Risk management for measuring instruments

There are several ways of formulating a satisfactory analysis of the risks inherent in a measuring instrument. The risk analysis data must include as a minimum

- A description of the measuring instrument (including the software version)
- A description of the anticipated usage
- A description of the anticipated environment

The risk analysis (risk management) itself must include as a minimum

- What assets are to be protected?
- What threats can be identified?
- What would be the consequences of any identified threat?
- How likely is it that any identified faults will occur (intentionally or accidentally)?
- What degree of probability and consequence is considered tolerable?
- What techniques have been undertaken in order to reduce the risks?
- What will the consequences be, or how likely is the fault to occur once measures have been taken?

Measuring instruments containing electronics and software are vulnerable to information security risks. Besides the above, the risk analysis must also include

- What threats are there to IT security?
- Which attack vectors have been taken into account?

Contact

Queries on risk analysis for measuring instruments will be answered by
Jan Jacobson, tel. +46 10 516 56 97, email jan.jacobson@ri.se
Charlotte de Bésche, tel. +46 10 516 51 36, email charlotte.debesche@ri.se

General MID and NAWI queries
Lennart Aronsson, tel. +46 10 516 52 41, email lennart.aronsson@ri.se
Bodil Tufvesson, tel. +46 10 516 54 63, email bodil.tufvesson@ri.se

Water meters
Kerstin Mattiasson, tel. +46 10 516 53 80, email kerstin.mattiasson@ri.se

Active electrical energy meters
Stefan Svensson, tel. +46 10 516 54 15, email stefan.svensson@ri.se

Thermal energy meters
Magnus Holmsten, tel. +46 10 516 56 82, email magnus.holmsten@ri.se

Metering systems
Kerstin Mattiasson, tel. +46 10 516 53 80, email kerstin.mattiasson@ri.se

Weighing instruments
Bengt Gutfelt, tel. +46 10-516 54 76, email bengt.gutfelt@ri.se

Taximeters
Ronny Lövstrand, tel. +46 10-516 56 95, email ronny.lovstrand@ri.se

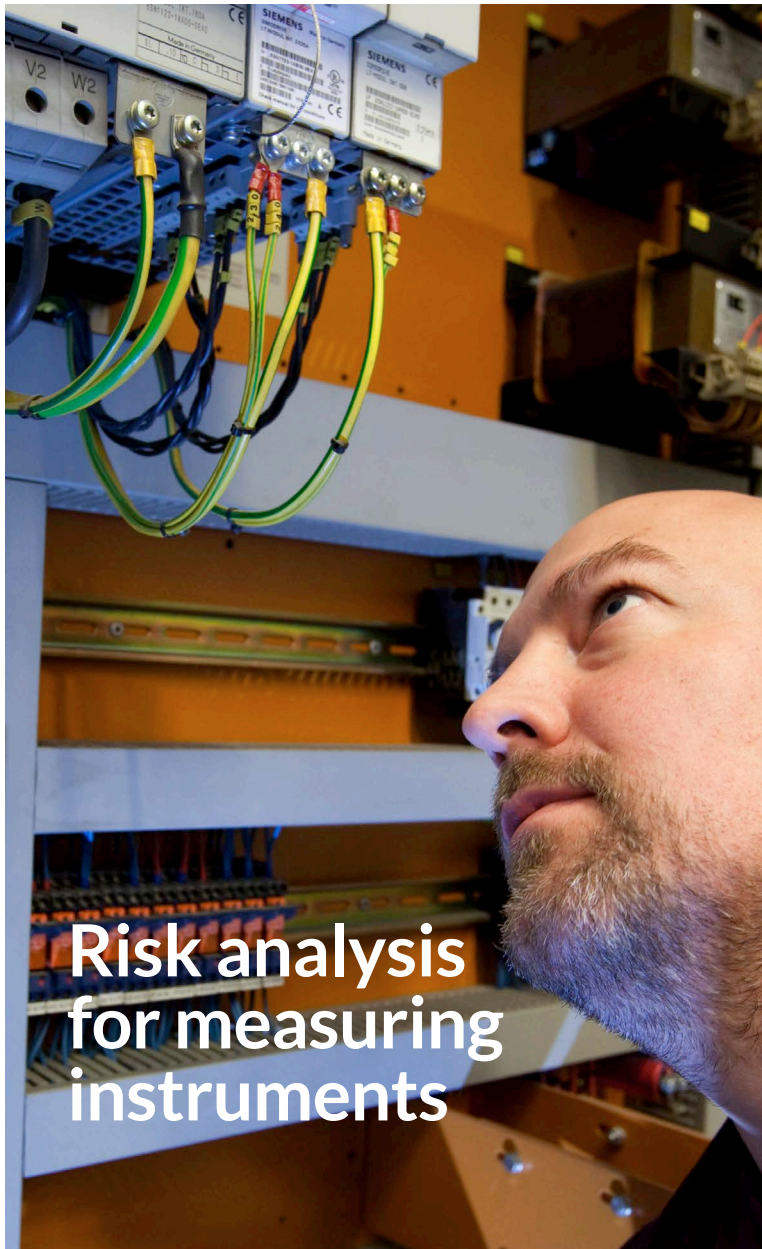
Material measures of length
Jan Elfström, tel. +46 10-516 57 74, email jan.elfstrom@ri.se

RESEARCH INSTITUTES OF SWEDEN

Brinellgatan 4
Box 857, SE-501 15 Borås , Sweden

+46 10 516 50 00
info@ri.se, www.ri.se

Innventia, SP and Swedish ICT have merged to form RISE, providing a focused Swedish institute sector and a stronger innovation partner for business and society.



Correct measurements are important

Correct measurements protect consumers and make it possible for businesses to compete on equal terms. Private individuals who buy products, energy or services rely on weighing instruments, electrical energy meters, gas meters, taximeters, water meters, fuel pumps, length measures and volume measures being correct

Manufacturers of measuring instruments can always benefit from planning with regard to how new measuring instrument qualities and functions affect the risks. For an example of new functionality, we only need to look at how measuring instruments are becoming an important part of the digitisation of society and are connected via communication networks. The option of connecting devices and sharing data is a good thing, but it also results in new risk sources to take into account when designing such devices.

There are collective European rules on how measuring instruments should be designed, manufactured and evaluated. The Measuring Instrument Directive, 2014/32/EU (MID), and the Non-automatic Weighing Instruments Directive, 2014/31/EU (NAWI), specify the basic requirements applicable along with the specific requirements applicable to certain instrument types.

These directives specifically refer to risks:
The documentation shall make it possible to assess the instrument's conformity to the relevant requirements, and shall include an adequate analysis and assessment of the risk(s).

To meet the above requirements in the directives, the manufacturer must carry out a risk analysis to supplement the technical documentation.

As regards risk analysis for the directives, the metrological risks are to be analysed. The personal injury risks due to electric shock and fire, for example, or disruptions to the ambient electrical environment do not need to be included in the metrological risk analysis.

The term "risk" describes a combination of the probability of an unwanted event occurring and its consequence.

Consequence
A consequence is when one of the fundamental requirements (Annex I to the directives) or the instrument-specific requirements (MI-001, etc. in the MID) are not met; when the measurements are incorrect or stored measurements are deleted, for example. The seriousness of the various consequences may be classified using terms such as "serious", "moderate" or "negligible".

Probability
The probability of various faults in a measuring instrument varies. The probabilities should be compared and described using terms such as "high", "medium" or "low". Both probability and consequence can be classified using numerical values. Resources for reducing risks must be invested in areas where they will be most beneficial. This is why it is important to know what the biggest risks are. Risk-reducing measures are implemented to ensure that all risks are tolerable.

Risks are never eliminated completely, but they can be reduced until they are deemed tolerable.

probability

		A	B	C	D	e
		Negligble	Minor	Moderate	Significant	Severe
E	Very Likely	Low Med	Medium	Med Hi	High	High
D	Likely	Low	Low Med	Medium	Med Hi	High
C	Possible	Low	Low Med	Medium	Med Hi	Med Hi
B	Unlikely	Low	Low Med	Low Med	Medium	Med Hi
A	Very Unlikely	Low	Low	Low Med	Medium	Medium

coherence

Information security

Measuring instruments handle information that is important for financial transactions. Measurements are sometimes used to control processes that may be critical to human health or to property or the environment. Primarily, however, the risks involve ensuring that the information (i.e. the measurements) is not corrupted or erased.

We expect the measurement function and measurements

- always to be available when we need to carry out measurement (availability)
- always to be correct and not manipulated or corrupted (correctness)
- only to be accessible by authorised individuals (confidentiality)
- to be capable of being monitored with regard to how and when the information has been handled and communicated (traceability)

The risk analysis is particularly important so as to show how IT security risks linked with the embedded software in a measuring instrument are to be managed. When working with IT security, it is important to understand what assets are to be protected. These assets are then threatened by means of various attack scenarios.

Assets
The assets of the measuring instrument may include

- The metrological software
- Measurement data
- Important parameters in terms of metrology
- Display of results
- Options for saving measurements
- Proof of any intrusions
- Unauthorised effect on metrological software (by means of other devices or software)
- The identity (version) of the metrological software

If any of these assets is affected, it is likely that the function of the measuring instrument will be adversely impacted so that it no longer meets the requirements of the directives.

Not all the above assets will definitely be available in all measuring instruments, and some measuring instruments may have more assets to protect. However, determining what assets are to be protected is always a useful part of the risk analysis.

Threats and attack vectors
To be able to develop good protective mechanisms, it is necessary to know what threats the measuring instrument faces. When the threat comes from an individual with limited options for manipulating the measuring instrument, the protective mechanisms may perhaps be moderate. Sometimes the threat comes from a large group – a major organisation or a large group of people, for example – with extensive resources. The protective mechanisms have to be very effective to be able to withstand serious threats.

It is necessary to analyse the threats to the measuring instrument so that the correct protection techniques and methods can be selected. Experience from similar applications may be very valuable as a way of achieving good information security.

In the case of measuring instruments used for buying and selling goods or services, there is an obvious threat if the buyer or seller wishes to manipulate the measuring instrument to his or her own advantage. The risk analysis should describe the attack vector; in other words, how the attack may potentially take place. The probability also needs to be described so that the threat can be evaluated.

The threat may develop while the measuring instrument is being used.

Example: A measuring instrument is designed to be able to constantly measure and display measurements on a built-in display. There is no access protection for the measuring instrument. The intention is to allow many people to read the display on the measuring instrument but not alter the measurements.

One additional function is offered when maintenance personnel can link up wirelessly to the measuring instrument using their smartphones. Maintenance personnel must be able to read trend curves and detailed measurement information on the phone display. The wireless channel is also used for calibration and programming of the measuring instrument, but it is password-protected.

If the maintenance personnel realise that further functionality is available if only they can "get past the password" in the measuring instrument, this constitutes a threat.

If unauthorised individuals realise that the measuring instrument has a communications port, this presents a further threat. These unauthorised individuals can use special software downloaded to their smartphones to scan the measuring instrument's wireless interface and search for inputs.

In both cases the manufacturer needs to identify the threat, describe the attack vector, assess the probability, decide whether action needs to be taken and assess the probability and seriousness once measures have been put in place, before then deciding again whether any further action needs to be taken.