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. In general, these are any goods that are relevant from a cybersecurity perspective. Goods are 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 supplier shall provide the following documentation to the SOR to demonstrate that its organisation has a sufficient approach to cybersecurity:

1. a CySe certificate, e.g. **ISO 27001, ISO 21434, TISAX** issued by an authorised person; or
2. a completed **CySe Supplier Questionnaire** containing an affidavit; and
3. **CySe Interface Agreement CIA**, or a customized version of the agreement.

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

Requirements for CySe components

In the case of a CySe component, the supplier is obliged to:

1. 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 the following email: notification@sor.cz;
2. provide up-to-date CySe documentation:
   - **unit/system description** (including SBOM),
   - current **TARA** of the unit/system,
   - description of **implemented measures** (existing features = secured by design, additional = additional mitigations),
   - reports on testing of measures (**penetration tests**);

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

3. unambiguously **identify the component** if it is intended for testing or development purposes;
4. a **list of CAN queries** to which the ECU will respond via CAN:
    - ECU hardware version (model number or product number),
    - ECU serial number,
    - software version,
    - Integrity Validation Data;
5. **End date of support** of goods (development and production of goods/components).

If the supplier is not able to deliver point 2, the cooperation of the SOR (KB 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 of the wiring, communication interface and operational states,
b. a description of the security mechanisms and measures used,
c. the provision of sufficient staff and expertise for the consultation and a proposal for its timing.

Recommendations for developing “CySe ready” components:

6. **technical measures**:
    - disable/lock **unused interfaces**,
    - disable/lock **debug**,
    - **encryption**
        - potentially high impact communications (e.g. high impact from TARA),
        - data transfer (SW, FW, parameter changes, logs) using a diagnostic tool,
        - data transfer between the component and the backend server,
        - the level of encryption compared to the nist.gov or nukib.gov.cz recommendations,
    - **user authentication with a certificate** (or 2-factor authentication)
        - for login and communication of the diagnostic tool,
        - for backend server login and communication,
    - other technical measures such as: secure boot, Data Integrity Validation, etc.;
7. Comment on all points of **Annex 5 of UN Regulation No. 155**,
    - has been applied / not applied and why.

SW requirements

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

1. **send information about any software update** to email: swupdate@sor.cz, the information must include:
    - HW version of the control unit,
    - SW version, or dataset version or description of parameter configuration,
    - purpose and extended description of possible influence on homologation parameters,
    - what vehicle systems or functions may be affected;
2. for production vehicles, **do not use OTA (Over The Air) SW update** (update the software remotely without the presence of an SOR technician);
3. provide **instructions for diagnostic software** and safe **procedures for updating software** or ECU parameterization;
4. provide secure access to **current ECU SW versions,**
5. clearly **distinguish SW** intended for mass production from unsafe or test SW,
6. ensure the **immutability of the SW during the upgrade process** e.g. by means of encryption and certificate verification (mentioned above).