Prinsipper for utforming av Alarmsystemer

Februar 2001
YA-710

OLJEDIREKTORATET

Innholdsfortegnelse

1 INNLEDNING

1.1 Bakgrunn og formå

Oljedirektoratet (OD) har gjennom sin tilsynsvirksomhet med sikkerhetsmessige forhold avdekket utilfredstillende forhold knyttet til alarmsystemer på produksjonsinnretninger på norsk kontinentalsokkel. Erfaringer har vist at utforming av alarmsystemer kunne vært viet mer oppmerksomhet under prosjektering og anskaffelse av nye alarmsystemer, og ved modifikasjon og operasjon av eksisterende systemer.
Siden alarmsystemer er viktige for sikker operasjon av petroleumsinnretninger, er det av vital betydning at disse utformes i samsvar med anerkjent prinsipper for menneske-maskin samspill og tilgjengelig kunnskap om menneskelige faktorer.

Dette dokumentet inneholder et sett med anerkjente prinsipper for utforming av et vel fungerende alarmsystem. Hensikten med dokumentet er å bistå involvert personell i forbindelse med prosjektering, innkjøp, vedlikehold og operasjon av alarmsystemer. Formålet er å gi støtte til forbedring av eksisterende systemer så vel som ved utvikling av nye systemer og i forbindelse med modifikasjoner. Målet er å bidra til at løsninger velges som ivaretar gjeldende norske regelverkskrav, samtidig som sikkerhet, lønnsomhet og høy regularitet ivaretas.

Dokumentet dekker alarmgenerering, strukturering, prioritering , presentasjon og alarmhåndtering. Innholdet i dokumentet er basert på de nyeste internasjonalt anerkjente retningslinjer for alarmsystemer tilgjengelig i dag, og fokuserer på realistiske løsninger basert på forskning og beste praksis fra ulike prosessindustrier. Dokumentet beskriver funksjonalitet som bør betraktes som vesentlig eller svært verdifull i et godt alarmsystem.

Dokumentet er blitt utarbeidet av Institutt for Energiteknikk (IFE) i Halden på oppdrag for OD. Følgende IFE personell har deltatt i utarbeidelsen av retningslinjen: Øystein Veland, Magnhild Kaarstad, Lars Åge Seim og Nils Førdestrømmen.

1.2 Strukturen i dokumentet

Etter de overordnede kravene til systemet følger mer detaljerte krav innenfor emnene generering, strukturering, prioritering, presentasjon og håndtering av alarmer.

Hvert krav er presentert på følgende format:

Krav

Hensikt: Forklarer bakgrunnen for hvorfor dette er et krav

Kommentarer: Utfyllende kommentarer med eksempler på hvordan kravet kan oppfylles osv.

1.3 Definisjoner

Dette avsnittet definerer en del sentrale begreper som benyttes i dokumentet. Noen begreper vil trolig være ukjente for enkelte lesere i industrien, og en del begreper som er i bruk i dag er blitt redefinert. Dette er gjort for å få etablert en mer presis terminologi som er bedre egnet til å beskrive egenskapene til et godt alarmsystem. Definisjonene i dette dokumentet er dessuten i tråd med viktig internasjonal litteratur på området.

Alarmtyper

Basisalarmer (basic alarms) genereres ved å detektere avvik på enkeltmålinger fra prosessen eller enkelte utstyrskomponenter.

Sammensatte alarmer (aggregated alarms) genereres ved å kombinere tilstanden til et antall basisalarmer på en slik måte at tilstanden til en prosessdel beskrives mer presist enn hva basisalarmer kan beskrive.

Modellbaserte alarmer (model-based alarms) er generert basert på online simuleringer av matematiske modeller av definerte prosesselementer.

Nøkkelalarmer (key alarms) er et utvalg av spesielt viktige alarmer som presenteres på en slik måte at de er tilgjengelige også under alarmras. Alle viktige sikkerhetsrelaterte alarmer skal defineres som nøkkelalarmer, men det kan også være hensiktsmessig å definere andre alarmer som nøkkelalarmer.

Alarmbehandling og håndtering

Signalfiltrering er prosessering av inngangssignalene til alarmsystemet for å fjerne målestøy og annen informasjon som er uviktig for alarmsystemets formål, f.eks. små, hurtige oscillasjoner.

Signalvalidering (*signal validation*) brukes for å verifisere at informasjonen fra et signal er pålitelig, og er tilgjengelig fra smarte transmittere eller spesiell software for signalovervåkning.

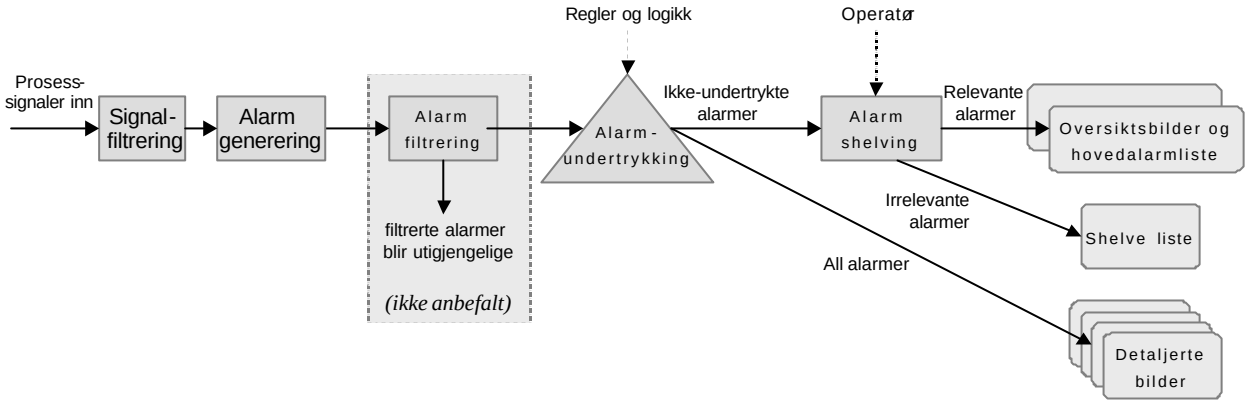
Alarmfiltrering (*alarm filtering*) er automatisk prosessering som i spesielle prosesstilstander gjør et alarmsignal utilgjengelig i hele systemet.

Alarmundertrykking (*alarm suppression*) er en automatisk prosessering som i spesielle prosesstilstander hindrer et irrelevant alarmsignal i å presenteres i hovedbilder for operatøren, men hvor tilstanden til alarmen fortsatt er tilgjengelig i mer detaljerte bilder

Manuell alarmundertrykking (alarm shelving) er en fasilitet for manuell fjerning av en alarm fra hovedalarmlisten ved at den overføres til en egen liste, slik at den forhindres fra å dukke opp igjen på hovedlisten helt til den er fjernet fra denne listen. Manuell undertrykking er normalt styrt av operatøren, og er tenkt å fungere som en "siste utvei" for å håndtere irrelevante problemalarmer som slipper gjennom til operatøren til tross for signalfiltrering og alarmundertrykking.

Inhibit og *blocking* betyr det samme og er relevante kun for aksjonsalarmer. Dette betyr å hindre shutdown aksjon ved å koble ut signalet fra alarm til shutdown-logikk, mens alarmtilstanden presenteres til operatøren.

Overbroing (override) betyr å koble ut signalet fra shutdown-logikken til en individuell shutdown aksjon. Selv om dette ikke direkte er relatert til alarmer er en overbroing en potensielt risikabel utkobling av en del av sikringssystemet, og representerer derfor en viktig unormalitet som bør vurderes ved utforming av oversikter over nøkkelinformasjon.



Figuren over viser sammenhengen mellom ulike prosesserings- og håndteringsmekanismer.

Andre definisjoner og begreper

Alarmprioritering er en kategorisering basert på viktigheten av alarmer for operatørens oppgaver.

Alarmrate er et mål på hvor mange alarmer som presenteres for operatøren per tidsenhet. Dette er en viktig indikator for å undersøke hvorvidt alarmsystemet i ulike situasjoner er anvendbart for operatørene eller om disse overbelastes med informasjon.

Oversiktsbilder er utformet for å hjelpe operatører å få en oversikt over prosesstilstanden. Oversiktsbilder kan omfatte: Hovedalarmliste, alarmtablå/tiles, og storskjermbilder for visning av nøkkelinformasjon.

Selektive lister viser kun et utvalg av den tilgjengelige alarminformasjonen, basert på utvalgs- og sorteringskriterier som kan settes opp av operatøren under drift.

Konseptuell enhet: En informasjonsenhet (prosess-, oppgave-, eller systemrelatert) som benyttes av operatørene i mental prosessering, slik som en sammenligning av en temperaturmåling mot en alarmgrense.

Sammensatt konseptuell enhet: Inneholder informasjonsstrukturen og innholdet til flere konseptuelle enheter, men er i seg selv en separat konseptuell enhet, slik som en kompressor-trip.

Persepsjon: Med persepsjon menes oppfatting av sanseinntrykk. For at en skal kunne oppfatte alarminformasjon på en best mulig måte, er det viktig at denne skiller seg klart ut fra annen informasjon og det må være lett å oppfatte de essensielle elementene i informasjonen (hva er galt, hvor alarmeres det, hvor alvorlig er det - dvs. de elementer som er vesentlig for den videre kognitive prosesseringen)

Kognitiv prosessering: Prosessering av ny informasjon i den menneskelige hjerne basert på tidligere ervervet kunnskap (lagrede data). Hvor effektivt prosesseringen skjer er avhengig av hvordan vi oppfatter inngående informasjon (vår persepsjonsevne) samt på hvilken form kunnskapen som benyttes i prosesseringen er lagret og hvordan den kan hentes ut (f.eks. ved enkel gjenkjenning eller krevende gjenkalling).

Kognitiv respons: En type respons der operatøren ikke utfører noen fysisk handling, men som krever at det gjøres en mental prosessering av informasjon.

2 FUNKSJONSKRAV

2.1 Formået med alarmsystemet

Alarmsystemet er et primært operatørstøttesystem for varsling og håndtering av unormale situasjoner, og har to grunnleggende funksjoner:

Hovedfunksjonen til alarmsystemet er å varsle operatøren om en unormal situasjon [3]

Varslingsfunksjonen hjelper operatøren til å påvirke den fremtidige utviklingen i et komplekst prosessanlegg ved å rette oppmerksomheten mot uønskede forhold i prosessen.

Systemet skal informere operatøren om forhold som krever vurdering og eventuelt inngrep i rett tid for å opprettholde ønsket prosesstilstand med hensyn på sikkerhet, produksjon, miljø og effektivitet/optimal drift.

Hver alarm skal varsle, informere og veilede operatøren. [1,3]

Alarmer skal:

- Være relevante i forhold til operatørens rolle til enhver tid
- Vise hvilken respons som kreves
- Presenteres med en alarmrate som operatøren kan håndtere
- Være lette å forstå

Den sekundære funksjonen til alarmsystemet er å fungere som en alarm- og hendelseslogg [3]

Logg-funksjonen hjelper operatøren ved analyse av en sekvens av hendelser som har ført til nåværende eller tidligere prosesstilstander.

Alarmloggen brukes til analyse av hendelser og til optimalisering av driften av anlegget.

Alarmloggen skal bære fleksibel og også inneholde hendelser, undertrykte alarmer og annen informasjon som ikke ble presentert i hovedalarmlisten, men som kan ha nytteverdi i en etterundersøkelse av en hendelse.

Informasjon fra alarmloggen kan også brukes til overvåking og forbedring av kvaliteten og ytelsen til alarmsystemet.

Alarmsystemet må gi *nyttig* informasjon og tilby nyttig funksjonalitet for å kunne støtte operatørens oppgaver. For å være *anvendelig* for operatøren må informasjon i tillegg presenteres og håndteres på en måte som tar hensyn til menneskelige evner og begrensninger

I tillegg til alarmsystemet vil flere andre informasjonskilder være viktige for å hjelpe operatørene å håndtere unormale situasjoner, som f.eks. trendsystem, videoovervåkning, oversiktsbilder, prosessimulering, og avanserte operatørstøttesystemer for tilstandsovervåkning, diagnose, eller elektroniske prosedyrer.

2.2 Generelle krav

1) Alarmsystemet skal eksplisitt utformes for å ta hensyn til menneskelige faktorer og begrensninger [3]

Dette skal sørge for at alarmsystemet forblir anvendelig i alle prosesstilstander, ved å hindre at operatørenes perseptuelle og kognitive begrensninger overskrides.

Alarmer skal alltid presenteres i en rate som gjør det mulig for operatørene å gjenkjenne og forstå alarmene, og det må være tilstrekkelig tid for operatørene å utføre nødvendig respons.

Perseptuelle faktorer:

Den menneskelige hjernes oppfatningsevne er begrenset. Det tar alltid en viss tid å oppfatte ting, og vi kan bare holde på 7±2 ulike informasjonsenheter samtidig. Derfor er det viktig at det for alle sannsynlige ulykkesscenarier bør kunne demonstreres at det totale antallet sikkerhetsrelaterte alarmer og den maksimale raten disse presenteres med ikke vil overbelaste operatøren.

Kognitive faktorer:

Dersom flere informasjonsenheter kan settes sammen til en meningsbærende enhet (f.eks. en sammensatt alarm), kan hjernen frigjøre kapasitet slik at vi kan oppfatte mer informasjon. Hjernen har også andre hjelpemidler som gjør at vi kan øke oppfatningskapasiteten, som blant annet kan støttes gjennom et intuitivt meningsinnhold og mønstergjenkjenning i informasjonen som presenteres.

Informasjonen som presenteres i alarmsystemet bør være effektiv og verdifull for operatøren:

- Det bør brukes så mange sammensatte konseptuelle enheter som mulig
- Sammensatte konseptuelle enheter bør brukes for undertrykking av informasjon med mindre meningsinnhold
- Innholdet i alarmmeldingen må være slik at den minimaliserer behov for gjenkalling av informasjon fra vår langtidshukommelse. Eksempelvis vil ikke en operatør kunne gjenkalle eller gjenkjenne 5000 tag nr. Derfor må det også finnes annen og mer beskrivende informasjon enn tag nr. i alarmmeldingen

Utførelse av aksjoner:

Ethvert krav til aksjon fra operatøren som respons til en alarm skal være basert på realistiske ideer om hva operatørene kan forventes å gjøre i den aktuelle situasjonen.

Alarmsystemet skal tilpasses til oppgavene som er definert for operatørene. Disse kan f.eks. være identifisert og beskrevet gjennom systematiske oppgaveanalyser.

2) Alarmsystemet skal være kontekstavhengig [1,2,3]

Alarmer skal være relevante og fortjene operatørens oppmerksomhet i alle prosesstilstander og driftsforhold hvor de vises.

Alarmsystemet skal designes for å støtte de ulike oppgavene til operatøren i en driftsforstyrrelse. Det skal tilpasse seg varierende informasjonsbehov og være anvendelig i alle prosesstilstander, slik som:

- Oppstart
- Normal drift
- Mindre driftsforstyrrelser
- Større driftsforstyrrelser
- PAS utløst og nedstenging pågår

- Etter PAS er sluttført
- Brann/gass varsel
- NAS utløst og nedstenging pågår
- Trykkavlastning

Eksempel: Idet en NAS utløses vil måltilstanden for prosessen og operatørenes oppgaver og prioriteringer endres betydelig. Alarmsystemet skal tilpasse seg denne endringen og presentere kun informasjon som er relevant i nåværende situasjon, slik som ventiler som ikke stenger som de skal o.l. Det store antallet alarmer som kan forventes som resultat av at prosessen stenger ned (lavt trykk, flow osv.) er i denne situasjonen irrelevante som alarmer, og skal undertrykkes fra hovedbildene som operatøren bruker. Etter at nedstengningen er fullført kan man koble inn spesielle alarmer som har som formål å detektere unormal utvikling i nedstengte prosessegmenter.

Kontektstavhengighet kan oppnås gjennom omfattende bruk av alarmundertrykking og/eller dynamiske alarmgrenser.

3) Operatørene skal ha opplæring og systematisk trening i all realistisk bruk av alarmsystemet [1,3]

Systematisk opplæring og trening skal sikre at operatørene fullt ut kjenner og forstår funksjonaliteten i systemet og bruken av dette.

Grunnleggende opplæring bør dekke følgende områder:

- Regler for alarmprioritering
- Undertrykkingsmekanismer
- Alarmsystemets brukergrensesnitt
- Praksis for akseptering av alarmer

Bruken av alarmsystemet under en større forstyrrelse vil typisk være svært forskjellig fra å bruke systemet under normal drift. Regelmessig og realistisk trening, slik som simulatortrening, bør derfor gjennomføres for å sikre at operatørene vil være i stand til å bruke alarmsystemet i de ulike situasjonene.

For at alarmundertrykking skal være en effektiv støtte for operatørene, trenger operatørene praktisk erfaring for å få tillit til undertrykkingsmekanismene som benyttes i systemet.

4) Alarmsystemet skal baseres på en alarmfilosofi [3]

Alarmfilosofien skal sikre at de grunnleggende prinsippene og begrunnelsene for de beslutninger som er gjort i designet av alarmsystemet er dokumenterte.

Alarmfilosofien bør beskrive:

- Funksjonene til alarmsystemet: Varsling og logging
- Operatørens rolle: Hvordan denne endrer seg med prosesstilstanden og hvilken støtte operatøren trenger i de ulike prosesstilstandene
- Hvordan systemet skal designes for å ta hensyn til menneskelige begrensninger
- Bruken av alarmprioriteter: Formålet med prioritering, hvordan prioriteter er definert i systemet, og begrunnelsene for disse definisjonene.
- Praksis for akseptering av alarmer: Formålet med akseptering av alarmer, og hvordan operatørene skal trenes til å praktisere dette
- Standarder
- Prinsipper for generering av alarmer
- Prinsipper for strukturering av alarmer
- Presentasjonsteknikker og medier

Viktige prinsipper i alarmfilosofien bør omfatte:

- Hver alarm skal kreve en respons fra operatøren
- Operatøren skal gis tilstrekkelig tid til å utføre den nødvendige respons

5) Alarmsystemet skal være godt dokumentert, og det skal være etablert klare roller og ansvarsforhold for vedlikehold og forbedringer i systemet [3]

Dokumentasjonen skal sikre at det etableres og opprettholdes god praksis gjennom endringer i systemet, og at utviklere og brukere av systemet har en felles forståelse av funksjonaliteten i systemet. Den skal også sørge for at hver alarm som er definert i systemet er dokumentert med beskrivelse av formålet med alarmen og en vurdering av hvor kritisk alarmen er. Klare roller og ansvarsforhold skal sørge for å definere eierskap til alle problemer og oppgaver knyttet til alarmsystemet gjennom hele livsløpet til systemet.

I tillegg til alarmfilosofien, som er beskrevet tidligere, skal alarmdokumentasjonen omfatte følgende:

Strategi for alarmdesign: Dette skal baseres på alarmfilosofien, og skal beskrive en strukturert metodikk for utvikling av alarmsystemet som sikrer at hver alarm er velbegrunnet, rett konfigurert og dokumentert. Viktige emner er: Involvering av sluttbrukere/operatører, identifisering av brukernes behov, ytelseskrav til systemet, veiledning til underleverandører med hensyn til design av alarmer, ordliste med begreper og forkortelser for bruk i alarmmeldinger.

Strategi for forvaltning av alarmsystemet: Beskriver fordeling av roller og ansvar i forhold til vedlikehold og oppfølging av alarmsystemet, i tillegg til prosedyrer for å føre tilsyn med systemet, overvåkning av ytelsen til systemet, vedlikehold, testing, endring og modifikasjon og dokumentasjon av systemet.

Dokumentasjon av hver enkelt alarm: Systemet bør være selv-dokumenterende, og inneholde detaljert informasjon om hver alarm (formålet med alarmen, og hvordan den er konfigurert med hensyn på undertrykkingslogikk osv.)

6) Det skal være lett for prosesseksperter å bygge inn og vedlikeholde kunnskap og intelligens i alarmsystemet gjennom hele livssyklusen til systemet [1]

For å oppnå et godt alarmsystem kreves det at mye prosesskunnskap bygges inn i systemet for å optimalisere alarmgenerering, undertrykking og presentasjon, basert på prosessekspertise og driftserfaring.

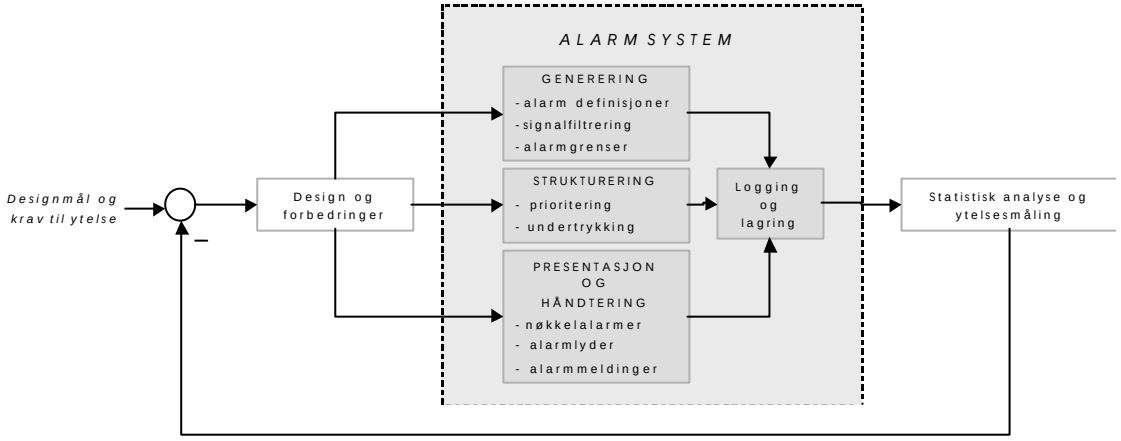
Verktøy for konfigurering av alarmsystemet bør være tilgjengelig, som gjør det lett for brukere med bakgrunn som prosessingeniør o.l. å forbedre systemet over tid, ved å legge inn den nødvendige kunnskapen som skal til for å få effektiv undertrykking av alarmer og tilpassing av parametre for signalfiltrering, alarmgrenser og prioriteter.

7) Det bør stilles ytelseskrav til alarmsystemet [3]

Ytelseskrav er viktig for å sikre at alarmsystemet er nyttig og anvendbart for operatørene i alle relevante operasjonelle situasjoner. For å møte kravene må det foretas ytelsesmålinger som skal brukes som input til et kontinuerlig arbeid med forbedring av alarmsystemet.

Et system for måling av ytelsen til systemet bør være tilgjengelig. Dette skal fungere som et verktøy som implementerer ulike metoder for måling av ulike ytelsesindikatorer i systemet. Systemet bør brukes til å utføre regelmessige analyser for å identifisere problemer og svakheter i alarmsystemet både i normal drift og under prosessforstyrrelser.

Denne informasjonen bør brukes i en kontinuerlig forbedringsprosess. Dersom en prosessimulator er tilgjengelig, bør ytelsesovervåknings-systemet brukes sammen med simulatoren for å justere og optimalisere alarmgrenser, signalfiltering, alarmundertrykking osv. i et bredere utvalg av drifts- og avvikssituasjoner enn hva man har tilgjengelig fra historikken til det virkelige anlegget.



Figur: Forbedringsprosessen for alarmsystemet illustrert som en tilbakekoplingssløyfe. Ulike online og offline mål brukes til å verifisere at ytelsen til systemet er tilfredsstillende, og avvik fra designmålene og -kravene fungerer som input til endringer og forbedringer av systemet.

Ytelsen til systemet bør vurderes i designfasen og igangkjøring for å sikre at det er anvendelig og effektivt i alle driftstilstander. Gjennom resten av livssyklusen til anlegget bør det føres regelmessig tilsyn med systemet for å gjøre de nødvendige modifikasjoner og forbedringer for å sikre at akseptabel ytelse opprettholdes.[3]

Viktige ytelsesindikatorer inkluderer:

- Rate av innkommende alarmer (med prioritetsfordeling)
- Antall alarmer i hovedalarmlisten (med prioritetsfordeling)
- Frekvensfordeling av alarmer: For å identifisere spesielle problemalarmer som bidrar betydelig til alarmbelastningen.
- Operatørenes responstider (tid før alarmer aksepteres) : For lange eller korte responstider tyder på at systemet ikke brukes slik det er tenkt.

Alarmrater under stabile driftsforhold:

Gjennomsnittlig alarmrate	*Konsekvens*
Mer enn 1 alarm i minuttet	Klart uakseptabelt
En alarm annet hvert minutt	Sannsynligvis for krevende

En alarm hvert femte minutt	Håndterbart
Færre enn en alarm hvert 10. minutt	Klart akseptabelt

Alarmrater under større driftsforstyrrelser:

Gjennomsnittlig alarmrate	*Konsekvens*
Mer enn 10 alarmer i minuttet	Definitivt for mange alarmer, operatører vil sannsynligvis oppgi bruken av systemet
2-10 alarmer i minuttet	Vanskelig å håndtere
Færre enn en alarm i minuttet	Burde være håndterbart, men kan være vanskelig dersom flere alarmer krever en kompleks operatørrespons.

Det bør verifiseres at prioritetsfordelingen for alarmer som forekommer i en driftsforstyrrelse er slik at den faktisk hjelper å fokusere på noen få viktige alarmer til enhver tid.

Andre loggede operatøraksjoner kan også analyseres statistisk for å finne mulige problemalarmer, ved å identifisere alarmer som ofte undertrykkes manuelt eller alarmgrenser som ofte endres.

8) Det bør finnes et administrativt system for å håndtere tilgangskontroll og dokumentering av endringer som utføres i alarmsystemet

Det administrative systemet skal hindre at det kan gjøres uautoriserte endringer i systemet og skal sikre at alle endringer er sporbare og tilstrekkelig dokumentert.

Systemet skal administrere alle endringer og justeringer i alarmsystemet, slik som endring av alarmgrenser, manuell undertrykking og inhibitering. Et integrert system bør kreve at visse opplysninger må oppgis før endringene trer i kraft, som f.eks:

- Ansvarlig person for endringen
- Bakgrunnen for at endringen gjøres
- For midlertidige endringer: Forventet varighet, med automatisk varsling når denne tiden har utløpt.

Mekanismer for tilgangskontroll bør gjøre det enkelt for operatører å gjøre endringer i ikke-kritiske alarmer, mens spesiell autorisasjon kreves for å gjøre endringer som er mer kritiske.

Det bør eksistere prosedyrer og systemer for rapportering av hendelser, mangler og mulige problemer relatert til alarmsystemet. Det bør være klart definert hvem som er ansvarlig for oppfølging av slike rapporter.

9) Alarmsystemet bør være feiltolerant

Et feiltolerant system skal sikre at sikkerhetskritisk informasjon alltid vil være tilgjengelig for operatørene, både i normal drift og i krisesituasjoner.

Faktorer som bør vurderes omfatter: redundant CPUm I/O og bus-system, UPS som backup for elektronisk utstyr og skjermer. Alarmsystmet skal evalueres kritisk og tilordnes et Safety Integrity Level (SIL klasse) i henhold til IEC 61508.

10) Responstiden i systemet skal ikke overstige 2 sekunder [4]

Kort responstid i systemet er av vesentlig betydning for at systemet skal forbli nyttig og anvendbart i kritiske situasjoner med stor belastning på operatørene.

Alarmer bør presenteres i hovedalarmbilder innen 2 sekunder etter aktivering.

For presentasjon i hovedalarmliste er det tilstrekkelig med en tidsoppløsning på 1 sekund. For presentasjon i alarm- og hendelseslogg og for bruk i undertrykkingslogikk vil en oppløsning på 100 ms og bedre være påkrevet.

11) Sikkerhetskritiske funksjoner bør identifiseres og dokumenteres. Statusinformasjon og feilalarmer fra disse funksjonene bør presenteres klart og tydelig på faste plasser i permanente oversiktsbilder

Dersom sikkerhetskritiske funksjoner er degradert eller truet, bør operatørene bli varslet umiddelbart på grunn av de mulige konsekvensene av denne typen problemer.

Eksempler på slike funksjoner kan være (men er ikke begrenset til):

- Statusinformasjon og feilalarmer fra nødstrøm system
- Statusinformasjon og feilalarmer fra brannpumper
- Brannbekjempingssystemer: Statusinfo (utløst, tilgjengelig) og feilalarmer (ikke utløst på kommando, lavt trykk i brannvannsledning osv.)
- Fakkel og trykkavlastingsystem

De sikkerhetskritiske funksjonene bør vises på et høyt abstraksjonsnivå gjennom å kombinere relevant informasjon i en enkel grafiske presentasjon som gir operatører en rask oversikt over tilgjengelighet og status for en funksjon.

12) Statusinformasjon fra sikkerhetssystemets funksjoner, slik som blokkering/inhibitering og overbroinger, skal være lett tilgjengelig på dedikerte lister og i prosessbildene

Det er svært viktig at operatørene kan få en rask oversikt over alle inhibiteringer og overbroinger som er aktivert i sikkerhetssystemet, med tidspunkt for aktivering, hensikten med aktiveringen, forventet varighet og ansvarlig person.

Denne typen aksjoner er viktige midlertidige endringer i systemet og bør kontrolleres av et administrativt system for håndtering av tilgangskontroll og dokumentering av hver enkelt endring.

2.3 Generering av alarmer

13) Enhver alarm skal kreve respons fra operatøren [1,3]

Dette er for å sikre at ingen unødvendige alarmer er definert i systemet.

En respons kan være et fysisk inngrep for å manipulere prosesstilstanden, kontakte feltoperatør, instrumentteknikere osv. Det kan også være en rent kognitiv respons der operatøren kun prosesserer informasjon mentalt.

En statusendring som aldri vil kreve noen respons fra operatøren skal defineres som en hendelse/event, og ikke som en alarm. Varsler om forhold som kontrollromsoperatøren ikke kan respondere på direkte bør i stedet føres direkte til rette personell.

14) Alarmsystemet skal kunne generere basisalarmer [1,3]

Basisalarmer gjør det mulig å detektere enkle forstyrrelser i prosessen.

Systemet må være tilrettelagt for å kunne generere følgende alarmtyper:

- Vanlige tilstandsvariabel-alarmer som sammenligner en analog måling med predefinerte statiske eller dynamiske alarmgrenser.
- Binære alarmbrytere
- Rate-of-change / endringsrate alarmer
- Komponentfeil-alarmer (f. eks. indikering av uoverensstemmelse mellom kontrollsignal og tilbakemelding, signal giver feil etc).
- Systemalarmer som indikerer feil i alarm eller prosesskontrollsystemet
- Enkle gruppealarmer

15) Alarmsystemet bør kunne generere sammensatte alarmer og modellbaserte alarmer [2]

Denne typen alarmer skal bare brukes når de kan gi en betydelig reduksjon i antallet presenterte basisalarmer gjennom undertrykking av disse, eller når de leder mer direkte mot årsaken til et problem i stedet for symptomene på problemet.

Sammensatte alarmer kan omfatte:

- Anleggdel tilstand alarm (kompressortrip o.l)
- Manglende alarmer når forventede følgealarmer ikke kommer inn
- Funksjonsalarmer (tap av kjøling o.l.)

Modellbaserte alarmer kan omfatte:

- Tidlig feildeteksjon ved å sammenligne virkelige måleverdier med beregnede målinger fra en simulert feilfri prosess.
- Bruk av informasjon fra modellbaserte regulatorer for å detektere unormale endringer i prosessdynamikken.

16) Alle alarmgrenser bør være systematisk fastsatt og dokumenteres under design av anlegget, igangkjøring og drift [3]

Korrekte alarmgrenser er viktige for å sikre at alarmer utløses tidlig nok til at operatørene får tid til å utføre en effektiv respons, samtidig som antallet unødige alarmer minimaliseres.

Alarmgrenser bør settes basert på

- Dynamikken i prosessen
- Nedstengings-grenser
- Sannsynlig endringsrate for signalet ved en driftsforstyrrelse
- Tiden det vil ta for operatøren å reagere og korrigere problemet som har ført til alarmen

17) Det kan være mulig for operatører å endre enkelte alarmgrenser [3]

Dette er for å gjøre systemet mer fleksibelt og anvendelig ved at operatørene kan tilpasse alarmsystemet til varierende driftsbetingelser.

Et administrativt system bør brukes til å hindre uautoriserte endringer og for å sikre at hver endring er dokumentert med en begrunnelse og ansvarlig person.

18) Signalfiltrering bør brukes [2,3]

Signalfiltrering brukes til å hindre at måleverdier som fluktuerer rundt sine alarmgrenser vil generere gjentatte, unyttige alarmer som forstyrrer operatøren unødig og bidrar til alarmras.

Analoge målinger bør lavpass-filtreres for å fjerne målestøy og annen informasjon i frekvensområder som ikke er til nytte i et alarmsystem. Filterfrekvensen skal være individuelt justerbar for hvert målesignal.

Dødbånd/hysterese bør brukes for å hindre en alarm i å gå av og på når målingen svinger i et ubetydelig lite område rundt alarmgrensen. Dødbåndet skal være individuelt justerbart.

Tidsforsinkelser og tidsbegrensninger bør brukes til å unngå uønskede alarmer fra digitale alarmbrytere uten tilstrekkelig innebygget dødbånd. Forsinkelser og tidsgrenser skal være individuelt justerbare.

19) Signalvalidering bør brukes [1]

Dersom dette er tilgjengelig bør signalvalidering brukes til å sikre at inngangssignalene til alarmsystemet er pålitelige.

Informasjon om påliteligheten til målesignaler kan være tilgjengelig fra smarte transmittere eller fra spesiell programvare for signalvalidering.

Operatøren bør varsles om upålitelige signaler i den grad dette vil ha direkte innvirkning på hans oppgaver, og informasjonen som gis skal være relevant og forståelig for en operatør.

Mekanismene for alarmundertrykking skal lages slik at ingen alarmer vil undertrykkes av et upålitelig signal.

2.4 Strukturering av alarmer

20) Det bør være mulig å selektere, gruppere og sortere alarmer

Muligheter for seleksjon, sortering og gruppering av alarminformasjon bør være tilgjengelig for å gjøre systemet fleksibelt og anvendelig ved å gi operatørene mulighet for online konfigurering av spesielle utvalg av informasjon som de ønsker å få presentert, basert på spesielle behov.

Kriterier for gruppering og sortering kan være:

- Tid
- System
- Område
- Ansvarlig operatør
- Prioritet

Det bør også være enkelt å få en oversikt over alarmer som er automatisk eller manuelt undertrykt, eller som er inhibitert.

21) Systemet skal inneholde alarmundertrykkings-funksjoner [1,3]

Formålet med alarmundertrykking er å sikre at alarmene som presenteres til enhver tid er relevante for operatørens oppgaver i nåværende prosesstilstand, og for å hindre alarmras under driftsforstyrrelser.

Prinsipper for alarmundertrykking bør være enkle å forstå.

Eksempler på undertrykkingsprinsipper som kan anvendes er:

- Undertrykk alarmer som kommer fra testing.
- Undertrykk alarmer som er direkte konsekvenser av andre alarmer i en forstyrrelse. Unntak fra dette kan være nøkkelalarmer.
- Undertrykk overflødige/redundante alarmer i tilfeller der flere alarmer varsler om det samme avviket.
- Undertrykk alarmer som kommer fra f. eks fra komponenter i ustand, komponenter som er utilgjengelige pga. vedlikehold, testing osv.
- Bruk undertrykking basert på driftstilstanden til de enkelte prosessystemene og tilstanden i sikkerhetssystemet.
- Bruk first-out prosessering av nedstengings-alarmer: Presenter kun den ene alarmen som utløser en nedstenging, og undertrykk alle andre alarmer som kun er naturlige følger av de automatiske nedstengings-aksjonene.
- Dersom alarmundertrykkingen baserer seg på et signal som ikke er pålitelig så skal ingen alarmer undertrykkes.

22) Alarmsystemet skal benytte alarmundertrykking, ikke alarmfiltrering[1]

Selv om en aktiv alarm i nåværende driftstilstand ikke er et relevant varsel om noe unormalt, så kan alarmen likevel utgjøre viktig statusinformasjon for bekreftelse av prosesstilstanden som bør være tilgjengelig for operatøren i detaljerte eller selektive bilder. Det bør derfor være mulig å undertrykke en alarm fra oversiktsbildene samtidig som alarmen fortsatt er tilgjengelig i detaljerte bilder.

Alarmundertrykking, i motsetning til *alarmfiltrering*, fjerner ikke informasjonen helt fra systemet. Undertrykking vil kun separere alarminformasjonen i et oversiktsnivå og ett eller flere detaljerte nivåer.

Dette sikrer at informasjonsmengden og raten som informasjonen presenteres med på oversiktsnivået kan optimaliseres til å ta hensyn til menneskelige begrensninger i hektiske situasjoner. Dermed sikrer man at alarmer alltid kan presenteres på en måte som gjør det mulig for operatøren å oppfatte disse. Samtidig vil mye mer informasjon være tilgjengelig i detaljerte bilder dersom operatøren henter opp disse.

23) Alarmundertrykkingen i systemet bør være kjent for operatørene, og den bør være dokumentert på en lett forståelig måte [1]

For å kunne stole på systemet må operatørene forstå hvorfor noen alarmer er undertrykte, mens andre ikke er det.

For å bli kjent med et alarmsystem med en høy grad av undertrykking kreves det:

- Grunnleggende opplæring og dokumentasjon som beskriver de generelle undertrykkingsmekanismene som finnes i systemet
- Lett tilgjengelig dokumentasjon av undertrykkingskriteriene som er konfigurert for hver alarm
- Systematisk trening i bruk av systemet i alle typer driftsforhold der undertrykkingsmekanismene blir aktivert

2.5 Alarmprioritering

24) Alarmer skal prioriteres [1,3]

Hensikten med alarmprioritering er å hjelpe operatøren til å bestemme hvilke alarmer som bør tas hånd om først når flere alarmer kommer inn samtidig i en driftsforstyrrelse, og for å fremheve spesielt viktige alarmer i normal drift.

Det anbefales å ikke bruke mer enn fire alarmprioriteter i et anlegg.

Maksimum tre prioriteter bør brukes innenfor en gitt type bilde for normal alarmpresentasjon. Et ytteligere prioretsnivå kan benyttes for sikkerhetskritiske alarmer.

Der det er flere alarmsystemer i ett og samme kontrollrom bør definisjonen og presentasjonen av prioriteter være slik at det er konsistens mellom alle de ulike systemene.

Det bør ikke være mulig for operatører å endre alarmprioriteter, men det skal være mulig å gjøre dette for personell med spesiell tillatelse.

25) Alarmer skal prioriteres basert på konsekvensene som operatørene kan forhindre ved å utføre korrigerende tiltak [1,3]

Alarmprioritet skal hjelpe operatøren å fokusere på de forholdene som, dersom de ikke korrigeres i tide, vil få de største konsekvensene.

Høy prioritet bør brukes til å alarmere forhold i prosessen som kan få store konsekvenser dersom ikke operatøren retter opp forholdet.

Konsekvensenes alvorlighetsgrad bør baseres å hensynet til sikkerheten til personell, beskyttelse av ytre miljø, beskyttelse av utstyr, og opprettholdelse og optimalisering av produksjon.

26) Alarmer skal prioriteres i henhold til hvor lang tid som er tilgjengelig for å utføre en vellykket korrigerende handling [1,3]

Alarmprioritet skal hjelpe operatøren å fokusere på de prosessforholdene som det vil være tid å gjøre noe med, og spesielt på de forholdene som det haster med å ta hånd om.

Høyere prioriteter skal alarmere forhold i prosessen som krever oppmerksomhet eller aksjon innen et begrenset tidsrom for å unngå konsekvenser.

For høyprioritets alarmer skal det være tilstrekkelig tid tilgjengelig til at operatøren kan handle effektivt for å unngå konsekvenser. Eksempel på alarmer som ikke bør være høyest prioritert er trip-alarmer som varsler om at en prosessavstenging er blitt utløst, ettersom den uønskede konsekvensen på dette tidspunktet allerede har inntruffet.

Lavere prioriteter bør brukes for avvik hvor det haster mindre med å utføre korrigerende aksjon.

27) Prosessalarmene som kommer inn under normal drift og i driftsforstyrrelser bør ha en effektiv fordeling av prioriteter [3]

Dette er for å sikre at alarmprioriteringen vil være til hjelp for operatørene i driftsforstyrrelser. Blant det store antallet alarmer som kan forekomme i slike situasjoner bør det være en relativt liten og håndterbar andel av høyprioritets alarmer som leder oppmerksomheten mot de mest viktige og presserende prosessavvikene som bør tas hånd om til enhver tid.

Tilordning av prioriteter bør gjøres ut fra klart definerte mål for hvordan prioritetsfordelingen for innkommende alarmer bør være. Det anbefales at frekvensen som de ulike prioritetene forekommer med bør avta med en faktor på omkring 5 for hver økning i prioritet, slik at ca. 80% av alarmene som forekommer er laveste prioritet, 15% nest laveste, 5 % høy prioritet osv.

28) Hvert anlegg bør ha skriftlige regler for tilordning av prioriteter [3]

Dette skal sikre at operatørene er kjent og fortrolig med hvordan prioriteter er satt i systemet, slik at denne informasjonen er en effektiv støtte for operatørene ved håndtering av alarmer.

Felles prioriteringsregler skal anvendes på en konsistent måte for alle alarmer i alle systemer som brukes av operatørene.

Prioriteringsregler med begrunnelser bør inngå som en del av alarmfilosofien.

2.6 Alarmpresentasjon

29) Et hovedalarmbilde skal være tilgjengelig [1,3]

Hovedalarmbildet skal støtte operatørens oppgaver i forhold til overvåkning og styring av den fremtidige utviklingen i prosessen ved å lede oppmerksomheten mot forhold i prosessen som krever vurdering eller aksjon. Det skal kun vise alarmer som er relevante i den aktuelle driftssituasjonen.

Hovedalarmbilder skal presentere alle aktive alarmer som ikke er automatisk eller manuelt undertrykket. Et viktig designmål for hele alarmsystemet er at *ingen alarmer presenteres* i hovedalarmbildet i situasjoner der det ikke er reelle problemer eller unormaliteter i prosessen som skal/kan håndteres av operatøren (det såkalte "mørk skjerm"-prinsippet).

Hovedalarmbildet skal være anvendelig under alle driftsforhold som det er laget for å dekke. Dette gjøres gjennom å presentere alarminformasjon på en form og i en rate som operatøren klarer å håndtere og nyttiggjøre seg av (ref. kravene 1 og 7 for anbefalte maksimumsrater).

For hver alarm bør det være lett å se prioritet og alarmtilstand (ny, akseptert, utgått).

Alarmlister bør være kronologisk ordnet, og ha funksjonalitet som sikrer at repeterende alarmer ikke fører til at listen blir ubrukelig (ved at samme alarm kan fylle opp flere linjer i listen).

Alarmtablå/tiles er bilder med alarmer vist på fast plass, og viser ikke den kronologiske rekkefølgen for aktive alarmer, men har den fordel at operatørene kan dra nytte av mønstergjenkjenning som gjør det mulig å effektivt håndtere og holde oversikt over et stort antall alarmer.

Et hovedalarmbilde kan være en kombinasjon av en liste og tiles, eller separate bilder som dekker ulike systemer og områder. Løsningen som velges for hovedalarmbilde skal baseres på en anerkjent drifts- og alarmfilosofi.

30) Nøkkelalarmer skal vises i oversiktsbilder som er permanent synlige, med alarmene vist på faste plasser [1,3]

Hensikten med nøkkelalarmer er å forbedre håndteringen av typiske alarmras-situasjoner. Alarmpresentasjonen skal ikke basere seg utelukkende på alarmlister for å gi oversikt over alarmsituasjonen. Alarmlister vil alltid ha mulighet for å overfylles med informasjon i større forstyrrelser, selv om tiltak slik som alarmundertrykking skal benyttes for å forhindre dette så langt som mulig. Nøkkelalarm-bilder sikrer både en informasjonsrate og presentasjonsform for de viktigste alarmene som gjør det mulig å beholde oversikten i alle situasjoner.

Nøkkelalarmer skal omfatte alle alarmer som er direkte sikkerhetsrelaterte (f.eks. brann/gass alarmer) og viktige prosessalarmer relatert til sikkerhetskritiske systemer (f.eks. høyt nivå i fakkel væskeutskiller).

Det kan også være hensiktsmessig å inkludere andre høyprioritets prosessalarmer som nøkkelalarmer. Et nøkkelalarmdisplay kan på den måten være nyttig for å unngå unødvendige nedstengninger ved å gi bedre oversikt over kritiske prosessalarmer i store forstyrrelser som er typiske alarmras-situasjoner der viktige alarmer ellers vil kunne overses i en alarmliste (f.eks. høyt nivå i separator). Dersom denne overses vil en full produksjonsnedstengning utløses idet høy-høy alarm nås.

Skjermbilder som egner seg til visning av nøkkelalarmer er:

- Alarmtablå/tiles [3]
- Oversiktsbilder for storskjerm som viser nøkkelalarmene integrert med annen viktig prosessinformasjon [1]

31) En historisk logg av alarmer og hendelser bør være tilgjengelig for operatørene [1,3]

Loggen brukes til å analysere hendelsesforløp.

Alarmloggen bør ha fleksibel funksjonalitet for seleksjon, sortering, gruppering og søking.

32) Alarmer bør integreres i prosessbildene [1,3]

Ved å kombinere relevant prosess- og alarminformasjon vil den mentale arbeidsbelastningen for operatørene reduseres.

Alarmer bør vises på en konsistent måte i alle prosessbilder ved bruk av symboler og ikoner plassert nær komponentene eller funksjonene som de er relatert til. Det bør være lett å se prioritet og status for hver alarm (aktiv, ikke aktiv, akseptert/uakseptert, blokkert, automatisk/manuelt undertrykt).

Aktive hovedalarmer (dvs. alarmer som ikke er automatisk eller manuelt undertrykt fra hovedalarmbildene) bør være lett å få øye på og klart fremtre som den viktigste informasjonen i bildet. Aktive alarmer som er undertrykt bør være mindre fremtredende enn hovedalarmene, og for hver alarm bør det indikeres om alarmen er automatisk eller manuelt undertrykt.

Prosessbildene bør vise hvilke alarmer som er definert og gi lett tilgang til tilleggsinformasjon om hver alarm, slik som alarmgrense og nedstengings-nivå og aksjoner for trip-alarmer.

33) Selektive lister bør være tilgjengelig [1]

Operatørene skal selv kunne konfigurere selektive lister for å dekke spesielle behov.

Krav 20 beskriver hvilke seleksjons, grupperings, og sorteringskriterier som bør være tilgjengelig i systemet. Operatører bør ha full fleksibilitet i å sette opp egne kriterier, men systemet bør også ha mulighet for enkel tilgang til et antall predefinerte konfigurasjoner som brukes ofte.

Eksempler på bruk av selektive lister er :

- Liste over bare høyeste prioritet kan være til nytte i en alarmrassituasjon der det er vanskelig å få oversikt over de viktigste alarmene.
- Systemalarmer på dedikerte lister kan være til nytte for vedlikeholdspersonell.

34) Alarmprioritet skal kodes ved bruk av farger og eventuelt andre virkemidler

Dette skal sikre at det skilles visuelt mellom de ulike prioritetene på en slik måte at det er enkelt og hurtig å få øye på de mest viktige alarmene blant de mindre viktige.

Alarmfargene skal:

- Være eksklusivt forbeholdt alarmer.

- Gjenspeile alarmens viktighet
- Gjøre alarmer lett å få øye på blant mindre viktig informasjon i alarm- og prosesskontrollsystemene.
- Være konsistent i alle bilder der alarmer vises.

Redundant visuell koding av prioritet er nyttig for å tydeliggjøre ytterligere, spesielt for fageblinde brukere. Ulike symboler og ikoner, plassering av informasjon og blinkefrekvens er blant mulige virkemidler som kan kombineres med fargebruk.

35) Nye alarmer som kommer inn skal varsles akustisk

Akustisk varsling brukes til å melde til operatøren at en ny alarm er kommet inn og krever oppmerksomhet, og om viktigheten til den nye alarmen.

Alarmlyder bør velges i henhold til en gjenomtenkt og helhetlig bruk av lyd i kontrollrommet, og alarmlyder som forstyrrer arbeid og kommunikasjon i kontrollrommet bør unngås.

Det anbefales å bruke maks. 4 ulike alarmlyder, og det skal være lett å skille mellom de ulike lydene.

Alarmer som er automatisk eller manuelt undertrykt skal ikke varsles med lyd. For lavprioritets alarmer bør det vurderes å bruke one-shot lyder eller ingen lyd i det hele tatt. Tale-alarmmeldinger kan brukes for å varsle om ekstreme sikkerhetsrelaterte situasjoner.

En felles funksjon for å stoppe alarmlyder bør være tilgjengelig.

En "stille kontrollrom"-funksjon er blitt foreslått for manuell utkobling eller neddemping av alle alarmlyder i en begrenset tidsperiode under større driftsforstyrrelser. Tanken er å la operatørene få arbeide sammenhengende med en krevende oppgave som de allerede er fullt ut oppmerksomme på, uten å tvinges til å forholde seg til et i praksis ubrukelig alarmsystem. Denne tilnærmingen griper ikke fatt i de underliggende årsakene til at alarmsystemet er ubrukelig i slike situasjoner.

Det anbefales at systemet designes slik at det vil være til hjelp for operatørene i alle situasjoner, i stedet for å tillate funksjonalitet som i praksis vil kunne dekke over svakheter i systemet. Dersom dette likevel implementeres, er det viktig å ha strenge prosedyrer som hindrer misbruk, og det må sikres at sikkerhetskritiske alarmer alltid gir varsling.

36) Nye alarmer som kommer inn skal varsles visuelt

Visuell varsling brukes for å trekke operatørens oppmerksomhet mot den nye alarminformasjonen og for å skille de nye alarmene fra de som er blitt akseptert tidligere.

Bruken av blinking bør begrenses. F. eks. i alarmmeldinger bør kun et lite symbol blinke. Alarmtekster skal aldri blinke.

I stedet for blinking kan man vurdere bruk av andre effekter som er mindre visuelt forstyrrende (f.eks. 3D effekter for utheving av ny alarminformasjon).

37) Alarminformasjon skal være informativ og lett forståelig

Dette er nødvendig for å unngå misforståelser og minimalisere tiden det tar å forstå betydningen av hver alarmmelding.

Alarmmeldinger bør være konsistente og basert på standard og anerkjent terminologi og forkortelser som brukes blant operatørene.

Alarmmeldinger kan inneholde: Prioritet, alarmtilstand (ny, akseptert, klarert), visuelt varslingssymbol, alarm identifikator, type avvik, og beskrivende tekst.

Man kan evt. også inkludere: Dato, tid, oppdatert måleverdi, alarmgrense og måleenhet.

Alarmmeldinger skal ikke inneholde noe unødvendig informasjon. På den annen side må den inneholde tilstrekkelig informasjon for at betydningen av meldingen kan oppfattes med minimalt behov for tolkning og memorering. (F .eks. man må ikke stole på at tag navn og nummer skal være tilstrekkelig)

Hovedalarmbildet og alarmlogg funksjonen kan eventuelt ha forskjellig innhold i alarmmeldingene, spesielt tilpasset bruken av hver funksjon. Dette bør gjøres på en gjennomtenkt måte for å unngå forvirring. Et eksempel kan være å kun vise dato og klokkeslett i alarmloggen.

38) Alarminformasjon skal være lett å lese

Dette skal sikre at innholdet i hver alarmmelding presenteres på en måte som er klar, godt strukturert og enkel og rask å lese.

Disse faktorene bør tas i betraktning i forbindelse med lesbarhet:

- Layout og gruppering av informasjon
- Rekkefølgen de ulike informasjonsenhetene presenteres i
- Fonttyper og størrelser bør velges for å gi god lesbarhet fra den tilsiktede leseavstand
- Bruken av farger i alarmmeldingen bør være slik at den ikke skaper vanskeligheter med å lese teksten
- Tekst som skal leses skal aldri blinke

39) Nødvendig alarminformasjon skal være tilgjengelig fra alle relevante arbeidsplasser

Dette skal sikre at alt relevant personell til enhver tid har et korrekt bilde av prosesstilstanden innenfor sitt ansvarsområde, og å sikre at alarmer vises i nærheten av de manøverinnretninger og visningsmedier som brukes til korrigerende tiltak eller diagnostisering.

Ulike typer personell kan ha behov for forskjellige typer informasjon:

- Kontrollromsoperatører
- Teknikere
- Ekstra personell behøves under en driftsforstyrrelse
- Prosessingeniører
- Testpersonell
- Personell fra beredskapslag

2.7 Alarmhåndtering

40) Nye alarmer som kommer inn skal kreve akseptering. [1,3]

Det bør kreves at operatørene aksepterer hver alarm for å bekrefte at alarmmeldingen er lest og forstått.

En alternativ praksis er at operatørene aksepterer en alarm først etter at den tilhørende respons har blitt utført. Operasjons- og alarmfilosofiene bør beskrive om det skal praktiseres akseptering etter at alarmmeldingen er lest, eller etter at respons er blitt utført.

Undertrykte alarmer (automatisk eller manuelt) skal imidlertid ikke kreve akseptering.

Det bør være mulig å akseptere alarmer fra alarmlister og detaljerte bilder på alle arbeidsstasjoner. Oppdatering av alarmstatus skal sendes til alle displayer når en alarm er blitt akseptert.

Separat akseptering for hver alarm skal være mulig, og en sentral akseptering av alle synlige alarmer i en liste kan også være tilgjengelig.

Alarmlyd bør forsvinne når alle alarmer er akseptert. I tillegg bør det være tilgjengelig en egen knapp for å stoppe alarmlyder uten å måtte akseptere.

Aksepteringsstatusen til en alarm kan være nyttig som en betingelse for styring av automatisk fjerning av alarmer fra listen

- For enkelte alarmer bør det kreves at operatøren har akseptert alarmen før den kan fjernes automatisk fra listen. Dette kan være aktuelt for høyprioritets alarmer, og alarmer som har utløst aksjoner i prosessen. I slike tilfeller kan operatørrespons være påkrevet selv om alarmsignalet har returnert til normal tilstand.
- Automatisk fjerning av enkelte typer uaksepterte alarmer kan brukes for reduksjon av alarmbelastningen. Lavprioritets alarmer vil typisk varsle om forhold som når de returnerer til normal ikke lenger krever oppmerksomhet eller respons fra operatøren.

To forskjellig prinsipper bør vurderes for hvordan listen skal oppføre seg idet en alarm fjernes:

- Håndteringen av listen forenkles ved å komprimere listen automatisk hver gang en alarm fjernes. Ulempen med dette er at det blir vanskelig å holde øye med en bestemt alarm i listen for å få bekreftelse på en vellykket korrigerende handling.
- Manuell komprimering av listen gjør det lettere å se når alarmer går av, siden operatøren ikke forstyrres av uventede endringer i listen. Ulempene med dette prinsippet er at det introduserer en ekstra operatøraksjon i alarmhåndteringen og at det er mulighet for at listen fylles opp med gamle/blanke alarmer dersom den ikke komprimeres tilstrekkelig ofte.

41) Det bør være mulig å undertrykke individuelle alarmer manuelt [3]

Formålet med manuell undertrykking er å la operatørene fjerne stående og andre irrelevante alarmer som ikke den automatiske undertrykkingen har tatt hånd om.

Manuell undertrykking av en alarm innebærer å fjerne den fra hovedalarmlisten og legge den over i en spesiell liste over manuelt undertrykte alarmer. Alarmen hindres med dette i å komme inn på hovedalarmlisten igjen før alarmen er fjernet fra denne undertrykkingslisten. Manuell undertrykking er operatørstyrt og skal fungere som en

siste utvei for håndtering av irrelevante alarmer som ikke er blitt stoppet av signalfilteringen eller undertrykkingsmekanismene.

Operatøren skal lett kunne få oversikt over hvilke alarmer som er manuelt undertrykt i en dedikert liste som viser disse, og i tillegg gjennom symbolbruken der alarmen vises i prosessbildene.

Det bør kreves at operatøren dokumenterer i et administrativt system hva som er grunnen til at alarmen undertrykkes manuelt.

Manuell undertrykking kan være tidsbegrenset for å forhindre at viktige alarmer fjernes fra hovedlisten og glemmes. Et administrativt system bør holde styring med manuell undertrykking gjennom bruk av tilgangskontroll for å hindre at viktige alarmer, slik som nøkkelalarmer, for lett kan undertrykkes manuelt av operatørene.

42) Det bør være hurtig og enkelt å navigere i alarmbilder [2]

Dette er viktig for å gjøre det mulig for operatører håndtere alarmer på en effektiv måte gjennom hurtig navigasjon til nødvendig tileggsinformasjon.

Det skal være mulig å navigere fra alarmlisten til prosessbildet som viser alarmen. Dette skal kreve et minimum antall operatørinteraksjoner.

Det bør være mulig å klikke på en alarm i ethvert bilde for å få mer informasjon om alarmen, som f.eks. responsprosedyrer.

Operatørene skal kunne velge mellom ulike modi i listene:

- Operatørstyrt modus, der operatøren fritt kan bla og scrolle til enhver del av listen uten å forstyrres av nye alarmer.
- Automatisk modus, der siste innkomne alarm alltid er synlig på toppen eller bunnen av listen.

Det skal være mulig å navigere i alarmlister ved bruk av scrollbar og side-opp/side-ned knapper, og det bør finnes en fleksibel funksjon for tekstsøking.

43) Det skal eksistere prosedyrer som spesifiserer individuelt ansvar for overvåkning og styring ved store driftsforstyrrelser og nødssituasjoner, og operatørene skal være kjent med disse

Slike prosedyrer skal sikre at arbeidet i kontrollrommet i kritiske situasjoner er effektivt og godt organisert.

For nødssituasjoner skal det beskrives hvordan arbeidet i kontrollrommet bør organiseres. Dette omfatter ansvar for overvåkning og styring av prosessystemene, sikkerhetssystemene, marine systemer og kommunikasjonssystemer, og også hvordan de ulike oppgavene skal prioriteres.

Opplæring og systematisk trening er nødvendig for at slike prosedyrer skal fungere.

3 REFERANSER

1. *Alarm-kravspesifikasjon for Amoco Norway Oil Company*, Valhall CCR Upgrade Project, IFE/HR/F-99/1118.
2. *Requirement Specification for the HAMBO Alarm System*, IFE/HR/F-2000/1141
3. *Alarm Systems: A Guide To Design, Management and Procurement*, The Engineering Equipment and Materials Users Association (EEMUA) publication No. 191
4. NORSOK Standard I-002