ISO/SAE 21434 SUPPLIER CYBERSECURITY KIT · WORKED EXAMPLE OVERVIEW

Ardel TCU-40: one telematics unit, all 15 modules

Free overview · 4 pages · Release 2026-11 v1.0 · Özer Koray Akdemir

Ardel Telematics GmbH, Velmora Automotive AG and all people, documents, vulnerabilities and cases in the example are fictional.

Vehicle manufacturers must manage the cybersecurity risks of their suppliers (UN Regulation No. 155), so ISO/SAE 21434 evidence now arrives in every request for quotation. The kit's worked example follows one supplier from the first questionnaire to the series release, the first vulnerabilities in the field and the customer's audit. This overview tells the story in four pages.

The component

The TCU-40 is a telematics control unit for the V-series of a passenger car manufacturer: remote services, stolen-vehicle tracking and software updates over the air. It sits between the mobile network and the vehicle, so every interface is a way in.

Interface	What it is for	What protects it
LTE to the manufacturer's back end	Remote services, updates, tracking	Mutual TLS with a device key that never leaves the HSM
CAN FD and Ethernet to the gateway	Forwarding authorised requests	Request filtering; SecOC keys used only inside the HSM
Diagnostics	Workshop and production	Authentication before any write, routine or flash service
USB service port, JTAG pads	Service flashing, board test	Flashing only when the service back end authorises it; JTAG fused at end of line

15
modules filled in, from applicability to the own-product CRA file

45
completed files: Word, PDF copies and Excel workbooks

18
threat scenarios rated and treated in the component TARA

30/30
refined requirements verified at the series release

Why the customer asks

Velmora's type approval depends on its cybersecurity management system, and that system must cover Ardel. So Velmora asks for organisational evidence, a signed interface agreement, a component TARA consistent with its own, verification evidence per sample, vulnerability notification for the support period, secure production and a cybersecurity case at every release. The example produces each of these, in the order Velmora needs them.

THE CENTRAL DECISION

Agree who does what before development starts

The interface agreement (SK-04) assigns 42 activities between Velmora and Ardel, each with exactly one party responsible. Most later disputes are settled by this matrix.

Activity (excerpt)	Velmora	Ardel
Item definition and vehicle-level TARA	**R+A**	**S**
Component TARA	**C**	**R+A**
Vulnerability analysis of the component	**C**	**R**
Treatment decision for vehicles in the field	**A**	**R**
Incident response	**R+A**	**S**
Signing of the component software; update campaigns	**I; R+A**	**R+A; S**

R responsible, A accepts, S supports, C consulted, I informed. The full matrix and the notification times are in EX_SK-04.

One threat, followed through the documents

TS-02
Code execution in an LTE-facing service

SK-07

CG-01, CG-03
Authenticated requests only; authentic software

SK-08

SR-01
TLS 1.3 only, mutual authentication through the HSM

SK-09

TC-01, PT-01
Test and penetration test passed

SK-10, SK-13

V-01
TLS library flaw in the field: notified in 2 working days, fixed in 1.0.6

SK-11

How the file grew

When	What happened
January 2027	Applicability record, organisational evidence and the answer to Velmora's questionnaire, with dated gap actions
February to April 2027	Interface agreement signed; plan; component definition; TARA; goals, claims and concept accepted by Velmora
July to September 2027	Refined specification; B-sample verification with four weaknesses; vulnerability management in operation
October 2027 to January 2028	Three vulnerabilities and one incident handled; C-sample software; the Fleet variant's CRA file and declaration
April to June 2028	Pilot production run; penetration test; independent assessment; series release; gap assessment before Velmora's audit

WHAT THE EXAMPLE TEACHES

Six lessons

1. Answer the questionnaire honestly

Ardel answered "partly" where it was partly ready and gave each gap an owner and a date. The gap assessment seventeen months later shows all of them closed, with evidence: 10 gaps closed, two new ones open.

SK-03, SK-14

2. Assumptions become requirements

Developed before the customer's item was known, the component rested on documented assumptions. Reconciling them with Velmora's TARA turned one of them, diagnostic authentication, into a requirement of the component.

SK-06, SK-08

3. Independence is checked, not assumed

The first plan made the quality manager both assessor and owner of the production control plan. The conflict was found and the production manager took the plan.

SK-05, SK-13

4. A weakness you cannot fix yet is handled in the open

The modem firmware signature check was not ready for the B-sample. It was accepted with a rationale, a field vulnerability depending on it was moved to the C-sample by an agreed deviation, and both closed with software 1.1.0.

SK-10, SK-11, SK-12

5. Production can undo the design

In the pilot run one unit failed the JTAG lock check after its certificate had been issued. It was scrapped and its certificate revoked (2028-04-11); the station was corrected and the day's units rechecked.

SK-12

6. The same board, two laws

Built into Velmora's cars, the TCU-40 is outside the Cyber Resilience Act. Sold by Ardel to fleet operators, it is inside. The 21434 work already covered 11 of 22 essential requirements; the 11 others were closed before the declaration.

SK-01, SK-15

THE KIT

What is in the ISO/SAE 21434 Supplier Cybersecurity Kit

Module	Template	Module	Template
SK-01	Role and Applicability Record	SK-09	Refined Cybersecurity Specification
SK-02	Organisational Cybersecurity Evidence	SK-10	Integration and Verification Report
SK-03	Supplier Capability Response	SK-11	Vulnerability Management and Incident Response
SK-04	Cybersecurity Interface Agreement	SK-12	Production, Updates and End of Support
SK-05	Cybersecurity Plan	SK-13	Cybersecurity Case, Assessment and Release
SK-06	Component Definition	SK-14	Gap Assessment and Audit Readiness
SK-07	Component TARA	SK-15	Own Products: Regulatory File and CRA Bridge
SK-08	Goals, Claims and Concept		

Editable Word templates with PDF copies, Excel workbooks with built-in checks, a guide for every module, the complete worked example, a Start Here guide and the licence. The files open in Microsoft Office or LibreOffice and stay on your systems. ISO/SAE 21434 is cited by clause and work product number only; you need your own copy of the standard.

See the full kit at get21434ready.com/kit
One payment per company licence, no subscription. Free updates until at least 31 December 2027, for example when the second edition of ISO/SAE 21434 is published.

This overview refers to ISO/SAE 21434:2021 by clause number only and reproduces none of its text. It is not affiliated with or endorsed by ISO or SAE International. It is not legal advice. Ardel Telematics GmbH, Velmora Automotive AG and their products are fictional. © 2026 Özer Koray Akdemir. You may share this overview unchanged.