DOI 10.5162/sensoren2024/C5.1

Towards Technology-Independent Software Requirements in Legal Metrology

Marko Esche[1], Martin Nischwitz[1], Felix Salwiczek[1], Peter Eekhout[2]
[1]Physikalisch-Technische Bundesanstalt, Department 8.5 „Metrological IT“, Abbestr. 2-12, 10587 Berlin, Germany
[2]Dutch Authority for Digital Infrastructure, Department “Admission and Standardisation”, Emmasingel 1, 9726 AH Groningen, The Netherlands

Abstract

Current practice for software examination of measuring instruments subject to legal control is based on requirements for physically separable instrument components. This approach has resulted in frequent updates to harmonized software requirement documents in recent years, while simultaneously putting serious strain on resources at standards setting bodies, such as the European Cooperation in Legal Metrology WELMEC. With the aim of establishing a future-proof method for software examination that does not restrict the use of new technologies and requires fewer revisions, an asset-based approach for software requirements is presented. This approach is based on a previously established risk assessment method based on ISO 27005 and ISO 18045 vulnerability analysis. With the help of several practical examples the applicability and fitness for purpose of the new approach is investigated and compared with the current component-based method for software examination. Based on this comparison, suggestions for further improvement of the method are derived.

Keywords: Legal Metrology, Conformity Assessment, Software Examination, Requirements, Risk Assessment

Introduction

A sizeable portion of measuring instruments used in the European Union (EU) for commercial transactions, such as utility meters, taximeters and length measuring instruments, are subject to legal requirements laid down in the Measuring Instruments Directive (MID) [1] or the Non-Automatic Weighing Instrument directive [2]. This practice is usually referred to as Legal Metrology. Among these requirements are metrological requirements regarding measurement errors but also software requirements which aim to ensure securing and protection for certain assets against inadmissible influence. Any measuring instrument that falls under the scope of Legal Metrology has to undergo a conformity assessment procedure in cooperation with a so-called Notified Body before being made available on the common EU market. Germany’s national metrology institute Physikalisch-Technische Bundesanstalt (PTB) is one such Notified Body. Measuring instruments are also regularly checked to ensure compliance when they are put on the market and while they are in use. The Dutch Authority for Digital Infrastructure (RDI) is one market surveillance and inspection body tasked with monitoring measuring instruments under the scope of Legal Metrology.

Similar to the aforementioned separation of requirements for metrological and software characteristics, conformity assessment itself is usually also split into metrological tests and software examination, which then produce separate test reports which are combined by an evaluator who determines if a certificate can be issued. To assist the software examination, the European Cooperation in Legal Metrology (WELMEC) has been publishing consecutive versions of the WELMEC 7.2 Software Guide [3] since 2004. This guide transfers the essential requirements of the MID to practically implementable requirements and also offers the manufacturers corresponding “acceptable solutions” as exemplary implementations. All versions of the guide have been identified by the EU commissions working group “Measuring Instruments” (wgMI) as normative documents which can be used to demonstrate compliance of a measuring instrument’s software with the essential requirements of the MID Annex I [4]. In recent years, the guide was revised on an almost yearly basis to correct

editorial and technical errors and adapt or specify additional requirements to address new technologies. In order to pave the way for speedier implementation of yet unknown technologies, the responsible WELMEC Working Group 7 “Software” set up a drafting group in March 2022 to recast the existing software guide.

Since its initial conception in 2004, the WELMEC 7.2 Software Guide has always consisted of six central parts: a basic requirement set for measuring instruments using build-for-purpose hardware and software, another basic requirement set for measuring instruments using universal devices such as tablets and PCs and four extensions for long-term storage of measurement data (Extension L), transmission of measurement data (Extension T), software separation (Extension S) and software download (Extension D). Most recently, requirements for operating systems (Extension O) were separated from the basic requirement set for measuring instruments using universal devices and introduced as a separate Extension O. As such, the guide currently mimics the setup of classical, fully integrated measuring instruments [5], where dedicated physical components containing clearly identifiable software modules fulfil specific requirements. See Figure 1 for a complex measuring system using said components.

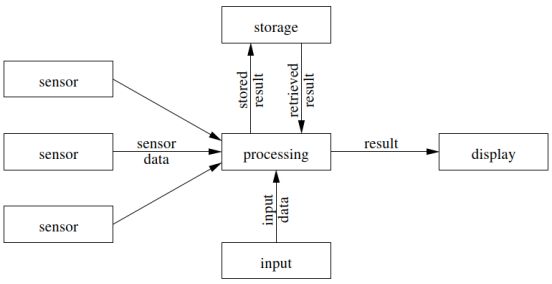

Fig. 1: Distributed measuring instrument processing data originating from multiple sensors. [5]

This approach offers very little flexibility with regard to applying certain securing and protection requirements when technical deviations (such as cloud computing or web-based indication solutions) come into play, e.g., it is typically not possible to secure the operating system of a cloud server against intentional manipulation by the cloud provider but the component-based approach does not offer means to establish if such a protection is indeed necessary. By using a risk-based approach, it might be possible to establish that only protection against manipulations of specific assets derived from the essential requirements in the MID has to be ensured.

Risk assessment has been a mandatory part of most conformity assessment procedures in the MID since 2004. To aid manufacturers and conformity assessment bodies with conducting risk assessments (see [6][7]) WELMEC has published a harmonized risk assessment method, see WELMEC 7.6 Risk Assessment Guide [8]. Whereas risk assessment currently plays the role of an add-on to classical software examination, it is proposed to use it as a basic tool for software examination in the recast guide: Requirements in Guide 7.2 will be rewritten and restructured to enable a risk-based software examination. For that purpose, the Guide will contain a chapter on general protection and securing of the identified assets. To evaluate if the solutions of the manufacturer are adequate to prevent inadmissible influence under certain circumstances such as data transmission, data storage, usage of operating systems, etc., a risk assessment is carried out The responsible drafting group has also proposed to separate the aforementioned acceptable solutions from Guide 7.2 and move them to two “living” guides 7.3 and 7.4.

The main contribution of the paper will be to explain this new approach and validate it using a number of generic measuring instrument examples. These will also be used to evaluate the applicability of and potential remaining issues with the anticipated recast guide and illustrate how established acceptable solutions and risk assessment can work together to ensure the applicability of the revised software guide to arbitrary technologies. The remainder of the paper is structured as follows: The next section briefly describes the current component-based approach to software examination as laid out in the current WELMEC 7.2 Software Guide [3]. Section 3 revisits the previously published risk assessment method used as a foundation for the new asset-based approach. The approach itself is introduced and explained in detail in Section 4. Afterwards, an attempt is made to validate the applicability of the new approach using a number of generic measuring instrument examples in Section 5. Finally, Section 6 summarizes the paper and provides suggestions for further work.

Component-Based Requirements in WELMEC Guide 7.2: 2023

The central paradigm behind the current state of the art in software examination for regulated measuring instruments, i.e., the WELMEC 7.2 Software Guide, is a combination of protection and securing requirements for physically

separable and locatable components: For each component individually, the guide imposes a combination of protection and securing requirements for software, measurement data and parameters. Regardless of the fact whether basic requirement set P for built-for-purpose devices or requirement U for universal devices is used, this encompasses measures that make changes in software, measurement data and parameters evident, i.e., protection measures for intentional and accidental changes, together with securing measures to prevent inadmissible influence. Additionally, interface protection is prescribed by the Guide in requirements P4, U4. This interface protection aims to prevent influence on software, parameters and measurement data through physically available interfaces, such as serial, Ethernet or Bluetooth ports, regardless of the fact if additional protection and securing measures exist within a physical component.
Should measurement data be stored within a component, the additional Extension L for long-term storage applies. The extension mandates a minimum content of stored datasets and requires that any dataset can be traced back to the originating component and the corresponding measurement. Simultaneously, protection measures are demanded to detect accidental and intentional changes or loss of datasets in storage. This automatically implies that these protection measures are checked upon retrieval of stored data (see requirement L6 in [3]).
Similarly, another extension exists for the transmission of measurement data between physically separable components. This Extension T again prescribes a minimum content for transmitted datasets and mandates protection requirements to detect unintentional or intentional changes or loss of data during transmission. In addition, requirements exist for the checking of protection measures by the receiver.
It should be noted that a distinction is made in [3] between so-called legally relevant and not legally relevant components: Any component that is needed to fulfil or can influence compliance with the essential requirements of the MID [1] is considered to be legally relevant. Following the above description, this implies that retrieval software for stored data and receiver for transmitted data are legally relevant. Any component that does not fulfil either criterion is deemed to be not legally relevant and is disregarded during software examination. It follows that any communication with a not legally relevant component must be done via a protective interface.

The application of the basic requirement sets and extensions to a complex combined measuring instrument for weight and length is illustrated in Figure 2.

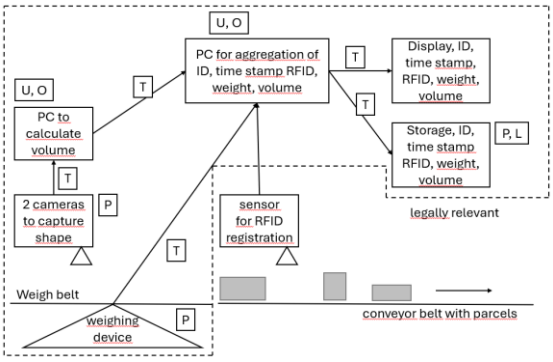

Fig. 2: Combined measuring instrument for dimensions and weight of parcels on a conveyor belt. The letters in boxes next to the individual components and communication connections indicate the applicable requirement sets of the WELMEC 7.2 Software Guide.

The instrument contains two sensor inputs, namely cameras for optical length measurements, and an automatic weighing instrument to measure the weight of parcels. In addition, an RFID sensor is used to provide additional identification information for parcels apart from their ID number and a timestamp. The latter can be considered not-legally relevant. This is denoted by the dashed box for the legally relevant part of the instrument in Figure 2.
It should be noted that the described structure and requirements of the WELMEC 7.2 Software Guide have been applied to thousands of measuring instruments over the past twenty years and should be considered as proven-in-use.

Software Risk Assessment Based on ISO 27005 and ISO 18045

Since 2014, the MID [1] requires manufacturers of measuring instruments to submit an analysis of the risks associated with their instrument during conformity assessment. To aid manufacturers with the risk assessment for software aspects, PTB developed and published a risk analysis method [6][7], which was later adopted and harmonized in a separate guide WELMEC 7.6 Risk Assessment for Measuring Instruments. [8] This method consists of three main phases, namely risk identification, risk analysis and risk evaluation.

During risk identification, assets to be protected are defined. In the context of the Risk Assessment Guide [8], these are software, parameters, measurement data, records and indication. The guide demonstrates that the MID requires three security properties, namely integrity, authenticity, and availability, for each asset mentioned. Based on these properties, generic threats can be formulated, e.g., 'An attacker manages to invalidate integrity of a stored record.' In principle, each combination of asset and security property needs to be reflected by a threat.

During risk analysis, each threat is assigned at least one technical attack vector that details how the threat might be realized for a specific measuring instrument, e.g., 'An attacker tries arbitrary password combinations to obtain administrator privileges on a measuring instrument and subsequently deletes all protected stored records.' For each such attack vector, a vulnerability analysis in accordance with ISO 18045 is used to assign point scores to the attack for needed time, expertise, knowledge, window of opportunity and equipment. The resulting sum score is then mapped to a probability score between 1 and 5. In addition, the potential impact of the attack is reflected by an impact score, which takes on a maximum value of 1 if all future or past measurements are affected by an attack. If several alternative attack paths exist to realize a threat, Attack Probability Trees [7] can be used to combine partial attacks or to determine the most likely attack vector. The product of impact and probability score finally yields the numerical risk associated with the original threat.

In the risk evaluation phase, the assessor has to check if the risks resulting from each score are acceptable, i.e. if the calculated risk score is below a predefined threshold. In case not all risks have been adequately mitigated by the instrument manufacturer's chosen design, the implementation needs to be amended and the risk assessment is repeated.

See the original publication [7] for a more detailed explanation with illustrative examples.

Proposal for Asset-Based Software Requirements

The harmonized risk assessment method published as guide WELMEC 7.6 Software Risk Assessment for Measuring instruments extends the originally described list of assets from [7] to also include inscriptions accompanying the indication, since these might be realized by software, too. As described in the introduction, the asset-based approach attempts to keep the current practice of using established acceptable solutions to demonstrate compliance with certain requirements while at the same time requiring no more frequent updates to the requirements themselves and opening said requirements for potential future technological solutions, too. The responsible WELMEC WG7 drafting group has determined three essential building blocks for the approach:

Firstly, currently established acceptable solutions for component-based requirements will be moved to a separate Guide 7.3.

Secondly, each acceptable solution will be subjected to a risk assessment by WELMEC WG7, which will document the outcome for future reference and to ensure comparability between technical solutions for a certain requirement.

Thirdly, the risk assessment method described above will be referenced in Guide 7.2 as an option to demonstrate that the level of protection realized by a new technological solution is comparable to other solutions for the same risk class.

To this end, all technical component-based requirements in Guide 7.2, e.g., interface protection in requirements P4/U4, will be replaced by the following new umbrella requirement for the six assets, "All instances of the assets in the instrument shall be adequately secured and protected against changes and inadmissible influences to ensure availability, integrity, and authenticity."

The envisioned effect of this separation is threefold: Guide 7.2 will remain the central requirement document but will become more technologically independent which is expected to promote technical progress because it is clear at the outset which requirements new innovations must meet. Frequent revisions of the Guide 7.2 requirement document should also no longer be necessary. Guides 7.3 (acceptable solutions) and 7.4 (complex configurations) can dynamically change if new acceptable solutions are put forward or old solutions become obsolete. The existing risk assessment procedure in Guide 7.6 can be kept and will be used to assess new technological solutions for which no acceptable solutions exist. In this manner, it is expected that examination practice for classical fully integrated instruments that implement the acceptable solutions will not change, while implementations using other solutions or new technologies can be evaluated using risk assessment to check the implementations' resistance to certain threats. Again, this should then allow for a speedy implementation of new technologies and also offer a harmonized

European approach of assessing such technologies.

Applicability to Exemplary Measuring Instruments

In this section, three examples of generic measuring instruments will be described. For each example, the applicability of component-based current software requirements and asset-based software requirements as proposed above will be investigated. The examples feature both, technical solutions already established in the market and known technical solutions not yet used in legal metrology.

Example 1: Simple Length Measuring Instrument

The first exemplary measuring instrument shall consist of two components. One of these is a distance sensor on an embedded device, the other is a universal device connected to the sensor via a dedicated serial communication link. The universal device calculates the measurement result based on transmitted raw sensor data and indicates it on an integrated display for user and customer. Figure 3 depicts the two components and their functions.

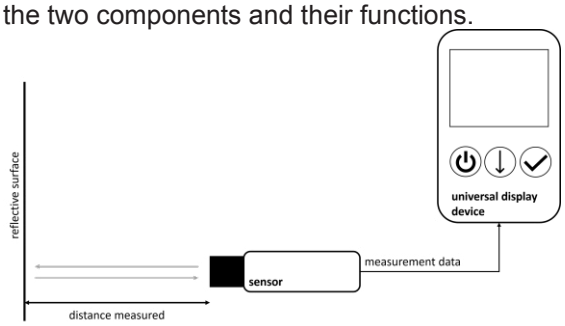

Fig. 3: A sensor on an embedded device measures the distance to a surface using an optical measurement principle and sends the obtained raw data to a universal device for processing and indication.

From the perspective of the current WELMEC 7.2 Software Guide 2023 [3], requirement block P would apply for the embedded device with the sensor and requirement block U would apply to the universal device for processing measurement data and indicating the result. Regarding the separable communication link, interface protection would be required for the corresponding interfaces on both devices, while the link itself would be subjected to requirements for transmission of measurement data, i.e., Extension T. This would ensure protection and securing of measurement data, parameters, and software in each device as well as protection and securing of measurement data during transmission. Software and measurement data protection on the universal device would similarly also ensure adequate protection and securing of the indication of the measurement result. Thus, the new umbrella requirement in the recast guide given above would also be fulfilled. It can be deduced that the first example instrument can be adequately addressed by both the current and future version of WELMEC software guidance.

Example 2: Measurement Data Processing in the Cloud

The second exemplary measuring instrument shall consist of a number of dedicated physically protected and secured sensors for liquids other than water which generate raw measurement data that are sent to a cloud application, i.e., an application running on a virtualized server that may change its physical location and undergo software modifications arbitrarily. To ensure authenticity of the measurement data and to enable checking of the cloud application's functionality, homomorphic signatures [9] are used, which accompany the datasets during each processing step. A retrieval application on a fully protected and secured physical indication device retrieves the measurement result, verifies the homomorphic signatures (thereby demonstrating correct functioning of the cloud application) and displays the result.

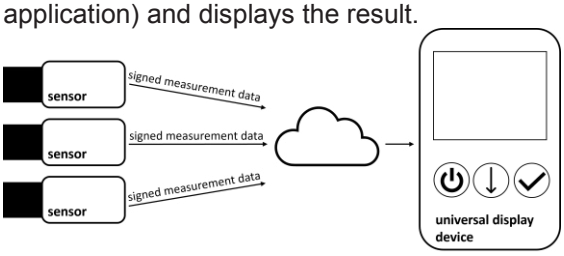

Fig. 4: A number of sensors obtain measurement data and sign them using homomorphic signatures before transmitting them to the cloud, where data and signatures are processes simultaneously. A retrieval device downloads the calculated result from the cloud and verifies the accompanying signature.

From the perspective of the current Guide 7.2, sending and retrieving device would classify either as type P or type U and can therefore be readily examined. The communication between both devices would fall under Extension T for data transmission, which could ensure end-to-end protection of transmitted data, if the data itself is static. However, once the cloud acts as

a processor rather than a simple storage and retrieval system, neither Extension T nor Extension L for long-term storage would be applicable. Instead, the examiner would have to come up with a way to apply requirement set U to the cloud, even though homomorphic signatures would enable checking of all performed calculations on the receiver side without additional protective measures in the cloud. In the current Guide 7.2, requirement set U would automatically result in application of extension O, which would mandate securing and protection of the cloud's underlying operating system regardless of the homomorphic signature scheme. Thus, the asset-based approach would not only provide more flexibility for manufacturers with regard to the second example but would also ensure that examiners can successfully deal with a technical solution not yet established in Legal Metrology.

Example 3: Measurement Data Processing Using Smart Contracts

In the third example, physically protected and secured smart utility meters communicate with a network of servers running a blockchain implementation. Every 15 minutes a new cumulative register value is transmitted by each utility meter. In the blockchain, smart contracts [10] are implemented to verifiably calculate the energy consumption for the current time interval and to assign different tariffs to the energy consumption values according to external triggers such as time, market prices etc.

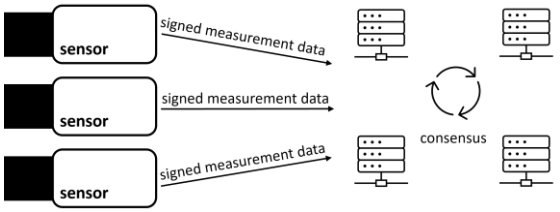

Fig. 5: Multiple sensors collect data and send them to a blockchain network where smart contracts are executed on the data in iterative consensus rounds. All processing steps of the smart contracts can later be verified by check the corresponding blocks and their signatures.

Similar to the second example, both the current Guide 7.2 and the new asset-based approach can easily deal with the smart utility meters as sending devices of either type P or type U. Data processing and retrieval in the blockchain, however, pose a problem for the current component-based requirements, since there is no physical component to secure and protect. Instead, verifiable execution of the smart contract by a majority of blockchain nodes can prove that the agreed algorithm for assignment of tariffs etc. has been correctly realized. Here, no trusted receiving or checking device is needed at all, since the structure of the blockchain ensures that all nodes perform the correct calculation with high probability. Once new blocks have been added to the blockchain, it can be assumed that previous blocks do not change anymore and that the calculation results are accepted by all parties involved. Again, it would be extremely difficult to demonstrate compliance with MID requirements using the current Guide 7.2, whereas an asset-based risk analysis of the solution will likely identify the used signature algorithm of the blockchain as the weakest link. If state-of-the-art cryptography is used, it should be easy to demonstrate that the blockchain solution achieves an adequate level of protection both during processing and during storage of results.

It should be noted that the risk assessment methodology described here currently only addresses intentional manipulations of the assets and their security properties. To address all essential requirements of the MID, such as protection against unintentional modification and random errors, the methodology would need to be extended to cover such effects, too.

Summary

In this paper, current practice for software examination in Legal Metrology was set into contrast with a new asset-based approach currently being discussed in WELMEC Working Group 7. It was shown with the help of a 'classical' example that both approaches can efficiently address established hardware-based securing and protection solutions for measuring instruments. However, it has also been demonstrated that the current requirements, with a strong focus on hardware as a trust anchor for software protection, will likely reach its limitations when technologies already used in other IT fields, such as cloud computing, are subjected to a conformity assessment. Specifically for blockchain implementations, which replace trust in hardware for example with a trust in the majority of executing nodes, new ways of demonstrating compliance with the essential requirements of the MID are needed. With the help of examples for cloud computing and smart contracts, it was shown that the asset-based new examination approach can be a viable alternative.

It should be noted that the MID itself might eventually need to be updated since it currently references certain technical solutions, i.e., protective interfaces, software identification and software separation, which might not be needed in the future. But even after a potential MID modification, the asset-based approach would still remain valid given that the definition of assets and security properties could easily be amended to follow new legal texts.
Future work will focus on extending the risk assessment methodology to random errors and on providing a complete draft implementation for a new WELMEC software guide. Once this draft is available additional practical examples will be used to validate the complete approach.

References

[1] “Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments,” European Union, Council of the European Union; European Parliament, Directive, February 2014
[2] “Directive 2014/3/1EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of non-automatic weighing instruments,” European Union, Council of the European Union; European Parliament, Directive, March 2014
[3] “WELMEC 7.2 Software Guide,” European cooperation in legal metrology, WELMEC Secretariat, Braunschweig, Standard, March 2023
[4] Working Group Measuring Instruments (E01349), http://ec.europa.eu/growth/single-market/goods/building-blocks/legal-metrology/index_en.htm, accessed January 8, 2024
[5] M. Esche, M. Nischwitz and F. Grasso Toro, "Investigation into the Applicability of Software Requirements from Legal Metrology to Sensor Networks," 2022 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Ottawa, ON, Canada, 2022, pp. 1-6, doi: 10.1109/I2MTC48687.2022.9806447
[6] M. Esche and F. Thiel, “Incorporating a measure for attacker motivation into software risk assessment for measuring instruments in legal metrology,” in Proceedings of the 18th GMA/ITG-Fachtagung Sensoren und Messsysteme 2016, Nuremberg, Germany, May 2016, pp. 735 – 742, doi: 10.5162/sensoren2016/P7.4.
[7] M. Esche, F. Grasso Toro, and F. Thiel, “Representation of attacker motivation in software risk assessment using attack probability trees,” in Proceedings of the Federated Conference on Computer Science and Information Systems, Prague, Czech Republic, September 2017, pp. 763–771. doi: 10.15439/2017F112
[8] “WELMEC 7.6 Software Risk Assessment for Measuring instruments,” European cooperation in legal metrology, WELMEC Secretariat, Braunschweig, Standard, March 2021
[9] Sergey Gorbunov, Vinod Vaikuntanathan, and Daniel Wichs, “Leveled Fully Homomorphic Signatures from Standard Lattices”, Proceedings of the 47th annual ACM symposium on Theory of Computing (STOC '15). Association for Computing Machinery, New York, NY, USA, 2015, pp. 469–477, doi:10.1145/2746539.274657
[10] B. K. Mohanta, S. S. Panda and D. Jena, "An Overview of Smart Contract and Use Cases in Blockchain Technology," *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Bengaluru, India, 2018, pp. 1-4, doi: 10.1109/ICCCNT.2018.8494045