Riskhantering för mätinstrument

Det finns flera möjligheter att utforma en tillfredställande analys av riskerna i ett mätinstrument. Underlaget för riskanalysen ska åtminstone innehålla

- Beskrivning av mätinstrumentet (inklusive version av programvara)
- Beskrivning av det användningssätt som förväntas
- Beskrivning av den miljö som förväntas

Själva riskanalysen (riskhanteringen) ska åtminstone innehålla

- Vad ska skyddas?
- Vilka fel kan identifieras?
- Vilka blir konsekvenserna av resp. identifierat fel?
- Hur sannolikt är respektive identifierat fel (avsiktligt eller oavsiktligt)?
- Vilken grad av sannolikhet och konsekvens har man ansett tolerabel?
- Vilka tekniker har man vidtagit för att minska riskerna?
- Vilka blir konsekvenserna resp. hur sannolikt är felet efter vidtagna åtgärder?

Mätinstrument med elektronik och programvara är utsatta för informationssäkerhetsrisker. Riskanalysen ska förutom ovanstående även innehålla

- Vilka hot mot IT-säkerheten finns?
- Vilka attackvektorer har man tagit hänsyn till?

Kontakt

Frågor om riskanalys för mätinstrument besvaras av
Jan Jacobson, tel 010 516 56 97, epost jan.jacobson@ri.se
Charlotte de Bésche, tel 010 516 51 36, epost charlotte.debesche@ri.se

Generella MID och NAWI frågor
Lennart Aronsson, tel 010 516 52 41, epost lennart.aronsson@ri.se
Bodil Tufvesson, tel 010 516 54 63, bodil.tufveson@ri.se

Vattenmätare
Kerstin Mattiasson, tel 010 516 53 80, epost kerstin.mattiasson@ri.se

Aktiva elenergimätare
Stefan Svensson, tel 010 516 54 15, epost stefan.svensson@ri.se

Värmemätare
Magnus Holmsten, tel 010 516 56 82, epost magnus.holmsten@ri.se

Mätsystem
Kerstin Mattiasson, tel 010 516 53 80, epost kerstin.mattiasson@ri.se

Vågar
Bengt Gutfelt, tel 010-516 54 76, epost bengt.gutfelt@ri.se

Taxametrar
Ronny Lövstrand, tel 010-516 56 95 e-post ronny.lovstrand@ri.se

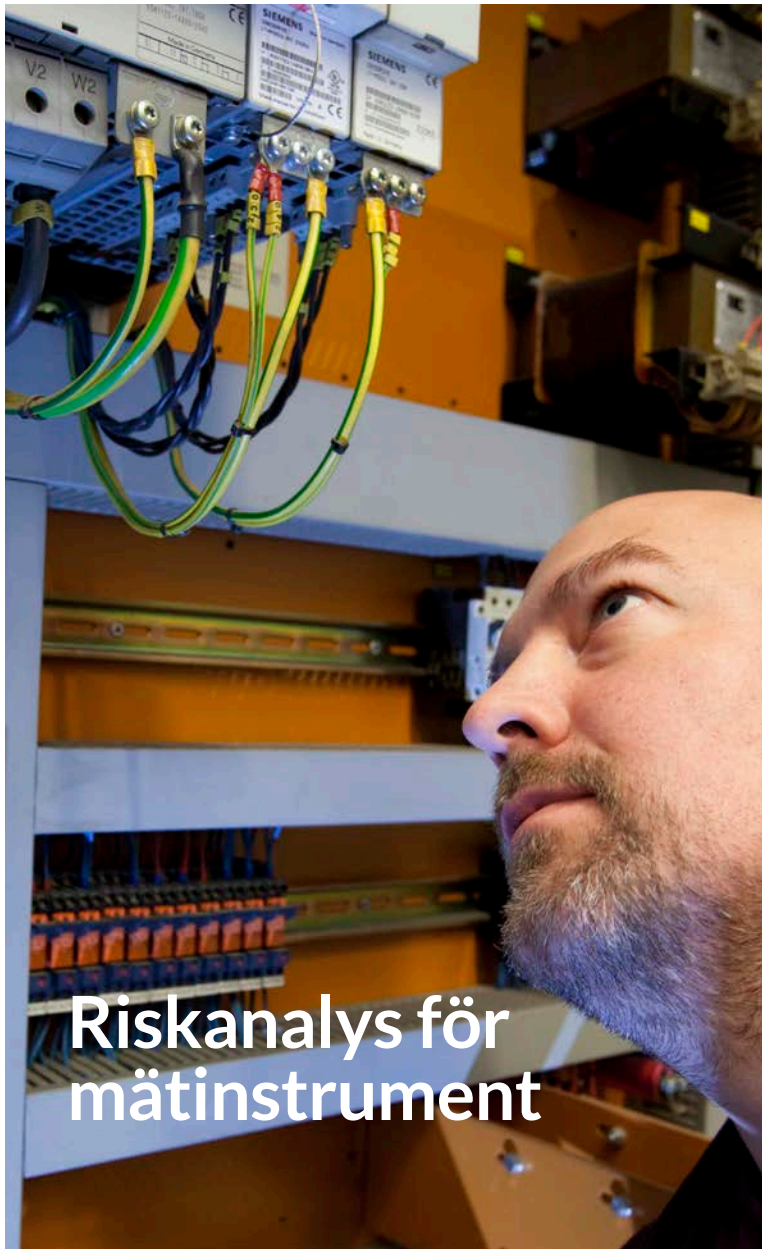
Längdmått
Jan Elfström, tel 010-516 57 74 e-post jan.elfstrom@ri.se

RESEARCH INSTITUTES OF SWEDEN

Brinellgatan 4
Box 857, 501 15 Borås

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

Innventia, SP & Swedish ICT har gått samman i RISE – för en samlad svensk institutssektor och en starkare innovationspartner för näringsliv och samhälle.



Riskanalys för mätinstrument

Korrekta mätningar är viktigt

Korrekta mätvärden skyddar konsumenten och ger förutsättningar för näringslivet att konkurrera på lika villkor. Privatpersoner som köper varor, energi eller tjänster förlitar sig på att vågar, elmätare, gasmätare, taxametrar, vattenmätare, bränslepumpar, längdmått och volymmått är korrekta

Tillverkaren av mätinstrument har alltid nytta av att planera för hur nya egenskaper och funktioner hos mätinstrumentet påverkar riskerna. Ett exempel på ny funktionalitet är hur mätinstrumenten blir en viktig del av digitaliseringen av samhället och därför kopplas upp via kommunikationsnätverk. Möjligheten till uppkoppling och delad data är positiv, men ger också nya riskkällor att ta hänsyn till vid konstruktionsarbetet.

Det finns gemensamma europeiska regler för hur ett mätinstrument ska vara utformat, tillverkat och utvärderat. Genom direktiven (”Measuring Instrument Directive” 2014/32/EU, MID) och direktivet för icke automatiska vågar (2014/31/EU, NAWI) specificeras de grundläggande krav som gäller, samt de specifika krav som gäller för en viss instrumenttyp.

Direktiven skriver speciellt om risker:
Den tekniska dokumentationen ska göra det möjligt att bedöma om instrumentet uppfyller de relevanta kraven i detta direktiv och innehålla en tillfredsställande analys och bedömning av riskerna.

För att uppfylla ovanstående krav i direktiven måste tillverkaren göra en riskanalys, som skall komplettera den tekniska dokumentationen.

När det gäller riskanalys för direktiven är det de mättekniska riskerna som ska analyseras. Risker för personskador genom t.ex. elchock och brand, eller störningar på omgivningens elmiljö behöver inte vara med i den mättekniska riskanalysen.

Begreppet ”risk” beskriver en kombination av sannolikheten för att en oönskad händelse inträffar och dess konsekvens.

Konsekvens
En konsekvens är att något av de grundläggande kraven (bilaga I i direktiven) eller de instrument specifika kraven (MI-001 etc. i MID) inte uppfylls t.ex. att mätningarna blir felaktiga eller att lagrade mätvärden raderas. Allvarligheten i de olika konsekvenserna kan klassas i begrepp som ”allvarlig”, ”måttlig” eller ”försumbar”.

Sannolikhet
Sannolikheten för olika fel i ett mätinstrument varierar. Sannolikheterna bör jämföras, och beskrivas i begrepp som t.ex. ”hög”, ”medel” eller ”låg”. Både sannolikhet och konsekvens kan klassas med numeriska värden. Resurserna för att minska riskerna ska satsas där de gör mest nytta. Därför är det viktigt att veta vilka risker som är störst. Åtgärder för att minska riskerna görs för att alla risker ska bli tolerabla. En risk försvinner aldrig helt, men kan minskas tills den anses tolerabel.

Sannolikhet		A	B	C	D	e
		Försumbar	Liten	Måttlig	Påtaglig	Allvarlig
E	Mycket sannolikt	LågMed	Medel	MedHög	Hög	Hög
D	Sannolikt	Låg	LågMed	Medel	MedHög	Hög
C	Möjligt	Låg	LågMed	Medel	MedHög	MedHög
B	Osannolikt	Låg	LågMed	LågMed	Medel	MedHög
A	Mycket osannolikt	Låg	Låg	LågMed	Medel	Medel

Konsekvens

Informationssäkerhet

Ett mätinstrument hanterar information som är viktig för ekonomiska transaktioner. Ibland används mätvärden för att styra förlopp som kan vara kritiska för människors hälsa, samt för egendom och miljö. Men primärt handlar riskerna om att informationen (dvs mätvärdena) inte ska förvanskas eller försvinna.

Vi förväntar oss att mätfunktionen och mätvärdena

- alltid finns när vi behöver mäta (tillgänglighet)
- alltid är korrekta och inte manipulerade eller förstörda (riktighet)
- endast kan nås av behöriga personer (konfidentialitet)
- kan följas med avseende på hur och när informationen har hanterats och kommunicerats (spårbarhet)

Riskanalysen blir extra viktig för att visa hur IT-säkerhetsrisker kopplade till den inbygga programvaran i ett mätinstrument ska hanteras. När man arbetar med IT-säkerhet är det viktigt att förstå vilka tillgångar man måste skydda. Dessa tillgångar hotas sedan genom olika attackscenarier.

Tillgångar
Tillgångarna i ett mätinstrument kan beskrivas bestå av

- Den mättekniska programvaran
- Mätdata
- Mättekniskt viktiga parametrar
- Visning av resultat
- Möjlighet att lagra mätvärden
- Bevis på att eventuella intrång gjorts
- Otillåten påverkan av den mättekniska programvaran (genom andra enheter eller annan programvara)
- Identiteten (versionen) hos den mättekniska programvaran

Om någon av dessa tillgångar påverkas är det sannolikt att mätinstrumentets funktion påverkas negativt så att det inte längre uppfyller direktivens krav.

Det är inte säkert att alla ovanstående tillgångar finns i alla mätinstrument, och för vissa mätinstrument kan det finnas fler tillgångar att skydda. Men det är alltid en nyttig del av riskanalysen att bestämma vilka som är de tillgångar man vill skydda.

Hot och attackvektorer
För att kunna utveckla bra skyddsmekanismer måste det vara känt vilka hoten mot mätinstrumentet är. När hotet kommer från en enstaka person med begränsade möjligheter att manipulera mätinstrumentet, kanske skyddsmekanismerna kan vara måttliga. Ibland kommer hotet från en stor grupp, t ex en stor organisation eller en stor grupp människor, med stora resurser. För att kunna motstå allvarliga hot måste skyddsmekanismerna vara mycket effektiva.

Det gäller att analysera hoten mot mätinstrumentet för att kunna välja rätt tekniker och metoder för skydd. Erfarenheter från liknande användningsfall kan vara mycket värdefulla för att nå en god informationssäkerhet.

Det uppenbara hotet mot mätinstrument som används för att köpa och sälja varor eller tjänster, är om köpare eller säljare vill manipulera mätinstrumentet till sin fördel. Riskanalysen bör beskriva attackvektorn, dvs på vilket sätt detta kan tänkas ske. Också sannolikheten behöver beskrivas för att man ska kunna värdera hotet.

Hotbilden kan komma att utvecklas under mätinstrumentets användning.

Exempel: Ett mätinstrument är konstruerat för att kontinuerligt kunna mäta och presentera mätvärden på en inbyggd display. Det finns inget åtkomstskydd för mätinstrumentet. Avsikten är att många personer ska kunna läsa av mätinstrumentets display, men inte påverka mätningarna. En extra funktion är att underhållspersonal trådlöst kan koppla upp sig mot mätinstrumentet med sin mobiltelefon. Underhållspersonalen ska kunna läsa trendkurvor och detaljerad information om mätningarna på telefonens display. Den trådlösa kanalen används också för kalibrering och programmering av mätinstrumentet, men är försedd med lösenordsskydd.

Ett hot är att underhållspersonalen inser att det finns ytterligare funktionalitet att använda bara man kan ”komma förbi lösenordet” i mätinstrumentet.

Ett ytterligare hot är att obehöriga personer förstår att mätinstrumentet har en kommunikationsport. Dessa obehöriga kan genom att ladda ned speciell programvara för sina mobiltelefoner scanna av mätinstrumentets trådlösa gränssnitt och söka efter ingångar.

I båda fall behöver tillverkaren identifiera hotet, beskriva attackvektorn, bedöma sannolikheten, bestämma om åtgärder behöver vidtas och bedöma sannolikhet och allvarlighet efter vidtagna åtgärder för att på nytt besämma om fler åtgärder behöver vidtas.