CySe rules for suppliers and goods

SOR Libchavy spol. s r.o.
Dolní Libchavy 48, 561 16 Libchavy
IČ: 15030865, DIČ: CZ15030865
Tel.: +420 465 519 411, sor@sor.cz
www.sor.cz

Purpose

This regulation is a summary of the requirements of SOR Libchavy spol. s r.o. for suppliers and goods that have been evaluated as CySe relevant. The purpose is to meet the requirements of the CSMS (Cyber Security Management System) according to UNECE R 155 and the SUMS (Software Update Management System) according to UNECE R 156.

List of terms

CySe	Cyber Security
CSMS	Cyber Security Management System
SUMS	Software Update Management System
CySe component	CySe relevant goods (control units, transmitters, sensors,...)
ECU	Electronic Control Unit

Definition of CySe relevant goods (components)

CySe relevant goods are defined by the SOR. Generally, this refers to any goods that are relevant from the perspective of cybersecurity. Goods are considered CySe-relevant if...

a. It is an EE component controlled by an ECU using a data bus and at the same time
b. it affects human health or life or the environment or confidential information; or
c. a software update can be performed on the component.

CySe requirements for suppliers

Prior to the first delivery of a CySe component and as part of the periodic supplier evaluation, the SOR supplier shall provide the following documentation to demonstrate a sufficient approach to ensuring the cybersecurity of their organisation:

1st a CySe certificate of the organisation, e.g. **UNECE R 155, ISO 27001, ISO 21434** or **TISAX** issued by an authorised person; or
2nd proof of the organisation's classification as an obliged person under Regulation Directive (EU) 2022/2555 of the European Parliament and of the Council - abbreviated as "**NIS2**"; or
3rd a completed **CySe Supplier Questionnaire** containing an affidavit. SOR reserves the right to verify the veracity of the affidavit by conducting a customer audit of the supplier;
4th and at the same time **CySe DIA Cybersecurity Interface Agreement**, or its own version of the agreement.

During the annual evaluation of suppliers, it is verified that the supplier still meets the above-mentioned conditions. On behalf of SOR, this evaluation and contact with the supplier is carried out by the Purchasing Department (in cooperation with the CySe Manager).

The Supplier is further obliged to:

5th immediately notify the SOR of the occurrence of a serious **vulnerability** or **cyber incident** or the **release of a critical update** (potentially affecting passenger security) to: notification@sor.cz

SOR Libchavy spol. s r.o.
Dolní Libchavy 48, 561 16 Libchavy
IČ: 15030865, DIČ: CZ15030865
Tel.: +420 465 519 411, sor@sor.cz
www.sor.cz

CySe requirements for purchased components

If it is a CySe component, the supplier is obliged to deliver:

1. **CSMS certificate** for the goods (UNECE R 155, ISO21434, TISAX) issued by an authorised person, if any;
2. current results of **TARA** analysis (according to ISO/SAE 21434 methodology or equivalent), at least the resulting **risks** including **corrective measures** that mitigate their negative impacts;
3. current **penetration test results** including implemented fixes;
4. clearly **identify the component** if it is intended for testing or development purposes;
5. **list of CAN queries** to which the ECU responds via CAN:
   - ECU hardware version (model number nebo product number),
   - ECU serial number,
   - software version,
   - Integrity Validation Data;
6. the end date of support for the goods (development and production of the goods/components).

If the supplier is unable to deliver point 2, the cooperation of the SOR (Director of Purchasing and Logistics, CySe Manager) and the supplier's technical experts is required. For this, the supplier shall prepare in advance:

a. technical documentation of the component, including block diagram, communication interface and operating states,
b. description of the security mechanisms and measures used,
c. ensuring sufficient staffing and professional capacity for consultations and proposing their timing.

Requirements for software

If it is a CySe component, the supplier is obliged to:

1. **send information about any software update** to email: swupdate@sor.cz, information must include:
   - hardware version of the control unit;
   - software version, possibly dataset version or description of parameter configuration;
   - the purpose and extended description of possible influence on homologation parameters;
   - what vehicle systems or functions may be affected.
2. for production vehicles:
   - use only the **OBD socket and the UDS protocol** for CAN diagnostics and software updates,
   - **do not use remote OTA (Over The Air) software updates** and update the software without the presence of an SOR technician.
3. provide **instructions for diagnostic software** and safe **procedures for updating the software** or parameterizing the ECU,
4. provide secure access to **current versions of the software,**
5. clearly **differentiate software** intended for mass production from unsafe or test software,
6. ensure the **immutability of the software during the upgrade process** (e.g. encryption, e-signature, checksum if applicable, verification of origin and immutability, etc.),
7. deliver **software test results** (e.g., CVE and CVSS and comparison to nvd.nist.gov);
8. use **encryption** for both components and software:
   - by using secure **cryptographic protocols, ciphers, and hashing functions** without known vulnerabilities according to:
     - NÚKIB or
     - NIST and
     - regularly (at least once a year) compare the status;
   - in case of use of other (unapproved) encryption algorithms, SOR must be informed.