CECIP Position regarding the recast of the WELMEC Guide 7.2

2 November 2022

The essential requirements of both the NAWI Directive and the MI Directive contain essential requirements that relate to software. These requirements are generic in nature and further detailed software requirements can be found in the relevant harmonised standards, normative documents and the WELEMC guides published by working group 7. These documents offer guidance and technical solutions to enable manufacturers to meet the essential requirements as respects software.

WELMEC WG7 is undertaking a review of the present guides, focusing on a recast of the Guide 7.2. This position paper outlines both the general and specific matters that CECIP would like to be considered when undertaking the recast.

Current guides complicated and not futureproof

The present guides have been developed in a piecemeal nature with extra requirements being added to pre-existing obligations. This has led to the document being overly complicated and subject to inconsistent interpretation in different Member States. This in turn has made it difficult for manufacturers to be confident that any software that is submitted for approval will be treated consistently.

The recast of the existing guide 7.2 is supported by CECIP and is regarded as fundamental to ensuring that manufacturers have a consistent and transparent framework for the development of software in the future.

General principles regarding future changes for the Guide 7.2

New innovations within weighing instruments bring significant benefits for society and industry. However, the increasing divergence between the rapid technical advances and the regulatory view of different Member States often hamper developments and create an unnecessary burden on the development of the market. A pertinent example would be the development of “standalone” weighing systems that are not fixed to one specific hardware module. The present frameworks do not permit this, but it is technically possible and demanded by the market. CECIP are favour of ensuring a simple and transparent method of ensuring software controls are appropriate for all stakeholders and maintain confidence in the market.

CECIP would like to ensure that the recast of the Guide 7.2 aims at:

- Reducing limitations on innovation and technical development
- Fostering greater cooperation between notified bodies with different interpretations.
- Reducing market distortions due to more consistent interpretations of WELMEC guides
- Creating a facility for the development of procedural control of software development

Specific issues about the Guide 7.2

The existing WELMEC Guide 7.6 introduces the notion of the risk assessment of software as a tool to ensuring that relevant obligations are met. These concepts are based on the ISO/IEC 27005 and support these ideas being reflected in the Guide 7.2. CECIP are very supportive of this general notion and its continued development. CECIP do however wish to see a more subtle distinction in the assessment of risk between different instrument types. This will ensure the application of more transparent risk assessments for different type of instruments is more reflective of the risks to be found in the marketplace.

CECIP believe that this can be achieved by a more sophisticated understanding of attacker motivation and the quantifying of the empirical risk relating to this. In conjunction with the existing processes outlined in Guide 7.6 we would like to see this as an intrinsic part of the risk assessment process. The present guide successfully considers that if an attack is possible, but the likelihood of an attack occurring varies with different instrument types. CECIP would be of the view that software attacks are very unlikely on automatic and non-automatic weighing instruments.

The rationale behind this position is.

- For automatic and non-automatic weighing instruments the result of a measurement can be repeated more easily than other types of weighing and measuring instruments such as electricity or gas meters. This may result in any alteration to software being easily identified and consequently reduce the motivation for an attack on that instrument.
- For both automatic and non-automatic weighing instruments the load and the sensors are more accessible than other types of instruments. If a potential attack is going to occur, it would appear more likely that a direct method would be chosen rather than an attack on the instrument's software.
- The level of expertise to undertake many of the attack vectors is greater than assumed which would also reduce the risk of attack
- Perhaps the most significant argument is the lack of empirical evidence of the occurrence of the attacks on weighing instruments. As far as CECIP are aware there are no recorded examples of a malicious attack on the legally relevant software of a weighing instrument and the assessed risk most reflect this.