# Automotive Cybersecurity Engineer

The Automotive Cybersecurity Engineer secures the product throughout the automotive development lifecycle. Their activities cover item definition, TARA (Threat Analysis and Risk Assessment), cybersecurity requirement derivation, system and software design, secure implementation, and verification/validation. They also contribute to audits, incident response, and supplier security assurance.

Responsibilities include integrating cybersecurity into vehicle ECUs, in-vehicle networks, diagnostics, and OTA systems, applying ISO/SAE 21434 and UNECE R155/156, and ensuring homologation evidence. The engineer supports organisational structures and processes for cybersecurity planning, risk assessment, vulnerability analysis, and incident management.

Essential competences span sector-specific (TARA, secure design, software/hardware security, HSM, penetration testing), digital (protocols, IDS, encryption), transversal (risk management, compliance, regulatory frameworks), soft (analytical thinking, problem solving, communication), and other organisational competences (planning, supplier security, processes and audits).

## ESCO Mapping

https://esco.ec.europa.eu/select-language?destination=/node/1

| ID | NAME | Concept URI |
|---|---|---|
| 2529.8 | cybersecurity risk manager | http://data.europa.eu/esco/occupation/7754d570-9519-48c2-b1c9-8e165f8bca0f |

## Context

| | |
|---|---|
| **EQF Level** | 7 |
| **Departments** | Production and Maintenance<br>R&D (Research and Development) |



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

## Sector Specific

| ID | Name | Type | Description | Level | ESCO |
|---|---|---|---|---|---|
| C279 | Perform threat analysis and risk assessment (TARA) | Skill | Identify assets, analyse threats and define cybersecurity goals.<br>▪ Conduct item definition<br>▪ Build attack trees<br>▪ Derive security goals<br>▪ Document TARA results | 3 | |
| C280 | System design and vulnerability analysis | Knowledge | Methods for analysing vulnerabilities in system architectures.<br>▪ Explain attack tree methods<br>▪ Identify weak design points<br>▪ Recommend secure patterns<br>▪ Support reviews | 2 | |
| C281 | Derive cybersecurity software requirements | Skill | Define and document secure software requirements.<br>▪ Identify critical functions<br>▪ Analyse risks to software<br>▪ Specify mitigations<br>▪ Provide to developers | 2 | |
| C282 | Integrate cybersecurity into software architecture | Skill | Embed cybersecurity considerations into SW architecture.<br>▪ Define secure design patterns<br>▪ Harden interfaces<br>▪ Align with ISO 21434<br>▪ Validate through reviews | 2 | |
| C283 | Secure software development | Knowledge | Standards and methods for secure coding and development.<br>▪ Explain MISRA/OWASP coding rules<br>▪ Describe defensive programming<br>▪ Support code reviews<br>▪ Monitor vulnerabilities | 2 | |
| C284 | Cybersecure hardware and firmware design | Knowledge | Principles for integrating HSMs and secure firmware in ECUs.<br>▪ Explain HSM architectures<br>▪ Identify secure environments<br>▪ Describe crypto services<br>▪ Support firmware resilience | 2 | |
| C285 | Cybersecure software testing | Knowledge | Methods for testing secure coding and integration.<br>▪ Explain unit/integration test needs | 2 | |



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

| ID | Name | Type | Description | Level | ESCO |
|---|---|---|---|---|---|
| | | | ▪ Apply ISO 21434 guidance<br>▪ Detect vulnerabilities in testing<br>▪ Document test evidence | | |
| C286 | Verify hardware security modules | Skill | Perform verification of HSM functions in ECUs.<br>▪ Validate key storage<br>▪ Test crypto ops<br>▪ Verify compliance with standards<br>▪ Report results | 2 | |
| C287 | Verify cybersecurity at system level | Skill | Execute system-level security verification.<br>▪ Define scope of tests<br>▪ Run EOL security tests<br>▪ Analyse system logs<br>▪ Document audit results | 2 | |
| C288 | Perform penetration testing | Skill | Conduct penetration tests with internal/external teams.<br>▪ Define scope and goals<br>▪ Simulate realistic attacks<br>▪ Document vulnerabilities<br>▪ Support mitigation plans | 3 | |

## Other Competences

| ID | Name | Type | Description | Level | ESCO |
|---|---|---|---|---|---|
| C322 | Legal and homologation aspects | Knowledge | Regulatory frameworks relevant to vehicle cybersecurity.<br>▪ Explain UNECE R155/156 requirements<br>▪ Identify homologation impacts<br>▪ Monitor new regional standards<br>▪ Support compliance activities | 2 | |
| C323 | Organisational structures | Knowledge | Organisational frameworks for managing cybersecurity.<br>▪ Describe cybersecurity governance<br>▪ Explain roles and responsibilities<br>▪ Identify interfaces across teams<br>▪ Support audits of processes | 2 | |
| C324 | Cybersecurity planning | Skill | Plan cybersecurity tasks across the vehicle lifecycle.<br>▪ Define security objectives | 2 | |



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

| ID | Name | Type | Description | Level | ESCO |
|---|---|---|---|---|---|
| | | | ▪ Allocate resources<br>▪ Monitor implementation<br>▪ Align with corporate strategy | | |
| C325 | Perform threat and vulnerability analysis | Skill | Execute threat and vulnerability analysis at product/system level.<br>▪ Collect threat intelligence<br>▪ Identify vulnerabilities in ECUs<br>▪ Evaluate exploit likelihood<br>▪ Recommend countermeasures | 3 | |
| C326 | Manage cybersecurity processes and audits | Skill | Apply and audit processes for cybersecurity assurance.<br>▪ Define audit scope<br>▪ Document evidence<br>▪ Support external auditors<br>▪ Recommend process improvements | 2 | |
| C327 | Manage incident response | Skill | Coordinate actions in case of cybersecurity incidents.<br>▪ Monitor alerts<br>▪ Escalate incidents<br>▪ Support containment<br>▪ Document lessons learned | 3 | |
| C328 | Manage supplier security | Skill | Ensure suppliers fulfil cybersecurity requirements.<br>▪ Define requirements in contracts<br>▪ Review supplier compliance<br>▪ Conduct audits<br>▪ Escalate risks to project teams | 3 | |



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.