

Fælles sikkerhedsrammer i procesanlæg

Brugere og leverandører får fælles sikkerhedsrammer i procesanlæg ved at anvende den internationale standard IEC

61508's "Safety Integrity Levels" (SIL) for definitionen af sikkerhedsniveauerne.

Af Morten B. Jensen

INSTRUMENTERING.

At der benyttes SIKKERA instrumentering i sikkerhedssystemer er ikke noget nyt. Det har længe været praksis at udstyre kritiske målekredse, hvor der har været risiko for mennesker eller omgivelser, med ekstra systemer til beskyttelse i tilfælde af, at noget skulle gå galt. Disse systemer fungerer normalt uafhængigt af de normale kontrolsystemer og har udelukkende til opgave at sikre anlægget i tilfælde af en fejl eller et systemsvigt.

Fælles ramme for brugere og leverandører

Indtil nu har sådanne systemer været designet i henhold til almindelig praksis inden for den enkelte virksomhed eller det lokale område. Noget af det anvendte udstyr, eksempelvis shut down systemer, har været tilgængeligt med specielle certifikater, men det meste af det perifere udstyr, som eksempelvis instrumenteringen, har ikke haft disse godkendelser. Det har derfor været op til den enkelte at opbygge systemerne med det udstyr, som har været til rådighed.

Denne situation skifter i disse år, idet den brede accept af IEC 61508 standarden "Functional Safety of electrical/ electronic/ programmable electronic safety related systems" giver såvel brugere som leverandører en fælles ramme at arbejde inden for.

En umiddelbar fordel for brugeren er, at specifikation og design af sikkerhedssystemerne nu kan kvantificeres gennem en beregningsmodel, der gør det muligt at vurdere om den valgte løsning passer til det ønskede sikkerhedsniveau, eller om den er over- eller underoptimeret.

International standard
IEC 61508 er en international standard, opdelt i syv dele, der omhandler elektriske systemer, som benyttes til sikkerhedsre-

vante opgaver. Standarden dækker produktion og levering af udstyr, der skal certificeres til brug i sikkerhedssystemer. Fra kontrolsystemer over PLC'er til transmittere, sensorer og aktuatorer.

IEC 61508 dækker hovedområderne:

- Målemetoder og teknikker for definition og beregning af fejl til anvendelse under design og udvikling af hard- og software.
- Opstilling af fejltolerancer og dækning af diagnostisering.
- Opstilling af pålidelighedsmodeller til sandsynlighedsberegning af "risiko for fejl".

Specifikt for procesindustrien arbejdes der i øjeblikket på en særskilt standard, IEC 61511, der bygger på SIL-klassificeringen,

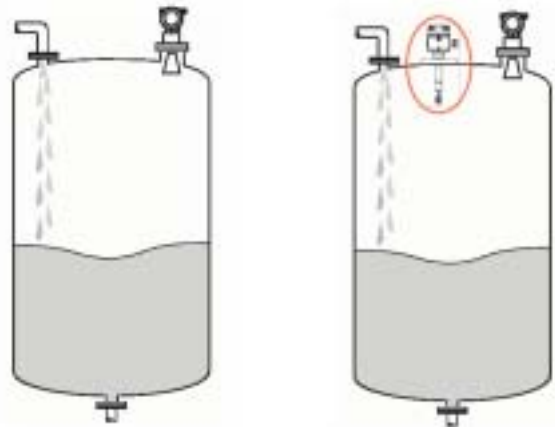
I et "normalt" procesanlæg med "lidt kemi" vil instrumenteringsdelen klassificeres i gruppen SIL 2 - i særtilfælde SIL 3 (afhængig af kompleksiteten). Den skrappeste klassificering SIL 4 henvender sig normalt til sensorer for kernekraft, fly- og rumfartsindustri. Selve definitionen skal ikke senere "godkendes" af myndighederne, men baseres udelukkende på, at en uafhængig gruppe sammensat på den enkelte virksomhed vurderer og analyserer sikkerhedsrisici.

Udvælgelse af instrumenter

Efter definition af det aktuelle SIL-niveau kan udvælgelsen af instrumenter foretages. Dette sker normalt ved hjælp af en FMEDA-analyse (FMEDA = Failure Mode, Effects and Diagnostic Analysis),

Eksempel på funktionssikkerhed

Uafhængig niveauswitch reducerer risiko for overløb



▲ Eksempel på funktionssikkerhed. Uafhængig niveauswitch reducerer risiko for overløb.

men også omfatter kapitler om installation, brug og vedligehold af sikkerhedsudstyret.

Implementering af IEC 61508 i det enkelte land er frivillig, men den betragtes i dag som "state of the art", ikke mindst i forbindelse med eventuelle tvister (forsikringssager), hvor en vurdering af det aktuelle sikkerhedsniveau skal danne grundlag for en ansvarsplacering.

Det korrekte sikkerhedsniveau

Sikkerhedsniveauet i det enkelte anlæg defineres af den virksomhed, der designer anlægget. Vurderingen foretages på basis af en række parametre, der udover de rent sikkerhedsmæssige funktioner også skal vurdere risiko og konsekvens ved et eventuelt uheld. Dette sker ud fra vurderinger omkring konsekvens, hyppighed og flugtmuligheder ved uheld omkring det aktuelle anlæg.

hvor parametre som PFD (Probability of Failure on Demand), SFF (Safe Failure Fraction), HFT (Hardware Fault Tolerances) og MTTF (Mean Time to Failure) vurderes i henhold til den definerede klassifikation.

Analysen opdeler de mulige fejl i fire kategorier:

- Ls,d. Sikre, detekterede fejl. Fejl, som kan opstå, men komponenten fungerer forsat: eksempelvis et display, der ikke fungerer.
- Ls,u. Sikre, ikke detekterede fejl. Fejl, som kan opstå, men komponenten fungerer forsat normalt: eksempelvis en mekanisk skade på indkapslingen af elektronikken.
- Ld,d. Farlige, detekterede fejl. Fejl, som kan trække processen i en farlig retning, men alarmer eller diagnostik muliggør, at situationen kan kontrolleres: typisk

De 4 SIL-niveauer



SIL	Generel beskrivelse	PFD _{avg}	SFF ¹⁾
4	Katastrofal påvirkning af omgivelser	$\geq 10^{-5} \dots < 10^{-4}$	—
3	Skadelig påvirkning af omgivelser	$\geq 10^{-4} \dots < 10^{-3}$	90 ... < 99%
2	Større anlæg med kompliceret proces Risiko for ansatte	$\geq 10^{-3} \dots < 10^{-2}$	60 ... < 90%
1	Mindre anlæg med ringe risiko	$\geq 10^{-2} \dots < 10^{-1}$	< 60%

1) For HFT = 0 anvendes IEC 61511-1 (PDS) / 11.4.4.

PFD_{avg}

Average Probability of Failure on Demand

▲ De fire SIL-niveauer.
PFD_{avg} = Average Probability of Failure on Demand

sensorfejl med efterfølgende alarm.

- Ld,u. Farlige, ikke detekterede fejl. Fejl, som kan trække processen i en farlig retning og ikke giver mulighed for at bringe processen under kontrol: eksempelvis et udgangssignal fra en transmitter, der "låser" ved en "gyldig" værdi.

I standarden angives hvilke intervaller de enkelte faktorer skal ligge inden for, for at kunne klassificeres i den aktuelle SIL-klasse. Her er det selvfølgelig vægtet således, at faktoren Ld,u skal være så lav som mulig.

Certificerede instrumenter

For instrumenter er det normalt leverandøren, der udfører de grundlæggende tests og analyser. Det er således i dag muligt at få leveret instrumenter, der er certificeret til et bestemt SIL-niveau. Med instrumentet medfølger da et særligt certifikat, hvor de for FMEDA-analysen nødvendige parametre er

specificeret. På den måde kan brugeren let kontrolberegne sikkerhedsniveauet i den aktuelle kontrolkreds.

Hvis det viser sig, at det beregnede niveau ikke når på højde med det niveau, man har specificeret for anlægget, kan det være nødvendigt at sikre sig gennem supplerende instrumentering. Et eksempel kunne være en proces-tank, hvori der er monteret en niveaumåling (radar) i toppen. Under uheldige omstændigheder kan der i tanken dannes et skumlag på væskens overflade. Skumlaget resulterer i, at radarmåleren "taber" sit ekko, og altså IKKE længere kan se den korrekte overflade. Det vil normalt give en alarm, som gør, at processen kan bringes sikkert til ro. Men hvor tykt er skumlaget, og hvor tæt er den egentlige væskeoverflade på tankens top.

Sikkerheden i overvågningen kan øges ved at indføre en uafhængig niveaularm, eksempelvis en vibrationsgaffel, der kan hjælpe til at sikre mod overløb.

Et arbejdsredskab

Som nævnt er SIL/IEC 61508 mere et arbejdsredskab end en egentlig standard, der skal følges slavisk. Den sikrer, at brugere og leverandører benytter de samme termer og udtryk, når der tales om sikkerhed og sikkerhedssystemer inden for procesindustrien. På sigt vil vi nok se, at standarden vil opnå langt større udbredelse, end det vi ser i dag. Ikke mindst da det er den eneste standard inden for dette hurtigt voksende fokusområde.

Endress+Hauser A/S kan i dag tilbyde et bredt udvalg af instrumentering certificeret til SIL 2 niveau inden for niveaumåling og -overvågning, samt flow-, temperatur- og trykmåling. Få mere information på www.dk.endress.com

Beregning af SIL-niveau i reguleringsløjfe

