Mange definisjoner er endret

Av Tore Guldbrandsen, Senioringeniør Sikkerhetsinstrumentering Tormatic AS

Ny standard innen sikkerhetssystemer IEC615 Ed 2.0

Tormatic AS har i en årrekke levert bl.a. sikkerhetsreleer og Ex barrierer fra GM International. I tillegg til innovative kvalitetsprodukter har denne leverandøren også utmerket seg ved å utarbeide svært godt og nyttig faglig stoff – bl.a. en SIL-manual som nå har kommet i 4. opplag!

Denne boken er også i Norge delt ut til fornøyde kunder som finner svar på utfordrende oppgaver innen systemsikkerhet relatert til standardene IEC61511 og IEC61508. Senioringeniør Tore Guldbrandsen har i denne forbindelse opparbeidet seg gode kunnskaper på området og deler her betraktninger rundt den nye versjonen av IEC61511 som ble fullført i juli i år – et sammendrag av de viktigste endringene som kan ha betydning for deg!

Introduksjon

IEC61511 Ed. 1.0 ble lansert for første gang i 2003 og var da basert på prinsippene i standard IEC61508 Ed. 1.0 som først ble utgitt i 1998. Denne standarden ble så erstattet med IEC61508 Ed. 2.0 i april 2010, og IEC61511 Ed. 1.0 er nå erstattet med IEC 61511 Ed. 2.0 fra februar 2016 med del 1 og senere i juli 2016 med hele utgivelsen inkludert del 2 og 3. Dessverre har det blitt oppdaget noen feil i del 1, det er derfor gitt ut en rettelse på dette (IEC61511-1: 2016 / COR1: 2016) som kan lastes ned via: https://webstore.iec.ch/publication/25880

Det bør understrekes at IEC61508 har klart mer fokus på de som produserer og utvikler sikkerhetsutstyr/instrumentering og systemer, mens IEC61511 er i hovedsak brukt av sluttbruker/fabrikk/prosjekter som innfører SIS i prosessindustrien.

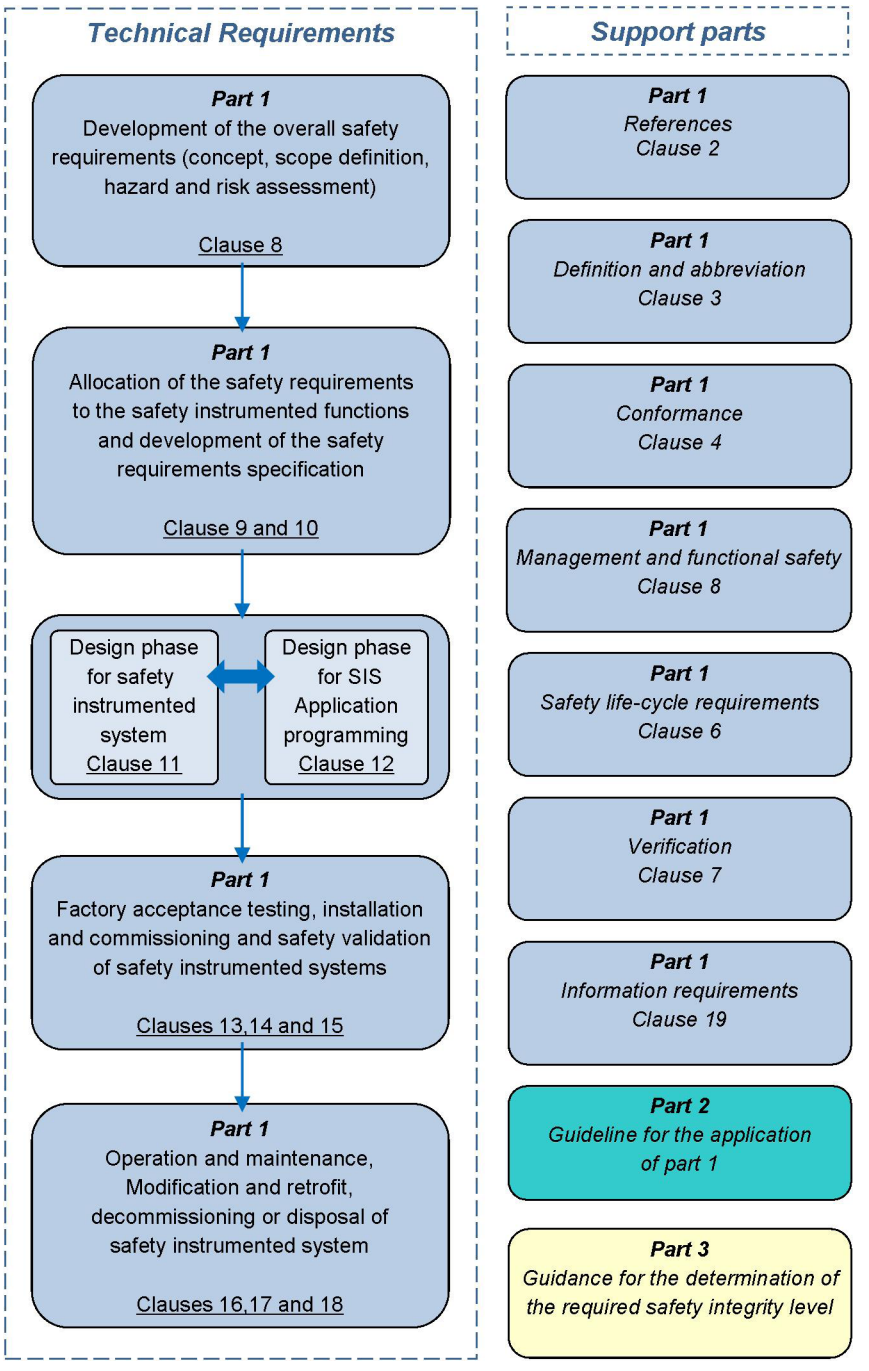
Aksepten for IEC61511 varierer rundt om i verden, men i mange land (f.eks. Norge, Storbritannia, Belgia m.fl.) er det en godt etablert standard for instrumenterte sikkerhetssystemer i prosessindustrien. Det er ikke et juridisk krav i seg selv, men det å implementere god praksis er faktisk et juridisk krav! →

Kortfattet sammendrag

Noen viktige endringer i IEC61511: 2016 utgivelsen:

- Sikkerhetsrisikovurdering SKAL gjennomføres! Cybersikkerhet blir et dominerende krav! Ref. veiledninger i: ISA TR 84.00.09, ISO / IEC 27001: 2013 og IEC62443.
- Sikkerhetskravspesifikasjonene (SRS) har 29 krav som SKAL beskrives pr. instrumenterte sikkerhetsfunksjon (SIF).
- Bypass krav og kompenserende tiltak skal beskrives.
- Sikkerhetsmanual for alle enheter, delsystemer og komplette systemer kreves.
- Minimums arkitekturbegrensninger (HFT) har blitt forenklet og er nå basert på 2H i IEC61508: 2010. Alternativt kan 1H i IEC61508: 2010 fortsatt brukes.
- Sluttbrukers komponentpålitelighet – kvaliteten på historiske data må nå bevises i henhold til strengere krav, veiledning i ISA TR 84.00.04: 2015 og Namur NE130
- Alle som leverer produkter eller tjenester i livsløpsfasen SKAL ha et funksjonelt sikkerhetsstyringssystem (FSM) og demonstrere samsvar med kravene i IEC61511: 2016.
- Endringer/modifikasjoner SKAL ikke begynne før en uavhengig funksjonell sikkerhetsvurdering er gjennomført og godkjent.
- Under drift og vedlikeholdsfasen, SKAL en periodisk funksjonell sikkerhetsvurdering utføres av en eller flere uavhengige kompetente personer som ikke er involvert i drift og vedlikehold av det samme SIS-systemet.

IEC61511: 2016 standarden er fortsatt en «ytelsesbasert» standard, selv om mange definisjoner har endret seg til å bli mer restriktive med bruk av ordet SKAL gjennom deler av standarden. To grunnleggende begreper er fortsatt sikkerhetslivssyklus og sikkerhetsintegritetsnivå (SIL) som uttrykker hvor godt systemet er forventet å virke. Sikkerhetslivssyklus er en rasjonell prosjekteringsprosess med en systematisk tilnærming som skisserer en god teknisk praksis for sikkerhetsinstrumenterte systemer innen design, utvikling og vedlikehold. Det er tekniske krav og ikke-tekniske eller styringskrav i standarden som vist i figuren nedenfor (IEC615: 2016 del 1).



Det er fremdeles 3 deler i IEC61511 Ed. 2.0:

Del 1 er den normative delen av standard og inneholder: Rammeverk, definisjoner, system, samt krav til maskinvare og programvare. Del 1 beskriver kravene til overholdelse av punkt 5 til 19. Det er prosjektplan-

lging, styring, dokumentasjon og krav til kompetanse. Det er også der de tekniske kravene for å oppnå sikkerhet gjennom sikkerhetslivssyklusen er definert.
IEC61511-1: 2016 ble utgitt 24. februar 2016 og teller 82 sider
IEC 61511-1: 2016 / COR1: 2016 ble utgitt 15. september 2016 - 3 sider

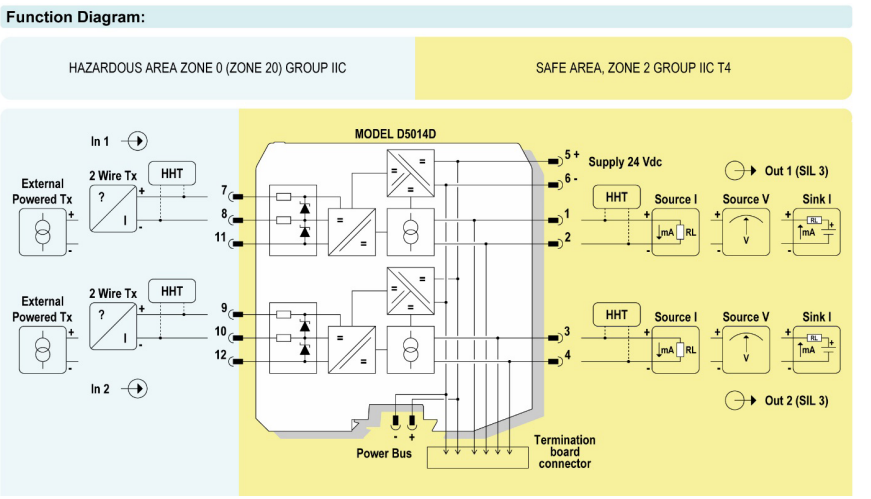
Del 2 er den informative delen av standarden og inneholder: Retningslinjer for bruk av IEC61511 del 1, så del 2 gir altså veiledning i hvordan klausuler i del 1 skal forstås.

IEC61511-2: 2016 ble utgitt 28. juli 2016 og teller 204 sider!

Del 3 er også en informativ del av standarden og inneholder: En veiledning for å bestemme nødvendige sikkerhetsintegritetsnivå.
Vedlegg A dekker ALARP-prinsippet (As Low As Reasonably Practicable) – "så lavt som praktisk mulig".
Vedlegg B dekker både kvantitative og kvalitative tilnærminger til SIL. Den bruker ETA analyse, sikkerhetslag matrise metode, risiko graf, LOPA og risikomatrise .
Vedlegg J er nytt i Ed. 2.0 og håndterer flere sikkerhetssystemer som beskriver systemiske avhengigheter.
IEC61511-3: 2016 ble utgitt 21. juli 2016 og teller 101 sider

Krav til sikkerhetsmanual:

Produsenten er nå påkrevd å ha en funksjonell sikkerhetsmanual for hvert produkt i henhold til den nye standarden. Her viser vi et eksempel på utdrag fra en slik manual tilhørende produktet D5014D – SIL 3 Repeater Power Supply HART – fra vår leverandør av SIL releer og Ex barrierer – GM International.



Example of the Safety Function and Failure behavior of the above device:
The model D5014 is considered to be operating in Low Demand mode, as a Type A module, having Hardware Fault Tolerance (HFT) = 0. The failure behavior is described from the following definitions:

- *fail-Safe State: state is defined as the output going Low or High, considering that the safety logic solver can convert the Low or High fail (dangerous detected) to the fail-safe state;*
- *fail Safe: failure mode that causes the module to go to the defined failsafe state without a demand from the process;*
- *fail Dangerous: failure mode that does not respond to a demand from the process (i.e. being unable to go to the defined fail-safe state) or deviates the output current by more than 5% (0.8 mA) of full span;*
- *fail High: failure mode that causes the output signal to go above the maximum output current (> 20 mA). Assuming that the application program in the safety logic solver is configured to detect High failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure;*
- *fail Low: failure mode that causes the output signal to go below the minimum output current (< 4 mA). Assuming that the application program in*

the safety logic solver is configured to detect Low failure and does not automatically trip on this failure, this failure has been classified as a dangerous detected (DD) failure;

- *fail "No Effect": failure mode of a component that plays a part in implementing the safety function but that is neither a safe failure nor a dangerous failure. When calculating the SFF, this failure mode is not taken into account;*
- *fail "Not part": failure mode of a component which is not part of the safety function but part of the circuit diagram and is listed for completeness. When calculating the SFF this failure mode is not taken into account.*

The 2 channels of the D5014D module could be used to increase the hardware fault tolerance, needed for a higher SIL of a certain Safety Function, as they are completely independent from each other, not containing common components. In fact, the analysis results for D5014S (single channel) are also valid for each channel of D5014D (double channel). This analysis is also valid for D5014D as Duplicator of 2 wires Transmitter Input Signal, but considering safety function is only applied to the channel configured as passive input. Failure rate data: taken from Siemens Standard SN29500

Sikkerhetsmanualen skal også gi en oppsummering av feilraten:
Tabellen nedenfor forutsetter et resultat på T-proof-testen = 99%. Dette vil ikke være praktisk uten råd og veiledning om hvordan testen skal utføres!

Failure rate table:

Failure category	Failure rates (FIT)
λ_{dd} = Total Dangerous Detected failures	135.30
λ_{du} = Total Dangerous Undetected failures	14.25
λ_{sd} = Total Safe Detected failures	0.00
λ_{su} = Total Safe Undetected failures	0.00
$\lambda_{tot\ safe}$ = Total Failure Rate (Safety Function) = $\lambda_{dd} + \lambda_{du} + \lambda_{sd} + \lambda_{su}$	**149.55**
MTBF (safety function, single channel) = (1 / $\lambda_{tot\ safe}$) + MTTR (8 hours)	**763 years**
$\lambda_{no\ effect}$ = "No Effect" failures	201.25
$\lambda_{not\ part}$ = "Not Part" failures	20.80
$\lambda_{tot\ device}$ = Total Failure Rate (Device) = $\lambda_{tot\ safe} + \lambda_{no\ effect} + \lambda_{not\ part}$	**371.60**
MTBF (device, single channel) = (1 / $\lambda_{tot\ device}$) + MTTR (8 hours)	**307 years**

Failure rates table according to IEC 61508:

λ_{sd}	λ_{su}	λ_{dd}	λ_{du}	SFF	DC_S	DC_D
0.00 FIT	0.00 FIT	135.30 FIT	14.25 FIT	90.47%	0%	90.47%

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes 10% of entire safety function:

T[Proof] = 1 year	T[Proof] = 15 years
PFDavg = 6.36 E-05 Valid for **SIL 3**	PFDavg = 9.54 E-04 Valid for **SIL 2**

PFDavg vs T[Proof] table (assuming Proof Test coverage of 99%), with determination of SIL supposing module contributes 20% of entire safety function:

T[Proof] = 3 years	T[Proof] = 20 years
PFDavg = 1.91 E-04 Valid for **SIL 3**	PFDavg = 1.27 E-03 Valid for **SIL 2**

Systematic capability SIL 3.

Testing procedure at T-proof

The proof test shall be performed to reveal dangerous faults which are undetected by diagnostic. This means that it is necessary to specify how dangerous undetected fault, which have been noted during the FMEDA, can be revealed during proof test. **The Proof test 1** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	By HART command or other technique, set the transmitter connected to the input of the repeater in order to go to high alarm current and verify that the output current of the repeater reaches that value. This tests for compliance voltage problems such as a low loop power supply voltage or increased wiring resistance.
3	By HART command or other technique, set the transmitter connected to the input of the repeater in order to go to low alarm current and verify that the output current of the repeater reaches that value. This tests for possible quiescent current related failures.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 30 % of possible Dangerous Undetected failures in the repeater.

The **Proof test 2** consists of the following steps:

Steps	Action
1	Bypass the safety-related PLC or take other appropriate action to avoid a false trip.
2	Perform step 2 and 3 of the **Proof Test 1**.
3	Perform a two-point calibration (i.e. down scale as 4 mA and full scale as 20 mA) of the transmitter connected to the input of the repeater. Then set the transmitter to impose some input current values of 4-20 mA range and verify that the correspondent output current values of repeater are within the specified accuracy. This proof requires that the transmitter has already been tested without the repeater and it works correctly according to its performance.
4	Restore the loop to full operation.
5	Remove the bypass from the safety-related PLC or restore normal operation.

This test will reveal approximately 99 % of possible Dangerous Undetected failures in the repeater.

Denne tabellen viser hvordan du skal utføre en T-proof test i henhold til produsentens anbefaling. Meningen med T-proof test er å luke ut farlige feil som er uoppdaget av diagnostikk. Derfor er det også obligatorisk å inkludere dette i sikkerhetshåndboken av produsenten. Produsenten må forklare hvordan, og hva, som må testes for å oppnå PFDavg. SIL-ytelsen til enheten.

Krav til aktive og passive systemer (ESD, F & G)

Et klassisk Fire & Gas (F & G) alarmsystem vil under normal drift ikke være aktivisert. Bekymringen med en slik type konfigurasjon er at den ikke er sikker! Anta at du har et ledningsbrudd til et overrislingsanlegg, du vil dermed ikke være i stand til å aktivisere solenoiden lenger. Det er derfor vi bruker sløyfeovervåking på en SIF utgang, for å måle motstand eller impedans på kabel/spole og sikre at enheten fortsatt er monitorert av det deaktiviserte DO-kortet fra sikkerhets PLS'en.

Når det gjelder sløyfeovervåkingsfunksjonalitet til DO-kort i sikkerhets PLS kan det være et problem. Overvåkingen er ofte tapt eller vil ikke fungere når du trenger å koble solenoider via et interposing relé. De fleste av releene på markedet støtter ikke denne funksjonen. Når det er behov for å overvåke kabel eller lastfeil på en SIF i en aktivisert til trip funksjon, så er det spesielle krav som bør spesifiseres.

Det finnes imidlertid en løsning for dette - et smart sikkerhetrelé for F & G-applikasjoner som støtter både sløyfe- og lastovervåking og kan gi informasjon tilbake til kontrollsystemet med full diagnostikk! Det å kunne monitorere hele sløyfen for brudd, kortslutning eller endring av lasten vil bli mer og mer viktig! Det nedbemannes både på land og offshore og det planlegges ubemannede oljeplattformer i framtiden. Monitorering av last, sløyfe for kortslutning, brudd, isolasjon og jordfeil vil bli en nødvendighet!

Vi vil også nevne at GM International er den eneste produktleverandøren i bransjen som har offisiell TÜV Rheinland godkjenning for å holde kurset: Functional Safety Engineer Safety Instrumented System. Kursholderen Tino Vande Capelle har personlig hatt nærmere 2000 ingeniører over hele verden på kurs i løpet av de siste 11 årene. I tillegg til denne opplæringen gir GM International fullverdige kurs i IEC61511: 2016. De har også gitt ut en SIL Håndbok – instrumenterte sikkerhetssystemer – som dekker både IEC61508: 2010 og IEC61511: 2016 med en oppsummering i siste utgave av boken (versj. 4). Ta kontakt med Tore Guldbrandsen i Tormatic dersom du ønsker et eksemplar!