EU project proposal

Adequate Securing of Software in Measuring Instruments by Means of a Tested Risk Assessment Procedure

Contents

1 Objectives

- **Develop an objective risk analysis and assessment procedure** for software and ICT products in measuring instruments subject to legal control for the benefit of Notified Bodies, Market Surveillance Authorities and manufactures.
- **Introducing and advancing a knowledge base** covering performed risk assessments and relevant attack scenarios to facilitate the adoption of the new procedure
- **Benefit from a synergetic approach** to combine the respective focus of risk assessment from the Market Surveillance Authorities and the Notified Bodies.
- **Evaluation of existing national and international knowledge bases** that monitor irregularities of measuring instruments in the market with the aim to extend the databases to mark IT-related incidents, to evaluate them, and use them for the risk analysis
- **Application and testing** of the procedure in the field
- **Harmonization, i.e. standardization** on the European and international level, via WELMEC and OIML
- **Advancing the risk concept of WELMEC**
- **Transfer of the results to ETSI or CEN/CENELEC** as a procedure for the realization of *adequate* IT-Security measures for innovative approaches, e.g. Industrial Internet, Internet of things or cloud computing.
- **Establish a cluster of metrology experts** to develop solutions for emerging information and communication technologies in legal metrology and to coordinate related services in Europe

2 Potential Project Partners

Possible project partners are:

- national metrology institutes (e.g. PTB, NPL, LNE, NMi, CMI, METAS, SP),
- market surveillance bodies (e.g. VERISPECT, NMO),
- manufacturers' associations (e.g. CECOD, CECIP).

3 Project Outline

3.1 Introduction

With the introduction of the revised European directives 2014/31/EU [1] and 2014/32/EU [2], the following requirement comes into force for almost all conformity assessment modules:

It shall be possible to evaluate an instrument's conformity with the essential requirements based on the submitted documentation. The documentation shall contain an adequate assessment of the risks.

This new requirement is due to the implementation of decision 768/2008/EC [3] dating back to 2008.

Both revised directives are to be translated into national legislation until April 2016. In Germany, for example, the new Measurement and Verification Act (MessEG) already prescribes risk analysis and assessment for all measuring instruments subject to legal control (see respective regulation (MessEV [4]). In view of the European internal market, conformity assessments performed in one county should be recognized in all other member states. A prerequisite for the acceptance are, of course, harmonized procedures that all Notified Bodies follow. Since information and communication technology (ICT) is ever more frequently an integral part of most measuring devices, threats and subsequent risks associated with ICT also become more important.

In the context of the New Approach [5], manufacturers are subject to requirements, but no explicit technical instructions are normally given. Similarly, manufacturers cannot be forced to follow a unified risk assessment procedure. From the perspective of a Notified Body, however, a standardized procedure would be very helpful when comparing assessment results between different Notified Bodies. In addition, attack scenarios described by different manufacturers could be compared or even amended on the basis of a unified procedure.

Thus, an objective evidential basis could be formed that would make it possible to demonstrate deficiencies in the documented risk assessment supplied by a manufacturer. Should a manufacturer use a risk assessment procedure similar to the one implemented by the Notified Bodies, then the process of examination and certification could be sped up considerably. If internationally accepted and established standards are employed, it is assumed that the procedure will be accepted much more easily by all parties involved.

Another important aspect of the procedure to be developed and an influential factor on its potential acceptance by the industry will be the ability to adapt to new technologies and innovations. Should the adoption of the procedure to new technologies be comparatively easy, its acceptance would be even more likely. A virtualized common knowledge base covering performed risk assessments and frequently occurring attack scenarios could further facilitate the adoption of the new procedure.

According to Regulation 765/2008 [5], market surveillance bodies, too, shall implement adequate procedures for risk assessment. However, due to the different perspectives of market surveillance and Notified Body, the respective focus of risk assessment is different, too. Market surveillance, on the one hand, evaluates the risks originating from a measuring instrument that no longer conforms to the essential requirements

(pre/post-market). The Notified Body, on the other hand, evaluates possible future risks with respect to the current threat landscape.

Measuring instruments that have shown irregularities are registered in national and European databases. An inclusion of the knowledge acquired by market surveillance bodies with the aim of further improving the risk analysis by closing the control loop thus seems advantageous.

The evaluation of existing national and international knowledge bases that monitor irregularities of measuring instruments in the market (e.g. the internet-supported information and communication system for the pan-European market surveillance (ICSMC)) will also be one part of the envisioned project. The aim of this evaluation will be to extend the databases to mark IT-related incidents and to evaluate them.

The results of the project shall be submitted to European and international harmonization bodies (WELMEC, OIML) to achieve harmonization or standardization on the European level. Letters of support from OIML and WELMEC will be collected.

Germany, represented by PTB, chairs the WELMEC working group “Software”, which currently consists of 19 representatives from EU member states, associated members, and big manufacturers’ associations. The working group deals with and seeks to harmonize procedures in conjunction with all issues related to ICT that are either of interest to the measuring instruments industry or that the Notified Bodies deem to be required for fulfilling the essential requirements.

Finally, the harmonized risk assessment approach produced by the WELMEC working group will be submitted to the OIML. The European Commission generally accepts OIML Documents as harmonized normative standards. Germany, represented by PTB, here chairs the subcommittee “Software in Measuring Systems”.

Since the adoption of adequate security measures may also be of interest to a wider community, the output of the project may also be submitted to other European standardization bodies such as ETSI or CEN/CENELEC.

3.2 Work Packages

The following section provides a brief description for each of the planned work packages. Further details and a detailed time plan may be found in Section 4.

3.2.1 WP1: Derivation of Requirements for a Risk Assessment Method

The first step of this work package will consist of the design of a questionnaire concerning desirable features of a risk assessment method. This questionnaire will then be distributed among the involved Notified Bodies and the results will be collected and evaluated. Based on the outcome of the survey, requirements for the targeted risk assessment method will be derived and defined.

3.2.2 WP2: Collection and Comparison of Available Risk Assessment Methods

In this work package, a literature overview concerning existing risk assessment methods will first be conducted resulting in an extensive list. In addition, risk assessment methods already employed by both Notified Bodies (see for example [6]) and manufacturers will be identified and added to the list. Users' experiences with the methods will also be evaluated.

The list will then be extended to cover certain common features of all/some risk assessment methods such as:

- required input data
- expected output
- ability to incorporate new attack vectors
- complexity of the method with respect to required evaluator skills, equipment etc.

At the same time, a similar research activity will be started to collect data on methods that are used to identify, track, and update attack vectors. In addition, all project partners will together develop an abstract concept of a measuring device with features commonly found in the field.

As a final step of this work package, the collected methods will be compared on the basis of said abstract measuring device.

3.2.3 WP3: Selection or Definition of an Adequate Method

With the help of the requirements resulting from WP2, the collected risk assessment methods from WP1 can be evaluated. At the same time, industry standards for extending or complementing the existing methods will be examined. With the help of the results of this activity, one (possibly augmented) method will be selected as the key investigation object for the remainder of the project.

3.2.4 WP4: Evaluation of the Chosen Method

After the definition of the common risk assessment method to be investigated, the abstract measuring instrument from WP1 will now be used to test the chosen method.

At the same time, possibilities for the inclusion of knowledge bases maintained by market surveillance (such as ICSMC and SAM) will be investigated. A virtual alert center for software-related incidents in the field will then be established with the help of the results of said investigation. This includes the production of guidance documents on software-related incidents for market surveillance bodies.

By making use of a procedure yet to be defined, data acquired by the virtual alert center will then be used to keep the database of attack vectors up to date.

3.2.5 WP5: Field Test

After the initial test of the selected method and after the inclusion of data originating from market surveillance knowledge bases, the method will be subjected to a field test.

This test will greatly profit from real-world examples supplied by the manufacturers involved. It will also help to evaluate the method in its proper context consisting of risk assessment, conformity assessment, putting on the market, and market surveillance activities. During this test phase, results obtained by market surveillance can now be fed back into the risk assessment procedure and into the associated virtual alert center.

Attempts at manipulating existing devices through black-box or white-box tests may further help to validate the risk assessment results. An analysis of the results obtained during the field test with the aim of further improving the method and its workflow will round off this work package.

3.2.6 WP6: Determination of Consequences

With the improved risk assessment method in place, it will then be submitted to the harmonization bodies WELMEC, OIML, and CEN/CENELEC. After an initial presentation of the project results further studies or harmonization activities within these bodies are to be initiated.

With the aim of keeping the evaluation ability of all Notified Bodies on the same level, a cluster of metrology experts will be established, that develops solutions for emerging information and communication technologies in legal metrology. This cluster will also serve the purpose to coordinate related services in Europe.

In addition, possible implications of the project outcome on the WELMEC Guide 7.2 “Software” should be considered. These implications may for example be:

- changes to the existing risk classes A to E
- changes to the device classification into type P and U
- introduction of module-related risk classes

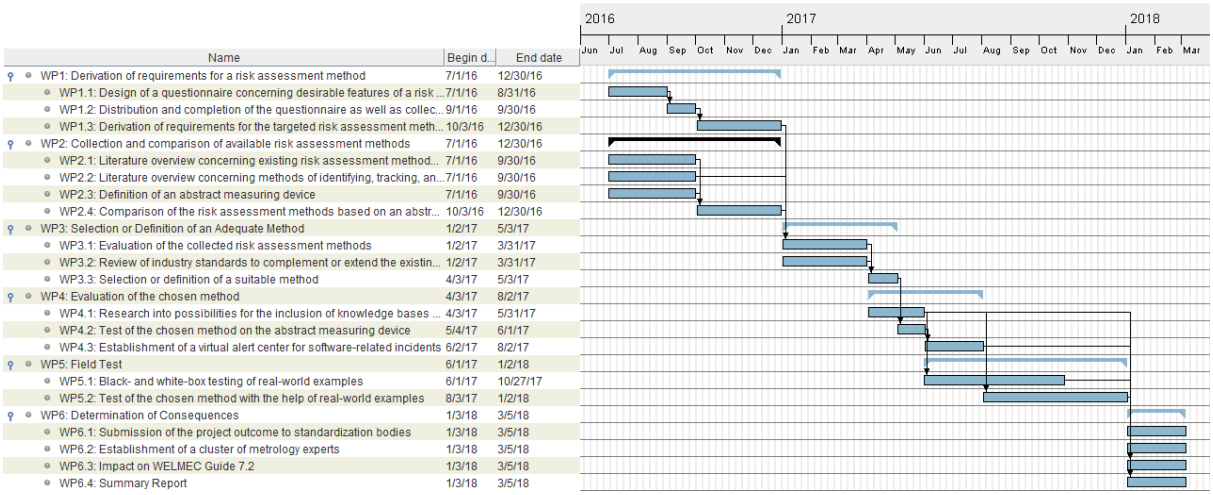
All results of the project and its consequences will be part of the summary report, which will also be generated during this work package.

4 Detailed Schedule and Gantt Chart

Work Package	Title	Time Span (months)	Participating Partners
WP1	Derivation of requirements for a risk assessment method	1-6	
WP1.1	Design of a questionnaire concerning desirable features of a risk assessment method	1-2	
WP1.2	Distribution and completion of the questionnaire as well as collection of the results	3	
WP1.3	Derivation of requirements for the targeted risk assessment method	4-6	
WP2	Collection and comparison of available risk assessment methods	1-6	
WP2.1	Literature overview concerning existing risk assessment methods and overview of the methods which are already applied by the Notified Bodies	1-3	NB
WP2.2	Literature overview concerning methods of identifying, tracking, and updating attack vectors and overview of the methods which are already applied by the Notified Bodies	1-3	
WP2.3	Definition of an abstract measuring device	1-3	
WP2.4	Comparison of the risk assessment methods based on an abstract measuring device	4-6	NB
WP3	Selection or Definition of an Adequate Method	7-10	
WP3.1	Evaluation of the collected risk assessment methods	7-9	
WP3.2	Review of industry standards to complement or extend the existing methods	7-9	
WP3.3	Selection or definition of a suitable method	10	
WP4	Evaluation of the chosen method	10-13	
WP4.1	Research into possibilities for the inclusion of knowledge bases maintained by market surveillance	10-11	
WP4.2	Test of the chosen method on the abstract measuring device	11	
WP4.3	Establishment of a virtual alert center for software-related incidents	12-13	
WP5	Field Test	12-18	
WP5.1	Black- and white-box testing of real-world examples	12-16	
WP5.2	Test of the chosen method with the help of real-world examples	14-18	
WP6	Determination of Consequences	19-20	
WP6.1	Submission of the project outcome to standardization bodies	19-20	
WP6.2	Establishment of a cluster of metrology experts	19-20	
WP6.3	Impact on WELMEC Guide 7.2	19-20	
WP6.4	Summary report	19-20	

4.1 Gantt Chart

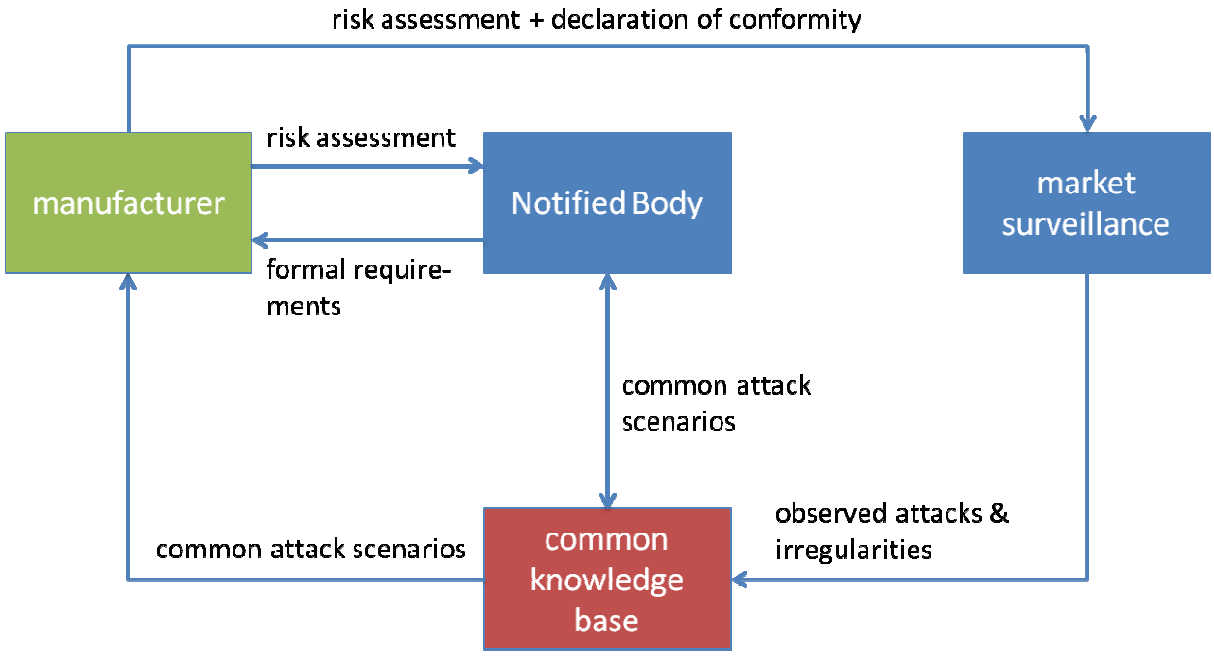
For illustration purposes the intended workflow of the entire project is given in the following figure.



Name	Begin d...	End date
WP1: Derivation of requirements for a risk assessment method	7/1/16	12/30/16
WP1.1: Design of a questionnaire concerning desirable features of a risk ...	7/1/16	8/31/16
WP1.2: Distribution and completion of the questionnaire as well as collec...	9/1/16	9/30/16
WP1.3: Derivation of requirements for the targeted risk assessment meth...	10/3/16	12/30/16
WP2: Collection and comparison of available risk assessment methods	7/1/16	12/30/16
WP2.1: Literature overview concerning existing risk assessment method...	7/1/16	9/30/16
WP2.2: Literature overview concerning methods of identifying, tracking, an...	7/1/16	9/30/16
WP2.3: Definition of an abstract measuring device	7/1/16	9/30/16
WP2.4: Comparison of the risk assessment methods based on an abstr...	10/3/16	12/30/16
WP3: Selection or Definition of an Adequate Method	1/2/17	5/3/17
WP3.1: Evaluation of the collected risk assessment methods	1/2/17	3/31/17
WP3.2: Review of industry standards to complement or extend the existin...	1/2/17	3/31/17
WP3.3: Selection or definition of a suitable method	4/3/17	5/3/17
WP4: Evaluation of the chosen method	4/3/17	8/2/17
WP4.1: Research into possibilities for the inclusion of knowledge bases ...	4/3/17	5/31/17
WP4.2: Test of the chosen method on the abstract measuring device	5/4/17	6/1/17
WP4.3: Establishment of a virtual alert center for software-related incidents	6/2/17	8/2/17
WP5: Field Test	6/1/17	1/2/18
WP5.1: Black- and white-box testing of real-world examples	6/1/17	10/27/17
WP5.2: Test of the chosen method with the help of real-world examples	8/3/17	1/2/18
WP6: Determination of Consequences	1/3/18	3/5/18
WP6.1: Submission of the project outcome to standardization bodies	1/3/18	3/5/18
WP6.2: Establishment of a cluster of metrology experts	1/3/18	3/5/18
WP6.3: Impact on WELMEC Guide 7.2	1/3/18	3/5/18
WP6.4: Summary Report	1/3/18	3/5/18

4.2 Risk Assessment Workflow for WP 5

The field test in WP5 will involve all project partners. A schematic for the field test may be found in the following figure.



5 References

[1] „Directive 2014/31/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 non-automatic weighing instruments," *Official Journal of the European Union,* 26 February 2014.

[2] „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," *Official Journal of the European Union,* 26 February 2014.

[3] „Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repeqling Council Decision 94/465/EEC," *Official Journal of the European Union,* 9 July 2008.

[4] „Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen," *Bundesgesetzblatt,* Bd. 1, Nr. 58, 2014.

[5] „The 'Blue Guide' on the implementation of EU product rules," *Council of the European Unioin,* 2015.

[6] M. Esche und F. Thiel, „Software Risk Assessment for Meausring Instruments in Legal Metrology," *Federated Conference on Computer Science and Information Systems (FedCSIS),* pp. 1113-1123, September 2015.