Manager
more than 3 years		more than 3 years	Automotive cybersecurity Manager
more than 3 years		more than 3 years	Automotive cybersecurity Manager
more than 3 years		more than 3 years	Automotive cybersecurity Engineer
more than 3 years		more than 3 years	Automotive cybersecurity Manager
more than 3 years		more than 3 years	Automotive cybersecurity Manager
less than 3 years	more than 3 years	None	Automotive cybersecurity Manager
less than 3 years	less than 3 years	less than 3 years	Automotive cybersecurity Manager
less than 3 years	less than 3 years	more than 3 years	Automotive cybersecurity Engineer
less than 3 years	more than 3 years	less than 3 years	Automotive cybersecurity Engineer
less than 3 years		less than 3 years	Automotive cybersecurity Engineer
less than 3 years		less than 3 years	Automotive cybersecurity Manager
less than 3 years	None	less than 3 years	Automotive cybersecurity Engineer
less than 3 years	None	less than 3 years	Automotive cybersecurity Engineer
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Manager
more than 3 years		more than 3 years	Automotive cybersecurity Engineer
less than 3 years		more than 3 years	Automotive cybersecurity Engineer
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Engineer

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

6.2. Automotive Cybersecurity Engineer – Skills

Question: An automotive cybersecurity engineer should:	agree	disagree
be aware of the development interface agreement (cybersecurity-related technical agreement between supplier and customer	10	
be able to assess known vulnerabilities and weaknesses regarding required actions for a system throughout the complete lifecycle	10	
know the technical approaches towards software updates, including relevant cybersecurity risks and protective measures on the backend, during transport and in-the vehicle, and should be aware of potential impact to other disciplines	10	
know relevant automotive cybersecurity-related standards and should be aware of laws and regulation regarding automotive cybersecurity	9	1
be able to select and use suitable methods (Asset analysis, Attack tree analysis, Vulnerability analysis, threat analysis) and knows usable tools depending on the project progress and development stage to identify damage and attack scenarios and rate impact and likelihood to assess risks. For this, the engineer is aware of different risk rating schemes	8	2
know and be able to select appropriate measures to address risks and vulnerabilities on the system/software/hardware level.	10	
know about methods that are used for performing malicious actions (methods used, such as SQL Injection)	9	1
be able to identify and rate assets and consider the granularity of assets, the difference between assets/components/information, and how different stakeholder views lead to different assets	7	3
be able to derive cybersecurity requirements from cybersecurity goals (highest level cybersecurity requirements, directly related to risks) and define technical requirements on the system/software/hardware level to implement necessary risk treatment.	10	
know cybersecurity design patterns on system-level and be able to assign defense mechanism to a system design based on cybersecurity goals and integrate cybersecurity into a system design.	8	2
be able to identify cybersecurity critical software functions and data.	10	
know cybersecurity design patterns on the software level, security-related Libraries and OS features, and the principles of preventive and defensive programming and be able to integrate them into a software design	9	1
be aware of software-related security guidelines, checklists, and tools and be able to conduct cybersecurity-related code reviews	9	1
know different types of Hardware-based security (HSMs, cryptographic modules, secure cryptoprocessor) and their usage	9	1
know hardware related security guidelines, checklists, and tools and be able to conduct a cybersecurity-related hardware review (interfaces, tamper-protection, …)	9	1
be aware of different test methods and their suitability during the lifecycle (penetration testing, vulnerability scanning, fuzz testing, ...)		
know how to plan, perform and document an automotive cybersecurity assessment of the achieved cybersecurity of a product	7	2

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

6.3. Further Comments – Cybersecurity Engineer - Skills

ID	Name	Responses
1	anonymous	1.Know how on in vehicle networking and protocols like CAN, LIN, Flexray etc. 2.Know how on E/E Architecture types (central gateway based / Domain controller based) 3.Know how on wireless protocols such as WiFi, USB, etc. 4.Know how on Remote Diagnosis and security updates 5.Know how of Penetration testing and Fuzz testing.
2	anonymous	No.

6.4. Automotive Cybersecurity Manager – Skills

Question: An automotive cybersecurity manager should:	agree	disagree
know which cybersecurity roles an organization needs to define, based on its position in the supply chain and the responding organizational structures supporting the implementation of the cybersecurity, including relation to other disciplines like information security, functional safety, data protection, and privacy.	9	1
be able to plan, perform and document an automotive cybersecurity audit regarding the organizational processes and understand the underlying mapping of standards to organizational processes	8	2
know requirements regarding secure development tools and environment and necessary protection measures for physical and logical access for development, production, and maintenance environment	10	0
know how to plan how cybersecurity is addressed in a project (cybersecurity plan), including the documentation and argumentation regarding method and tool selection and the management of work products and artifacts through the project.	10	0
be aware of the need to protect cybersecurity work products and artifacts through the lifecycle and during an exchange with supply chain partners	9	1
be able to develop a development interface agreement (cybersecurity-related technical agreement between supplier and customer), including the organizational and technical interfaces regarding security during development, operation, and maintenance between customer and supplier.	9	1
be able to conduct the evaluation of cybersecurity competence as a supplier and customer (previous projects, audits, …)	8	2
be able to plan and execute a cybersecurity monitoring process, including the planning of the usage of internal and external information sources and organizational intern incident handling. In addition, the manager should be able to develop strategies regarding incident communication regarding supplier, customer, and authorities	7	3
know the standards and regulations regarding software updates and understand the interfaces to other disciplines regarding software update campaign planning and execution and the role of software updates in cybersecurity incident management.	9	1
know relevant threat lists (CVE, NVD, ...), weakness and vulnerability information sources (e.g. CWE), and domain-independent and domain-specific vulnerability disclosure and sharing groups and is able to utilize these sources to compile a list of relevant sources for a project.	8	2
know and understand the regulatory landscape regarding automotive cybersecurity (data protection laws (GDPR and similar), product liability law) and automotive cybersecurity engineering (regulations concerning usage of "hacker" tools)	10	
be able to define risk management and escalation processes, including decision criteria regarding risk acceptance, risk transfer, risk mitigation, and other risk treatment options	10	
be aware of different sources of cybersecurity risks (Backend technology cybersecurity risks, Supply chain cybersecurity security risks, Hardware, Software, Communication, Physical, cybersecurity risks)	9	1
be aware of different types of attacks (Single-step / multi-step / STRIDE categories)	9	1
be able to manage requirement traceability from risks to goals, requirements on system/software/hardware level to test cases, and test results.	9	1

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

6.5. Further Comments – Cybersecurity Manager - Skills

ID	Name	Responses
1	anonymous	For the cyber security manager role, there is some subtlety with the level for some of the skills mentioned. E.g. I wouldn't necessarily expect the security manager to be able to perform an audit but should know what is expected from an audit and how one is performed
2	anonymous	Knowledge does not necessarily being given by all managers, but based on their tasks.
3	anonymous	NA
4	anonymous	Be able to identify individuals to fulfill the roles and responsibilities for cybersecurity in the project.

6.6. Further Comments

ID	Name	Responses
1	anonymous	May be worth considering levels of competence. Such as supervised practitioner, practitioner, expert etc. Taking skills and experience into consideration. (I wonder too if the security engineer role shouldn't be tailored to one role alone, but rather consider what competence is required during the development (and other lifecycle) phases, e.g. during design, requirements definition etc
2	anonymous	I understand most of the skills are relevant, but few are not mandatory.
3	anonymous	N/A
4	anonymous	I feel there could be a 3rd role on security governance. A manager is not in charge of defining the strategy, but ensuring it is applied in projects. This is the role of a governance function.

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

7. Annex II. – Survey on Skills – Not Public

This annex contains the results of the not public survey.

7.1. Self-assessment of the Respondent

Security expertise		Automotive expertise	Would you like to give feedback to the automotive cybersecurity engineer or manager skillset?
Automotive sector	Other sectors		
None	more than 3 years	None	Automotive cybersecurity Engineer
less than 3 years	None	more than 3 years	Automotive cybersecurity Engineer
less than 3 years	None	more than 3 years	Automotive cybersecurity Manager
less than 3 years	None	more than 3 years	Automotive cybersecurity Manager
less than 3 years	None	more than 3 years	Automotive cybersecurity Manager
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Engineer
more than 3 years		more than 3 years	Automotive cybersecurity Manager
less than 3 years	less than 3 years	more than 3 years	Automotive cybersecurity Manager
less than 3 years	None	more than 3 years	Automotive cybersecurity Manager
None	more than 3 years	None	Automotive cybersecurity Manager
less than 3 years	None	more than 3 years	Automotive cybersecurity Engineer
less than 3 years	None	more than 3 years	Automotive cybersecurity Engineer
None	None	more than 3 years	Automotive cybersecurity Manager
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Manager
less than 3 years	less than 3 years	less than 3 years	Automotive cybersecurity Engineer
less than 3 years	less than 3 years	less than 3 years	Automotive cybersecurity Manager
	more than 3 years	None	Automotive cybersecurity Manager
None	less than 3 years	None	Automotive cybersecurity Engineer
less than 3 years	more than 3 years	less than 3 years	Automotive cybersecurity Manager
less than 3 years	more than 3 years	less than 3 years	Automotive cybersecurity Engineer
None	more than 3 years	None	Automotive cybersecurity Manager
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Manager
more than 3 years	more than 3 years	less than 3 years	
	more than 3 years	less than 3 years	Automotive cybersecurity Manager
	less than 3 years	more than 3 years	Automotive cybersecurity Engineer
None	less than 3 years	None	Automotive cybersecurity Engineer
None	more than 3 years	None	Automotive cybersecurity Engineer
None	None	less than 3 years	Automotive cybersecurity Engineer
None	more than 3 years	None	Automotive cybersecurity Engineer
less than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Engineer
None	None	None	Automotive cybersecurity Engineer
None	None	None	Automotive cybersecurity Manager
less than 3 years	None	more than 3 years	Automotive cybersecurity Manager
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Engineer
None	None	None	Automotive cybersecurity Engineer

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

None	None	None	Automotive cybersecurity Engineer
more than 3 years		more than 3 years	Automotive cybersecurity Manager
None	more than 3 years	None	Automotive cybersecurity Engineer
less than 3 years	None	more than 3 years	Automotive cybersecurity Engineer
less than 3 years	more than 3 years	less than 3 years	Automotive cybersecurity Engineer
less than 3 years	more than 3 years	less than 3 years	Automotive cybersecurity Manager
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Manager
more than 3 years		more than 3 years	Automotive cybersecurity Manager
None	more than 3 years	None	Automotive cybersecurity Engineer
None	less than 3 years	less than 3 years	Automotive cybersecurity Manager
less than 3 years	less than 3 years	less than 3 years	Automotive cybersecurity Manager
less than 3 years	less than 3 years	more than 3 years	Automotive cybersecurity Manager
less than 3 years	more than 3 years	less than 3 years	Automotive cybersecurity Engineer
less than 3 years	None	more than 3 years	Automotive cybersecurity Manager
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Engineer
None	less than 3 years	None	Automotive cybersecurity Engineer
less than 3 years	less than 3 years	more than 3 years	Automotive cybersecurity Manager
less than 3 years	less than 3 years	more than 3 years	Automotive cybersecurity Engineer
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Manager
more than 3 years	more than 3 years	more than 3 years	Automotive cybersecurity Engineer
None	None	more than 3 years	Automotive cybersecurity Manager
None	None	more than 3 years	Automotive cybersecurity Engineer
None	None	less than 3 years	Automotive cybersecurity Engineer
less than 3 years		more than 3 years	Automotive cybersecurity Engineer
None	None	more than 3 years	
less than 3 years	less than 3 years	more than 3 years	Automotive cybersecurity Manager

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

7.2. Automotive Cybersecurity Engineer – Skills

Question: An automotive cybersecurity engineer should:	agree	disagree
be aware of the development interface agreement (cybersecurity-related technical agreement between supplier and customer	29	1
be able to assess known vulnerabilities and weaknesses regarding required actions for a system throughout the complete lifecycle	32	
know the technical approaches towards software updates, including relevant cybersecurity risks and protective measures on the backend, during transport and in-the vehicle, and should be aware of potential impact to other disciplines	31	1
know relevant automotive cybersecurity-related standards and should be aware of laws and regulation regarding automotive cybersecurity	30	2
be able to select and use suitable methods (Asset analysis, Attack tree analysis, Vulnerability analysis, threat analysis) and knows usable tools depending on the project progress and development stage to identify damage and attack scenarios and rate impact and likelihood to assess risks. For this, the engineer is aware of different risk rating schemes	29	3
know and be able to select appropriate measures to address risks and vulnerabilities on the system/software/hardware level.	32	
know about methods that are used for performing malicious actions (methods used, such as SQL Injection)	29	2
be able to identify and rate assets and consider the granularity of assets, the difference between assets/components/information, and how different stakeholder views lead to different assets	22	9
be able to derive cybersecurity requirements from cybersecurity goals (highest level cybersecurity requirements, directly related to risks) and define technical requirements on the system/software/hardware level to implement necessary risk treatment.	30	2
know cybersecurity design patterns on system-level and be able to assign defense mechanism to a system design based on cybersecurity goals and integrate cybersecurity into a system design.	30	2
be able to identify cybersecurity critical software functions and data.	30	2
know cybersecurity design patterns on the software level, security-related Libraries and OS features, and the principles of preventive and defensive programming and be able to integrate them into a software design	30	2
be aware of software-related security guidelines, checklists, and tools and be able to conduct cybersecurity-related code reviews	27	5
know different types of Hardware-based security (HSMs, cryptographic modules, secure cryptoprocessor) and their usage	25	6
know hardware related security guidelines, checklists, and tools and be able to conduct a cybersecurity-related hardware review (interfaces, tamper-protection, …)	27	5
be aware of different test methods and their suitability during the lifecycle (penetration testing, vulnerability scanning, fuzz testing, ...)		
know how to plan, perform and document an automotive cybersecurity assessment of the achieved cybersecurity of a product	21	11

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

7.3. Further Comments – Cybersecurity Engineer - Skills

ID	Name	Responses
1	anonymous	11: The responsibility of identification and assets rating belongs to the security manager rather than engineer as it has no direct impact on the engineer's duties and the ability to support security related topics in their discussion especially when one takes into consideration that the role of a security manager exists.
2	anonymous	Planning activities are part of the Manager role. There have to be defined different focused competences for Systems, HW, SW. There will not be a general Engineer that covers all their aspects.
3	anonymous	Not sure if one need the ability to perform code reviews. This should be out-of-scope for most cybersec engineers and more a task for specialists. This also goes for in-depth hardware reviews. Furthermore, question 18 and 19 are identical.
4	anonymous	For a lot of the questions I would like to have a 1-5 scale, as most topics are relevant for engineers, but there is different in in-depth know-how required (system-level know-how vs. detailed security know-how)

7.4. Automotive Cybersecurity Manager – Skills

Question: An automotive cybersecurity manager should:	agree	disagree
know which cybersecurity roles an organization needs to define, based on its position in the supply chain and the responding organizational structures supporting the implementation of the cybersecurity, including relation to other disciplines like information security, functional safety, data protection, and privacy.	29	
be able to plan, perform and document an automotive cybersecurity audit regarding the organizational processes and understand the underlying mapping of standards to organizational processes	26	3
know requirements regarding secure development tools and environment and necessary protection measures for physical and logical access for development, production, and maintenance environment	23	6
know how to plan how cybersecurity is addressed in a project (cybersecurity plan), including the documentation and argumentation regarding method and tool selection and the management of work products and artifacts through the project.	27	2
be aware of the need to protect cybersecurity work products and artifacts through the lifecycle and during an exchange with supply chain partners	27	1
be able to develop a development interface agreement (cybersecurity-related technical agreement between supplier and customer), including the organizational and technical interfaces regarding security during development, operation, and maintenance between customer and supplier.	22	7
be able to conduct the evaluation of cybersecurity competence as a supplier and customer (previous projects, audits, …)	24	5
be able to plan and execute a cybersecurity monitoring process, including the planning of the usage of internal and external information sources and organizational intern incident handling. In addition, the manager should be able to develop strategies regarding incident communication regarding supplier, customer, and authorities	27	2
know the standards and regulations regarding software updates and understand the interfaces to other disciplines regarding software update campaign planning and execution and the role of software updates in cybersecurity incident management.	23	6
know relevant threat lists (CVE, NVD, ...), weakness and vulnerability information sources (e.g. CWE), and domain-independent and domain-specific vulnerability disclosure and sharing groups and is able to utilize these sources to compile a list of relevant sources for a project.	17	12
know and understand the regulatory landscape regarding automotive cybersecurity (data protection laws (GDPR and similar), product liability law) and automotive cybersecurity engineering (regulations concerning usage of "hacker" tools)	29	

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

Question: An automotive cybersecurity manager should:	agree	disagree
be able to define risk management and escalation processes, including decision criteria regarding risk acceptance, risk transfer, risk mitigation, and other risk treatment options	29	
be aware of different sources of cybersecurity risks (Backend technology cybersecurity risks, Supply chain cybersecurity security risks, Hardware, Software, Communication, Physical, cybersecurity risks)	27	2
be aware of different types of attacks (Single-step / multi-step / STRIDE categories)	22	7
be able to manage requirement traceability from risks to goals, requirements on system/software/hardware level to test cases, and test results.	24	5

7.5. Further Comments – Cybersecurity Manager - Skills

ID	Name	Responses
1	anonymous	Threat list knowledge is arguable from my point of view - since the manager has to ensure the conformity to a norm in the end - he has to make sure that the relevant threats were addressed. Relevant threats can be compiled by 3rd (without manager knowledge).
2	anonymous	Should also know: - know how to build and manage competence, e.g. through trainings - know how to create and maintain awareness, e.g. through campaigns - be able to create and leverage a network between expert teams (e.g. product security, IT security, supply chain security, FuSa, ...), to foster information sharing and to drive cross-team alignment and collaboration
3	anonymous	Diese Rolle wird extrem komplex, man muss sich entscheiden wie man abstrahiert: 1. Detaillevel (mE muss er nicht wirklich alle genauen CVEs wissen, das wäre eher einer operativen Rolel angemessen) 2. Ausgeglichenheit, zB Cybersecurity Manager (der tut) vs. Cybersecurity Auditor (der kümmert sich um Evaluierung). Diese beiden Rollenaspekte können divergierend sein (vgl. Operations Manager vs. IT Auditor).
4	anonymous	In my view it is important to have a clear borderline between the different roles: The topics I disagreed are about what is the focus of a cyber security manager in relation to a cybersecurity Engineer (Specialist) and what responsibility belongs to the whom. I also recommend distinguishing between a cybersecurity manager and an auditor, ass assessments require much more additional skills

7.6. Further Comments

ID	Name	Responses
1	anonymous	Interaction with Safety is very important -> Safety and Security Co-Engineering has to be taken into account.
2	anonymous	ADAS/AD Function Developer / Lead Researcher
3	anonymous	THX, a very relevant initiative/project!
4	anonymous	I would probably have used a Likert scale (from 0 to 5) rather than only "agree" or "disagree". Furthermore, the second question is not very clear (what do you mean with "automotive expertise"? is someone who is working in the automotive industry? or someone who simply uses a car? or someone who know very well cars as a "car lover"?)

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