Introduksjon til SIL, integrert sikkerhetsnivå

v/Bjørn Snorre Kaupang, Trainor Automation AS

Artikkelserie, del 2 av 2

Dette er andre artikkel av to som tar for seg introduksjon til temaet SIL. Formålet med artikkelserien er å gi en grunnleggende innføring i hva integrert sikkerhetsnivå handler om. I første artikkel drøftes grunnlaget for SIL, funksjonell sikkerhet og retningslinjen Norsk olje og gass 070. I andre del drøftes ledelse av funksjonell sikkerhet, utvikling av SIL-krav og SIL-sertifisert utstyr i forhold til kjent ytelse.

Ledelse av funksjonell sikkerhet.

SIL griper så dypt inn i sin nisje av helse, miljø- og sikkerhetsarbeidet (HMS) at det i alle henseender er nødvendig å begynne å betrakte nye anlegg fra SIL-perspektiv allerede på planstadiet. Utfallet av en slik første gjennomgang av et system vil være at SIL enten må håndteres eller kan sees bort ifra. Målet for HMS-arbeidet er at grunnlaget opprettes for alle nødvendige aktiviteter som sikrer at SIL-krav identifiseres og håndteres i grunnleggende konstruksjon og deretter vedlikeholdes gjennom hele sikkerhetssystemets livssyklus.

Ledelse av funksjonell sikkerhet stiller klare krav til at sikkerhetsinstrumenterte system skal ledes av personell som har kompetanse til dette etter relevante krav nedfelt i Petroleumstilsynets forskrifter, samt IEC 61508 og IEC 61511. Det er også slik at alt personell og organisatoriske enheter som er ansvarlige for utførelse, gjennomføring og gjennomgang av respektive levetidsfaser for det sikkerhetsinstrumenterte anlegget skal være kjent med og informert om ansvaret som er pålagt dem. Som del av ledelsen av funksjonell sikkerhet ligger også krav om oversiktlige og konsise planer. Plan skal være levende dokumenter som vedlikeholdes gjennom hele sikkerhetsanleggets levetid. Det skal i samsvar med Petroleumstilsynets krav også finnes et program for jevnlig vurdering, gjennomgang og revisjon av sikkerhetsprosesser i hele sikkerhetsanleggets levetid. Det stilles også minimumskrav til nødvendig konstruksjons- og driftsteknisk ekspertise til å forestå slike vurderings- og revisjonsaktiviteter.

Retningslinjen Norsk olje og gass 070

Arbeidsmetodikk i håndteringen av SIL innebærer aktivitetene verifikasjon og validering. Innholdsmessig forskjell på disse aktivitetene håndteres slik at verifikasjon innebærer bekreftelse på at løsningen oppfyller kravspesifikasjon. Validering innebærer bekreftelse av at løsningen passer til oppgaven ved sjekk mot behov og myndighetskrav. I disse sammenhengene skal vesentlige dokument som Safety Requirement Specification (SRS) og Safety Analysis Report (SAR) utvikles og vedlikeholdes.

Safety Requirement Specification (SRS) skal inneholde tre typer krav:

- Funksjonelle krav, for eksempel anleggsytelser
- Integritetskrav, for eksempel feilsannsynlighet og SIL-nivå.
- Driftsmessige forhåndsregler og begrensninger.

SRS skal fastsette nødvendig testhyppighet, i tillegg må kravene i SRS også være forenlige med anleggets eller installasjonens bemanning for gjennomføring av pålagte aktiviteter.

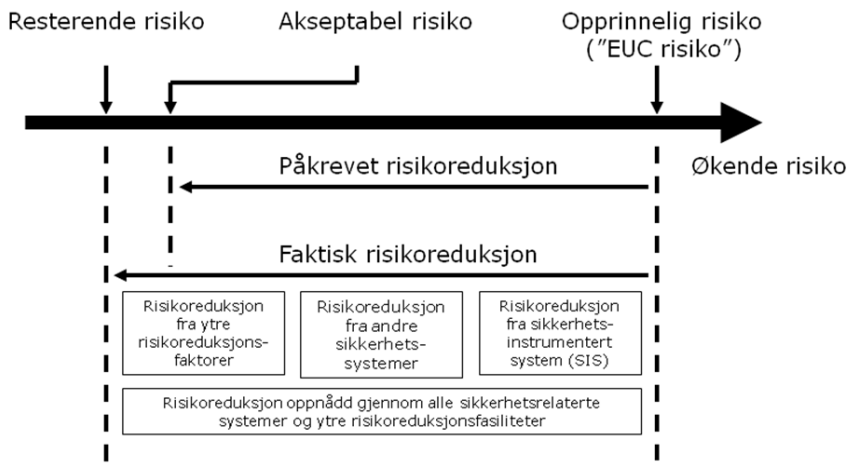
Safety Analysis Report (SAR) skal fremstilles av involverte utstyrsleverandører som del av detaljkonstruksjonen for å dokumentere samsvar med fremstilt SRS. SRS for installasjonen må altså dermed være tilgjengelig før anskaffelser iverksettes, slik at utstyrsleverandører har mulighet til å møte nødvendige krav.

Utvikling av SIL-krav.

Fra sikkerhetssynspunktet handler SIL om sikkerhet som resultat av pålitelighet. Fra drifts- og vedlikeholdsteknisk synspunkt kvantifiseres utstyrets sikkerhetsytelser sett fra antall forekommende detekterte feil, udetekterte feil og feilmodus (feil til sikker/feil til farlig tilstand) sammen med følgende sammenhenger:

- Tilgjengelighet.
- Sannsynlighet for feil ved behov for sikkerhetsfunksjonen.
- Feilrate.
- Andel sikre feil.
- Risikoredusjonsfaktor.
- Sikkerhetssystemets natur som Type A/B iht. IEC 61508/Norsk olje- og gass 070.

Gjennom risikoreduksjonsfaktor kommer man til nødvendig struktur og SIL-nivå. Det er dessuten også slik at et SIL-nivå faktisk er et intervall. Det er ikke nødvendigvis slik at kravet til funksjonell sikkerhet er oppnådd når utstyr og installasjon tilfredsstiller SIL 2, det kan være at kravet ligger i øvre del av intervallet for SIL 2. Da må det i tilfelle demonstreres at utstyr og installasjon også har ytelsesmessige kvaliteter som tilfredsstiller øvre del av intervallet.



Rammeverk for risikoreduksjon (basert på IEC 61508-5, fig. A.1)

SIL-sertifikat i forhold til kjent ytelse

Det er også nyttig å være oppmerksom på at SIL-sertifikater og SIL-sertifisert utstyr faktisk ikke inneholder noen garanti for at utstyr kan benyttes i tiltenkt sammenheng. Erfaringsbaserte typetall med sertifisert utstyr kan faktisk være dårligere enn det som oppgis i sertifikatet. Det kan også hende at det for realisering av en sikkerhetsfunksjon er nødvendig å benytte utstyr som ikke har noe SIL-sertifikat. Vi forholder oss dermed til bransjens erfaringsbaserte verdier og benytter "kjent ytelse" som utgangspunkt. Ikke minst; når vi har etablert kjennskap til standarden og krav gjennom IEC 61508 og Norsk olje og gass 070 forstår vi at omfanget av SIL er større og mer omfattende enn at kravene enkelt tilfredsstilles gjennom anskaffelse av utstyr med SIL-sertifikat.

SIL overført til instrumenteringsteknikk og fiskale sammenhenger

Når vi nå har skrapet lett i overflaten på SIL ser vi at det kan være nødvendig med bedret forståelse for hva SIL handler om for mange fagdisipliner som er engasjert i petroleumsnæringen. For elektro, instrument- og automasjonsfolk er det særlig viktig å ha et godt fundament i bearbeiding av utfordringene, sammen med disipliner som teknisk sikkerhet, prosess og mekanisk.

Hvis vi strekker det hele litt lengre og ser hva spesialiseringen som fiskale sammenhenger innebærer for disiplinene prosess, mekanisk, instrumentering og automasjon, så er det ganske åpenbart at det kan trekkes veksler på kunnskap og erfaring fra oppetidskrav og driftsmessig kvalitet fra SIL og overføre nettopp til fiskale målinger. Nødvendige ytelser og kvaliteter som det er pålagt virksomhetene å inneha innenfor fiskale målinger er eksplisitt gitt i Oljedirektoratets "Forskrift om måling av petroleum for fiskale formål og for beregning av CO2 –avgift", samt NORSOK-standardene I-104 Fiskale målesystemer for hydrokarbongasser og I-105 Fiskale målesystemer for hydrokarbonvæsker. Myndighetenes fokus på pålitelighet og nøyaktighet for fiskale hydrokarbonmålinger innebærer et nesten like omfattende kvalitetsregime som kravene til funksjonell sikkerhet.