

## Overordnet alarmfilosofi for Jernbaneverket

00A	Første utgave	10.12.2015	Engsol		
Revisjon	Revisjonen gjelder	Dato:	Utarb. av	Kontr. av	Godkj. av
Tittel:		Målestokk:			
<b>Alarmfilosofi for Jernbaneverket</b>		Utarbeidet av:			
		<b>Solbjørg Engeset</b>			
Prosjekt: Smart vedlikehold		Erstatning for:		Antall sider	
Parsell: Ikke relevant				39	
Site ID:		FDV nummer:			
Delsys.: <b>NA</b>					
		Dokumentnummer:		Revisjon	
		<b>IUP-00-A-00961</b>		<b>00A</b>	

# Innholdsfortegnelse

<b>1. BAKGRUNN</b>	<b>5</b>
<b>2. INNLEDNING</b>	<b>5</b>
<b>3. DOKUMENTSTRUKTUR OG KNYTNING MOT STANDARD</b>	<b>6</b>
<b>4. DEFINISJONER OG FORKORTELSER</b>	<b>7</b>
<b>4.1 DEFINISJONER</b>	<b>7</b>
<b>4.2 FORKORTELSER</b>	<b>10</b>
<b>5. ALARMSYSTEMET</b>	<b>11</b>
<b>5.1 HENSIKT MED ALARMSYSTEMET</b>	<b>11</b>
<b>5.2 ROLLER OG ANSVAR FOR ALARMSYSTEMET</b>	<b>12</b>
<b>6. IDENTIFIKASJON OG UTVELGELSE AV ALARMER</b>	<b>13</b>
<b>6.1 GENERELT</b>	<b>13</b>
<b>6.2 PRINSIPPER</b>	<b>14</b>
<b>6.3 DELTAKELSE</b>	<b>14</b>
<b>6.4 ALARMER OG MELDINGER TIL TRAFIKKSTYRINGSSYSTEMENE</b>	<b>14</b>
<b>6.5 ALARMER RELATERT TIL FEIL PÅ TOGMATERIELL</b>	<b>15</b>
<b>6.6 KONTROLLSPØRSMÅL OG KRAV TIL DOKUMENTASJON VED UTVELGELSE</b>	<b>15</b>
<b>7. KLASSIFISERING AV ALARMER</b>	<b>18</b>
<b>7.1 KLASSE 1 – SIKKERHETSALARMER</b>	<b>18</b>

<b>7.2 KLASSE 2 - ALARMER FRA JERNBANEINFRASTRUKTUR</b>	<b>19</b>
<b>8. PRIORITERING AV ALARMER (KRITIKALITET)</b>	<b>19</b>
<b>8.1 FØRINGER FOR OVERGANGSFASE</b>	<b>19</b>
<b>8.2 PRIORITETSNIVÅER/KRITIKALITETSNIVÅER</b>	<b>20</b>
<b>9. DESIGNPRINSIPPER FOR ALARMSYSTEMET</b>	<b>21</b>
<b>9.1 TILLATTE TILSTANDER</b>	<b>21</b>
<b>9.2 FASTSETTING AV ALARMTERSKELE (SET POINT)</b>	<b>23</b>
<b>9.3 FUNKSJONALITET OG BRUKERGRENSESNIITT HMI</b>	<b>23</b>
<b>9.3.1 FØRINGER FOR ALARM DESIGN</b>	<b>23</b>
<b>9.3.2 KVITTERING AV ALARM</b>	<b>23</b>
<b>9.3.3 UNDERTRYKKING AV ALARM</b>	<b>23</b>
<b>9.3.4 PRESENTASJON AV ALARMER (HMI DESIGN PRINSIPPER)</b>	<b>23</b>
<b>9.3.5 ALARMHISTORIKK</b>	<b>24</b>
<b>10. OPPLÆRING, INSTRUKSER OG DOKUMENTASJON</b>	<b>24</b>
<b>10.1 OPPLÆRING</b>	<b>24</b>
<b>10.2 INSTRUKSER</b>	<b>25</b>
<b>10.3 DOKUMENTASJON</b>	<b>25</b>
<b>11. IMPLEMENTERING OG IDRIFTSETTING</b>	<b>26</b>
<b>12. DRIFT OG VEDLIKEHOLD AV ALARMSYSTEMET</b>	<b>27</b>
<b>12.1 VEDLIKEHOLD</b>	<b>27</b>

<b>12.2 ENDRINGSHÅNDTERING</b>	<b>27</b>
<b>13. OVERVÅKING OG OPTIMALISERING AV ALARMSYSTEMET</b>	<b>28</b>
<b>13.1 MÅLING AV KVALITET OG EFFEKTIVITET FOR ALARMSYSTEMET</b>	<b>28</b>
<b>13.2 REVISJON AV ALARMSYSTEMET</b>	<b>29</b>
<b>14. REFERANSER</b>	<b>29</b>
<b>15. VEDLEGG</b>	<b>31</b>
<b>VEDLEGG 1- KPIER FOR FJEL OG TEMIP</b>	<b>32</b>
<b>VEDLEGG 2 SAMSVARSTABELL MELLOM KRAV TIL INNHOLD I ALARMFILOSOFI SOM DEFINERT I [2] OG ALARMFILOSOFI FOR JBV.</b>	<b>38</b>

## 1. Bakgrunn

Jernbaneverket har en strategi for mer tilstandsbasert overvåking. Bredden av fagområder som skal overvåkes blir derfor større. I tillegg har nye typer utstyr flere muligheter for å varsle om feil og avvik. Behovet for å behandle alarmer er økende og dette stiller nye krav til operatører og overordnede alarmsystemer.

Det er derfor behov for å etablere en felles definisjon av alarm og en helhetlig tilnærming til alarmer i Jernbaneverket.

Alarmfilosofien skal gi overordna føringer og prinsipper for alarmhåndtering i Jernbaneverket fra hvordan alarmen identifiseres og til den presenteres for og behandles av operatør. Filosofien gir dessuten føringer for overvåking og revisjon av alarmsystemet.

Jernbaneverket har i dag kontinuerlig overvåking av alarmer 24/7 i hovedsak via Fjel og TeMip, men også trafikkstyringssentralene overvåker relevante alarmer via trafikkstyringssystemene (CTC/TMS). (Av historiske årsaker inneholder eksisterende CTC/TMS systemer også feilmeldinger som er mer relevant for vedlikehold enn for trafikkstyring).

## 2. Innledning

NEK EN 62682:2015 «Management of alarm systems for the process industries» [2] samt EEMUA 191 «Alarm systems» [5] er lagt til grunn for arbeidet med alarmfilosofi i Jernbaneverket.

Alarmfilosofien skal være et levende dokument, og praktiske erfaringer bør benyttes for å forbedre filosofien basert på Jernbaneverkets egne erfaringer og behov.

[Standarden \[2\] deler livssyklusen for alarmhåndtering inn i et antall trinn, der alarmfilosofien skal gi overordna føringer for alle trinn. Figur 1 Livssyklus for alarmhåndtering](#)

viser livssyklusen for alarmer.

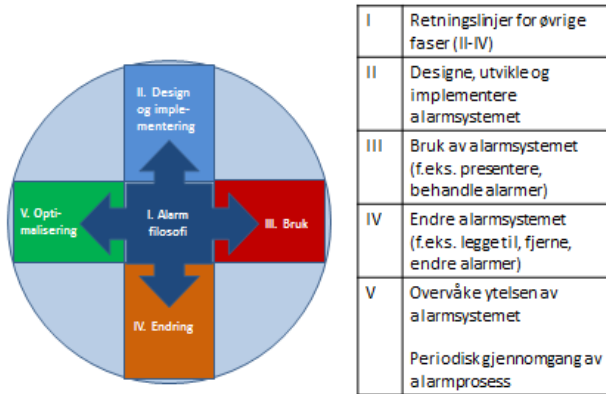
Alarm benyttes i dette dokumentet om et signal som varsler (visuelt og/eller akustisk) om funksjonsfeil i utstyr, prosessavvik eller andre avvik som krever en reaksjon. Dette er uavhengig av hva som er årsaken til avviket.

En alarm kan for eksempel oppstå når vi har endringer i en tilstand som indikerer mulig fremtidig svikt, eller fordi det er oppstått en feil. En alarm kan også oppstå som følge av at deteksjonssystemer aktiveres i situasjoner hvor rettidig reaksjon skal kunne forhindre topphendelse eller eskalering av risiko for topphendelse. Alarmen skal med andre ord varsle om at det er behov for tiltak, enten dette er for å forebygge feil, rette feil eller forebygge topphendelser. Alarmen skal sendes til den som har ansvar/mandat til å gjøre noe med hendelsen alarmen varsles om.

Alarmsystemene inngår som støtte for vedlikeholdsprosessen og skal bidra til at oppetidskrav og punktlighetskravene for Jernbaneverket oppnås og forbedres.

Dette krever at alarmsystemene gir effektiv støtte for operatører og driftspersonell slik at disse kan reagere raskt og riktig på alarmen.

Alarmer kan, hvis de ikke blir håndtert riktig, bidra til handlingslammelse og kaos. For eksempel hvis operatøren mottar altfor mange alarmer samtidig eller hvis det ikke er klart hvordan operatøren skal reagere på alarmene.



**Figur 1 Livssyklus for alarmhåndtering**

Operatørene av et alarmsystem kan ha ulike funksjoner avhengig av organisering, mulighet for fjerntilgang (for feilanalyse og tilbake stille tilstand) samt kompetanse. Dvs. noen operatører kan kun ha ansvar for å overvåke og registrere alarm samt kalle ut riktig personell til riktig tid, mens andre operatør i tillegg har ansvar for å kontrollere, styre og utføre nødvendige tiltak. Operatørene kan dessuten sitte sentralt eller desentralt. Organisering og ansvar for operatører anses å være strategiske valg og alarmfilosofien tar ikke stilling til dette.

Ettersom JBV allerede har eksisterende alarmsystemer, vil første utgave av filosofien være begrenset med tanke på hvilke områder som er konkretisert. Det vil likevel kreve en del arbeid for å tilpasse eksisterende systemer til føringer i filosofien.

I forkant av nyanskaffelser av overordna alarmsystemer, eventuelt omfattende endringer av eksisterende alarmsystemene, skal alarmfilosofien revideres og benyttes som føringer for kravspesifikasjon.

Alarmfilosofien eies av Infrastrukturdirektør som peker ut ansvarlig for å forvalte den. Trafikk og Markedsdivisjonen skal involveres ved revisjoner av dokumentet.

### **3. Dokumentstruktur og knytning mot standard**

Innholdsmessig baserer dokumentet seg på [2]. Oppbyggingen avviker imidlertid noe fra standarden. For å gjøre det enklere å knytte kapitlene i dokumentet opp mot anbefalingene i standarden, er det laget en oversikt som viser samsvar mellom kapitlene i alarmfilosofien og standarden. Denne finnes i Vedlegg 1.

Filosofien angir prinsipper på følgende måte: «*√ prinsipptekst*». Prinsippene har ofte tilknyttet seg en forklarende tekst, samt mer konkrete føringer.

## 4. Definisjoner og forkortelser

### 4.1 Definisjoner

Begrep	Engelsk	Definisjon
Alarm	Alarm	Varsel (akustisk og/eller visuelt) om funksjonsfeil i utstyr, prosessavvik eller andre avvik som krever rettidig reaksjon .  Note: for å håndtere hendelsen som forårsaket alarmen.
Alarmundertrykking	Alarm suppression	Automatisk prosessering som hindrer et irrelevant alarmsignal i å presenteres i hovedbilder for operatøren, men hvor tilstanden til alarmen fortsatt er tilgjengelig i mer detaljerte bilder.
Alarmfiltrering	Alarm filtering	Automatisk prosessering som gjør et alarmsignal utilgjengelig i hele alarmsystemet.
Basisalarmer	Basic alarms	Genereres ved å detektere avvik på enkeltmålinger fra prosessen eller enkelte utstyrskomponenter.
Feil	Fault	En tilstand som er karakterisert ved at enheten ikke er i stand til å utføre en krevd funksjon. Hvis dette er som følge av forebyggende vedlikehold, andre planlagte aksjoner eller mangel på eksterne ressurser betraktes tilstanden ikke som en feil. Kommentar: En feil (tilstand) er ofte et resultat av en svikt på enheten, men kan også inntreffe/eksistere uten en tidligere svikt. Eksempel: Vekselmotoren er i en tilstand hvor den ikke kan gi kraft til å legge om. Den har allerede sviktet.
Feilmode	Fault mode	En av flere mulige feiltilstander til en enhet. Feiltilstanden fører til at en gitt krevd funksjon ikke tilfredsstilles.  Eksempel: En vekselmotors feilmode kan være at den ikke gir kraft.

Hendelseslogg	Event Log	Manuell eller automatisk registrering av hendelser under utøvelsen av en funksjon, ett program eller et system. Hensikten er å dokumentere revisjonsspor som kan benyttes for å forstå sekvensen av aktiviteter og diagnostisere problemer.
Instruks	Instruction	Beskriver hvordan en bestemt aktivitet eller oppgave skal utføres av sikkerhets- eller leveransmessige grunner. Formes og baseres på brukernes kompetanse [16].
Indikering	Indications	Informasjon om en tilstand, flere indikeringer kan rapporteres for samme tilstand.
Jernbaneinfrastruktur	Rail Network	Består av delsystemet infrastruktur, de faste innretninger av delsystemet energi, samt de faste innretninger av delsystemet styring, kontroll og signalering, ref.[8].  Note: Her benyttes infrastruktur slik det er definert i Jernbaneinfrastrukturforskriften [8] dvs. Spor, sporveksler, byggverk (broer, tunneler osv.), infrastruktur knyttet til jernbanestasjoner (plattformer, ganganlegg, herunder anlegg som er tilpasset bevegelsehemmedes behov osv.), sikkerhets- og verneutstyr.
Korrelering av alarmer	Alarm Correlation	Tolkning av flere alarmer sett i sammenheng som medfører en ny forståelse av alarmene.
Krevd funksjon	Required function	En enhets funksjon eller kombinasjon av funksjoner som betraktes som nødvendig for å sikre en gitt ytelse. Eksempel: En vekselmotors funksjon er å gi kraft til å legge om vekselen.
Kvittert alarm	Acknowledged alarm	Kvittert alarm er alarm som er under behandling og registrert i støttesystem.
Manuell undertrykking av alarm	Shelved alarm	Midlertidig undertrykking av alarm initiert av operatør.



Modellbaserte alarmer	Model based alarms	Alarmer generert på basis av online simuleringer av matematiske modeller av definerte prosesselementer.
Operatør	Operator	Person som overvåker tjenester og agerer på alarmer i henhold til definert aksjon.
P-F intervall	Possible fault to fault interval	Estimert tid fra avvik som forventes å resultere i en feilsituasjon kan detekteres til feil inntreffer.
Prosedyre	Process	Prosedyre/prosessbeskrivelse med aktiviteter, oppgaver og roller (f.eks. Hvem gjør hva og i hvilken rekkefølge) [16].
Rotårsaksanalyse	Root Cause Analysis	Metodikk for å kartlegge grunnleggende og systematiske årsaker til feil.
Sammensatte alarmer	Aggregated alarms	Genereres ved å kombinere tilstanden til et antall basisalarmer på en slik måte at tilstanden kan beskrives mer presist enn hva de enkelte basisalarmene kan gjøre.  Begrepet korrelerte alarmer, benyttes også.
Sikkerhetsfunksjon	Safety Function	En funksjon kun har som oppgave å ivareta safety (unngå tophendelse). (EN50126).  Merk1 en sikkerhetsfunksjon er alltid en sikkerhetsrelatert funksjon, men ikke motsatt.  Merk 2 En sikkerhetsfunksjon kan bidra til en eller flere sikkerhetsbarrierer. En sikkerhetsbarriere er imidlertid ikke alltid implementert av en sikkerhetsfunksjon.
Sikkerhetsrelatert funksjon	Safety-related function	En sikkerhetskritisk funksjon er en funksjon som hvis den feiler gir økning i sikkerhetsrisiko  Merk (EN 50126) en funksjon, komponent eller instruks er kalt

		sikkerhets (safety) relatert hvis minst en av egenskapene er benyttet i sikkerhetsargumentasjonen for systemet den benyttes for.
Stående alarm	Stale alarm	Alarm som blir stående over en lang periode f.eks. 24 timer.
Svikt	Failure	Opphør av en enhets evne til å utføre en krevd funksjon. Kommentar: Etter en svikt har enheten en feil (tilstand). Svikt er en hendelse, og er forskjellig fra "feil" som er en tilstand. Eksempel: I tidspunktet når vekselmotoren ikke kan gi kraft for å legge om vekselen, svikter den.
Tilstand	Condition	Et forhold (situasjon eller handling) som kan utvikle seg til tilløp til svikt, (forholdet ble avdekket før noe skjedde), eller svikt.
Ukvittert alarm	Un-acknowledged alarm	Alarm som er presentert for operatør, men ikke under behandling og registrert i støttesystem.

#### 4.2 Forkortelser

CTC –	Centralized Traffic Control
FMECA-	Failure Modes, Effects, and Criticality Analysis
GUI-	Graphical User Interface – brukergrensesnitt (vanlig brukt i IT systemer)
HMI -	Human Machine Interface – brukergrensesnitt (omfatter GUI, brytere etc.)
KV IKT -	Kjøreveis IKT
KPI -	Key Performance Indicator
MLD -	Mean Logistic Delay
MRT -	Mean Repair Time
MTBF -	Mean Time Between Failure
MTTR-	Mean Time To Repair
RCM-	Reliability Centered Maintenance (Pålitelighetsstyrt Vedlikehold)

TMS- Traffic Management System

## 5. Alarmsystemet

Alarmsystemet skal inneholde funksjoner knyttet til alarmbehandling, lagring og presentasjon, se Figur 2.

Alarmfilosofien gjelder alarmsystemet (se Figur 2).

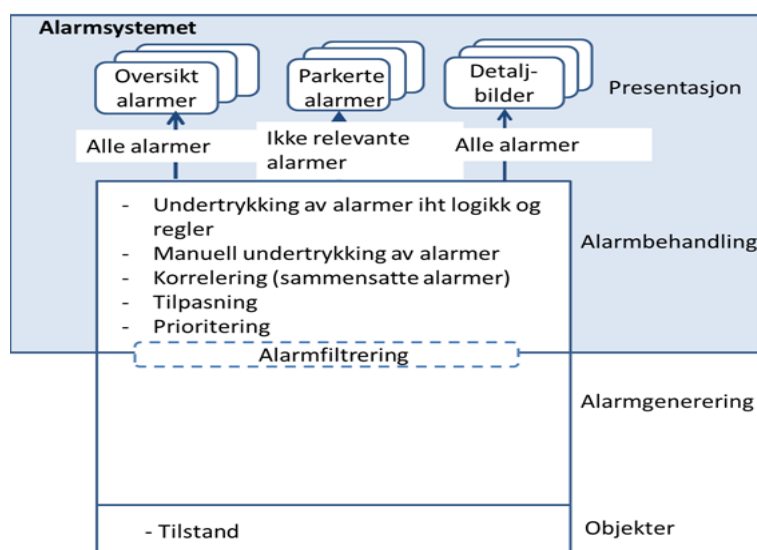
Jernbaneverket (JBV) har – og kommer til å ha – et antall ulike systemer som genererer alarmer for ett eller flere objekter. Slike systemer leveres ofte med objektet. Ettersom disse systemene skal levere alarmer inn til ett (evt. flere) overordna systemer, vil alarmfilosofien implisitt gi føringer også for disse systemene. Det er viktig at samspillet mellom alarmsystem og system som genererer alarmer fungerer slik at føringene i alarmfilosofien oppfylles.

### 5.1 Hensikt med alarmsystemet

Hensikten med alarmsystemet er å fungere som støtte for effektivt å identifisere og håndtere unormale hendelser, og ved behov prioritere de rette tiltakene i henhold til kritikalitet.

Alarmsystemet skal ha tre hovedfunksjoner:

1. Varsle operatøren om en hendelse som krever reaksjon og gi informasjon om hva som har skjedd, hvor det har oppstått, kritikalitet og helst også hva som må gjøres for å tilbake stille til normal tilstand.
2. Lagre alarmer og hendelseslogger i tilknytning til alarm slik at en i etterkant kan gjennomføre feil- og trendanalyse og for å gjøre tiltak slik at alarmen ikke oppstår i fremtiden.
3. Å vise forventet følge av en gitt alarm. For eksempel hvilket utstyr evt. utstyr på andre geografiske steder kan forventes å miste funksjonalitet som følge av feilen. (Dette vil være til hjelp for operatør når han samtidig får telefonisk forespørsel om svikt som kan skyldes primæralarmen.)



Figur 2 Alarmsystemet

Alarmer kan benyttes i sammenheng med tilstandsdata for diagnose og prognose enten dette gjøres automatisert eller manuelt.

Hendelsesloggen skal inneholde hendelser, alarmer som er samlet inn, men ikke presentert for operatør, operasjoner på alarmer samt tilleggsinformasjon som kan være relevant for analysefunksjonen generelt. Loggen skal være tilgjengelig for innsyn av relevante personer – inkludert operatør.

Komplett hendelseslogg (eller en så nær komplett logg som mulig) lagres som historikk for diagnose og prognose, mens deler av hendelseslogg kan gjøres tilgjengelig for spesifikk rapportering.

## 5.2 Roller og ansvar for alarmsystemet

- ✓ *Ansvar for å ivareta rollene som skal ivareta de ulike føringene i alarmfilosofien skal være klart i organisasjonen.*

Alarmsystemene er ikke statiske. Nye alarmer tilføres over tid og operatørene vil i samarbeid med systemansvarlige og vedlikeholdspersonell opparbeide seg bedre kompetanse på alarmer og feilsituasjoner over tid. Som en del av prosessen med å sikre at alarmsystemene fungerer etter hensikten, må nye alarmer tilføres basert på definerte kriterier, ytelsen av systemet overvåkes og tiltak iverksettes ved behov. I Tabell 1 Roller og ansvar, fremgår hvilke roller som har ansvar og oppgaver i forbindelse med å implementere og etterleve alarmfilosofien.

Med rollen systemansvarlig, mener vi den i organisasjonen som har forvaltningsansvar for systemet det gjelder.

Organisering av roller kan variere. Det er imidlertid viktig at ansvar og oppgaver i rollene ivaretas uavhengig av organisering.

<b>Roller</b>	<b>Ansvar og oppgaver (kun relatert til alarmfilosofi)</b>
Systemansvarlig for alarmsystemet	<ul style="list-style-type: none"> <li>- ansvar for at det bygges inn og vedlikeholdes kunnskap og intelligens i alarmsystemet gjennom hele livssyklusen</li> <li>- sørge for at det gjennomføres tilstrekkelig overvåking av ytelsen av alarmsystemet både med tanke på oppetid og alarmovervåking og i henhold til føringene i alarmfilosofi til alarmsystemet</li> <li>- sørge for å fremme tiltak for forbedringer og at besluttede tiltak iverksettes</li> <li>- sørge for at systemet er godt dokumentert og at det er etablert klare roller og ansvarsforhold for vedlikehold og forbedringer</li> </ul>
Systemansvarlig for fagsystem	<ul style="list-style-type: none"> <li>- definere og velge ut alarmer for sine fagsystemer</li> </ul>

(alternativt navn: Objekteier f.eks. Elkraft, Signalanleggstype)	<ul style="list-style-type: none"> <li>- bistå med å optimalisere alarmsystemet</li> <li>- bistå med etablering av instruksjoner for alarmer</li> <li>-</li> </ul>
Prosjekteier/tiltakseier (eier av prosjekt eller tiltak som introduserer nytt utstyr som krever alarmovervåking evt. endringer i nytt utstyr som krever alarmovervåking)	<ul style="list-style-type: none"> <li>- initiere og gjennomføre prosess for identifikasjon og utvelgelse av alarm</li> <li>- ivareta nødvendige tiltak for opplæring og dokumentasjon knyttet til alarm</li> </ul>
Problemløser (Problem Manager)	<ul style="list-style-type: none"> <li>- sørge for at det gjennomføres rotårsaksanalyse</li> <li>- sørge for at tilstander som forårsaker alarmer utbedres</li> <li>- bistå med å optimalisere alarmsystemet</li> </ul>
Infrastrukturdirektør	<ul style="list-style-type: none"> <li>- eie og godkjenne alarmfilosofien samt sørge for at denne vedlikeholdes</li> <li>- fastsette mål og krav til kvalitet på vedlikeholdsprosess og overvåkingsfunksjon</li> </ul>

**Tabell 1 Roller og ansvar**

## 6. Identifikasjon og utvelgelse av alarmer

### 6.1 Generelt

Alarmer bør:

- Presenteres i et omfang og visuelt slik at det er håndterbart for operatøren.
- Inneholde tilstrekkelig informasjon til at operatøren kan forstå alarmen og reagere på riktig måte.

Hensikten med identifikasjons- og utvelgelsesfasen er å verifisere at alarmen er nødvendig og sikre at operatøren har tilstrekkelig informasjon til å kunne reagere riktig på alarmen. Utvelgelse av alarm skal gjennomføres i forkant av at alarmen tas inn i alarmsystemet, men prosessen kan også benyttes ved revurdering av alarmer som allerede er i systemet.

Nytt utstyr (enten nye instanser av eksisterende utstyr eller nye typer utstyr) vil ofte leveres med et antall mulige alarmer. I tillegg vil prosjekter gjennom RAMS-analyser kunne identifisere behov for spesifikke alarmer.

Disse alarmene skal gjennom utvelgelsesprosessen som definert i 6.4 **Feil! Fant ikke referanse-kilden.**, før de implementeres i alarmsystemet. Alarmer som ikke implementeres i alarmsystemet, kan fortsatt ha verdi som støtte for feilanalyse.

Det er prosjekteier/oppdragseier som har ansvar for å gjennomføre denne prosessen og å involvere

de riktige rollene i arbeidet. Prosjekteier/oppdragseier må i forkant ha klargjort hvem som skal ha systemansvar for utstyret og hvem som skal ta ansvar for feilretting.

Unntak er ved «revidert» utvelgelse av alarmer, der hensikten er å gjøre en gjennomgang av eksisterende alarmer for å vurdere om de fortsatt skal presenteres til operatør for reaksjon. Det er i dette tilfelle systemansvarlig for alarmsystemet som har ansvar for å gjennomføre prosessen.

## 6.2 Prinsipper

Viktige prinsipper som skal legges til grunn i identifikasjons- og utvelgelsesprosessen er:

- *Alarmer skal kreve rettidig reaksjon fra operatør for å sikre at normaltilstand tilbakestilles.*
- *Det skal finnes en systemansvarlig (objektansvarlig) samt en ansvarlig funksjon for å utøve vedlikehold og forvaltning for utstyr som skal overvåkes.*
- *Duplisering av alarmer skal unngås.*
- *Det skal være entydig hvilke oppgaver en operatør har i tilknytning til en alarm.*
- *En alarm skal i prinsippet kun sendes til en funksjon for reaksjon. Dersom den av en eller annen grunn rutes til mer enn en funksjon eller der det for samme tilstand både genereres indikering evt. melding og alarm, skal ansvar og oppgaver for mottakerne av alarmene være entydig definert.*
- *Ingen alarmer skal med hensikt designes slik at de ender opp som stående alarmer.*

## 6.3 Deltakelse

Utvelgelse av alarmer skal som hovedregel gjennomføres med deltakelse fra følgende roller:

- Systemansvarlig for utstyr som genererer alarmer (objekteier bør ha kunnskap bl.a. om regelverk for systemet).
- Systemansvarlig for alarmsystemet.
- Prosjekt/tiltaksansvarlig (når prosjekter har anskaffet nytt utstyr som skal overvåkes).
- Vedlikeholdspersonell.
- Operatør.

Representant for funksjonell godkjenning i Trafikk- og markedsdivisjonen skal involveres for alarmer og meldinger som har betydning for eller kan ha betydning for togfremføringen.

Leverandør av utstyr involveres ved behov. Det er viktig at noen med prosesskompetanse deltar i møtet.

## 6.4 Alarmer og meldinger til Trafikkstyringssystemene

Jernbaneverket har egne trafikkstyringssentraler for togfremføring.

Det vil utarbeides en egen detaljert alarmfilosofi for presentasjon av alarmer og meldinger for nytt Trafikkstyringssystem (TMS-prosjektet, nytt trafikkstyringssystem for det nasjonale jernbanenettet). Filosofiene skal harmoniseres i det videre arbeidet.

Trafikkstyringssystemene skal motta alle meldinger/alarmer som har betydning for togfremføring, sikkerhet og beredskap. Disse meldingene/alarmene skal vises/indikeres i CTC/TMS/betjeningsanlegg via særskilt direkte grensesnitt mot aktuelt system/objekt [11].

Trafikkstyring skal ha alarmer:

- Hvis det finnes en trafikal regel for håndtering av alarm f.eks. godstog skal stoppe ved neste stasjon ved detektert hjulslag.
- Ved situasjoner som kan forårsake tophendelser.

Trafikkstyring skal motta informasjon (meldinger/indikeringer):

- Om status (inklusive feilstatus) dersom status påvirker hvordan togleder styrer trafikken.
- Om status på operasjon utført av togleder.
- Om status på automatiserte operasjoner (her er det i hovedsak snakk om interne meldinger).

**Merk.** I en overgangsfase hvor det er implementert egne instanser for overvåking av alarm for alle objekter og hvor man er avhengig av feilmelding fra trafikkstyring for å melde feil og kalle ut personell, vil det være nødvendig at trafikkstyringssystemene mottar alarmer/meldinger også om andre feiltilstander enn de som er nevnt over. Dette gjelder primært for hendelsene som har, eller kan få konsekvenser for togfremføring, sikkerhet og beredskap.

## 6.5 Alarmer relatert til feil på togmateriell

Dette er f.eks. alarmer om hjulslag. Jernbaneforetakene har ansvar for tilstand på sitt rullende materiell. Jernbaneverket har imidlertid egne overvåkingssystemer bl.a. hjulskadedeteksjonssystemer som identifiserer og varsler om feil på rullende materiell. Jernbaneforetakene skal motta varsling og tilstandsinformasjon knyttet til deres materiell.

Både alarm og tilstandsdata bør lagres i Jernbaneverkets systemer for saksbehandling med Jernbaneforetakene ved skader på infrastruktur.

Det er trafikkstyring som skal reagere på alarm dersom tog skal stanses.

## 6.6 Kontrollspørsmål og krav til dokumentasjon ved utvelgelse

Følgende kontrollspørsmål skal benyttes ved utvelgelse av alarm (ref. Tabell 2).

Karakteristikk	Kontrollspørsmål	Kommentar
----------------	------------------	-----------

Relevans	Kan operatøren gjøre noe med denne alarmen?	
Relevans	Hva er konsekvensen ved ikke å reagere på alarmen?	<p>Kun direkte konsekvens skal vurderes</p> <p>Dersom konsekvensen ved ikke å reagere på alarmen er neglisjerbar, skal alarmen ikke overvåkes</p>
Relevans	Retter alarmen oppmerksomheten til operatøren mot de riktige hendelsene?	<p>Dersom det genereres mange falske alarmer, kan dette kreve oppmerksomhet fra operatør på ikke-relevante hendelser.</p> <p>Nødvendighet av kontinuerlig overvåking skal vurderes grundig og støtte skal eventuelt «bygges inn» i instruksene for kvalitetskontroll av alarm før den behandles videre.</p>
Relevans	Skal alarm eller melding til trafikkstyringssystem?	Hvis alarm skal både til operatør og trafikkstyring, må ansvar og oppgaver være entydig definert
Relevans	Ønskes alarmen implementert i alarmsystemet primært for trendanalyse, statistikk eller rapportering?	<p>Dersom underliggende system ikke gir tilstrekkelig støtte for feilanalyse og rapportering, kan det være behov for at dette gjøres i alarmsystemet.</p> <p>Plassering av alarm skal følge føringer i OSS arkitektur.</p> <p>Det må være tydelig om det er relevant at alarm presenteres i overvåkingsbilde eller ikke.</p>
Unik	<p>Finnes utstyret og alarmen allerede?</p> <p>Se 6.4 og 6.5</p>	<p>Gjenbruk.</p> <p>Dersom utstyret benyttes på en ny måte/i en annen prosess, bør en vurdere om det er behov for å endre eksisterende dokumentasjon og/eller instruksjer tilknyttet alarmen.</p>
Unik	Finnes det allerede en alarm som	Vurder hvilken alarm som gir best



	varsler om det samme evt. nesten det samme?	informasjon om tilstanden.  Vurder behov for å opprette en ny alarm som erstatter eksisterende.
Operatørstøtte	Gir alarmmelding operatøren god bistand til diagnostisering?	Hvis alarm ikke gir god støtte til operatør, bør en vurdere om den har verdi evt. om en kan berike alarmen, eller gi operatør støtte til diagnostisering på annen måte f.eks. tilleggsdokumentasjon
Operatørstøtte	Gir alarmen god indikasjon på viktighet?  Trenger alarmen spesiell oppmerksomhet?	Riktig bruk av prioritet og eventuelt behov for ekstra varsling
Presentasjon	Vil oppgaven til operatør alltid være å rute alarmen videre til andre for utbedring av feil og avvik?	Vurder om dette bør gjøres automatisert
Ansvar	Er systemansvaret for fagsystemet plassert?	Det er viktig at det er etablert et systemansvar for utstyret som skal overvåkes.
Ansvar	Er ansvaret for feilretting definert?	Hendelsen som alarmen overvåker, må håndteres. Det vil ikke være hensiktsmessig å overvåke en alarm hvis ikke dette ansvaret er avklart.

Tabell 2 Kontrollspørsmål ved utvelgelse av alarm til overvåking

Hvis konklusjonen av utvelgelsesprosessen er at alarmen skal implementeres i alarmsystemet, så skal følgende informasjon samles inn og dokumenteres i tilknytning til alarmen (se også kap. 7 for spesielle krav):

- Kilde til alarmen: Objekt ID (ref. Banedata) og objektnavn (utstyr) alarmen stammer fra.
- Hvem skal rette feil/avvik (rolle og kontaktinformasjon).
- Alarmklasse.
- Alarmprioritet (kritikalitet), ref. 8.2.
- Område hvor objektet befinner seg.

- Forventet årsak til alarmer.
- Konsekvens ved ikke å reagere.
- Instruks for håndtering av alarm (inklusive hvilken trafikkstyringsentral som skal konsulteres/informeres samt hvem som skal feilrette/håndtere avvik).
- Spesifikke opplæringskrav til operatør.
- Eventuelle krav for spesifikke alarmklasser, fremgår av 7.

Hvis mulig skal også følgende informasjon innhentes og dokumenteres:

- Forventet P-F intervall.

## 7. Klassifisering av alarmer

Klassifisering er en måte å organisere alarmene basert på felles karakteristikk og krav f.eks. felles krav til opplæring, testing, instruks og dokumentasjon.

For alarmer som ikke tilhører en av de definerte klassene, gjelder de generelle kravene til opplæring og dokumentasjon som fremgår i dette dokumentet.

### 7.1 Klasse 1 – sikkerhetsalarmer

En sikkerhetsalarm er en alarm som varsler om feil/avvik på en sikkerhetsfunksjon eller sikkerhetsrelatert funksjon, eller om endrete betingelser/forhold som medfører en betydelig risikøkning for at en topphendelse inntreffer.

- ✓ *Kun alarmer som vil bli implementert med høyeste prioritet/kritikalitet skal vurderes som kandidater for å være sikkerhetskritiske.*

Eksempler på sikkerhetsalarmer er alarmer som varsler om:

- En topphendelse har inntruffet.
- Sikkerhetsfeil i signalanlegg (definert i «Instruks for mulige sikkerhetsfeil i signalanlegg» [14]).
- Sikkerhetsfeil i infrastrukturen (definert i «Instruks for mulige sikkerhetsfeil i over-/underbygning» [15]).
- (Siste) barrierebrudd.
- Andre betingelser som kan føre til topphendelser og/eller økt risiko når definert nivå passert (for eksempel rasvarsling, innbrudd, person i sporet).

Nye sikkerhetsalarmer skal identifiseres under RAMS-analysen i prosjektene. Det skal fremgå av alarmdokumentasjon at det er en sikkerhetsalarm.

Dersom det av RAMS-analysen avdekkes spesifikke krav til operatør eller til alarmsystemet for å ivareta akseptabel risiko, skal dette klart fremgå av dokumentasjon samt i instruks og krav til

opplæring.

Sikkerhetsalarmer skal presenteres for operatør på en måte som skiller den fra andre alarmer.

*(Merk. i neste revisjon av dokumentet bør tekst gjennomgå og vurderes ift pågående arbeid med å konkretisere sikkerhetsfunksjoner.*

## 7.2 Klasse 2 - alarmer fra jernbaneinfrastruktur

Utstyr i jernbaneinfrastruktur er underlagt forskrifter og regler.

Jernbaneinfrastrukturforskriften, kapittel 2-4. Drift og vedlikehold av jernbaneinfrastruktur [8], pålegger Infrastrukturforvalter (Jernbaneverket) å drifte og vedlikeholde jernbaneinfrastrukturen i henhold til nasjonale og internasjonale standarder. Infrastrukturforvalter skal ha en vedlikeholdsplan for hver strekning. Vedlikeholdsplanen skal inneholde grenseverdier for alle systemer, deler og komponenter av sikkerhetsmessig betydning som angir når umiddelbare tiltak skal iverksettes.

- Alarmgrenser og prioritet må ta inn over seg vedlikeholdsgrenser som er definert for denne type utstyr.
- Operatører skal ha opplæring i henhold til krav i godkjente læreplaner. Læreplanen skal være definert ref. <https://trv.jbv.no/jk/doku.php> «Læreplaner og retningslinjer for jernbanekompetanse» basert på hvilke oppgaver de skal utføre i henhold til instruksene de har for alarmene.
- Alarmer og tilhørende operasjoner skal lagres i minimum 3 måneder med hensikt å kunne revidere jernbanehendelser.
- Ved dokumentasjon av område for hvor utstyr som avgir alarm befinner seg, skal strekningsbeskrivelse og stedskoder som angitt i Banedata benyttes.

## 8. Prioritering av alarmer (kritikalitet)

### 8.1 Føringer for overgangsfase

Jernbaneverket har i dag utstyr med ulike prioritetsnivåer (fra 2 til 5 nivåer) og med ulik tolkning av gitt prioritetsnivå. En alarm som er definert som kritisk (høy prioritet) innenfor et fagområde, er ikke nødvendigvis kritisk for Jernbaneverkets evne til å levere sikker togtransport, oppetidskrav eller god informasjon til kunde og passasjerer.

Jernbaneverkets ambisjon bør i første omgang være å etablere et prioriteringsregime som:

- Er enhetlig for rapportering av alarmer.
- Sikrer at alarmer fra ulike fagområder som overvåkes i samme system prioriteres basert på samme prioritetsskala.
- Gir føringer ved anskaffelse av nytt utstyr/systemer som avgir alarmer.
- Skaper felles oppfatning blant alle som arbeider med alarmer om hvilke alarmer som er mest kritiske i situasjoner hvor det oppstår mange eller komplekse alarmer.

-

## 8.2 Prioritetsnivåer/Kritikalitetsnivåer

- ✓ *Alle alarmer skal behandles av operatør.*

**Alle** alarmer skal behandles når den presenteres for operatør. Dette gjelder også alarmer med lav prioritet.

Prioritering av alarmer skal være til hjelp for operatørene når han/hun ikke klarer å behandle alarmene etter hvert som de kommer (f.eks. når flere alarmer mottas samtidig eller når alarmene oppstår raskere enn at operatøren klarer å behandle dem).

Prioritet skal reflektere kritikaliteten for alarmer og presenteres for operatøren slik at operatøren får best mulig støtte i arbeidet sitt.

- ✓ *Alarmene skal tildeles en prioritet avhengig av konsekvens for Jernbaneverkets evne til å tilby samfunnet et sikkert, pålitelig og tilgjengelig transportsystem.*

I transportsystem inngår også tjenester til publikum og togselskaper som f.eks. trafikkinformasjon.

For vurdering av prioritet benyttes en kvalitativ vurdering. **Riktig kompetanse må delta i vurderingen.**

Alarmer skal gis en prioritet basert på følgende vurderinger:

- Konsekvensen ved at alarmer ikke blir reagert på (se [4], instruks for RCM analyse for konsekvensklasser slik disse er definert i JBV). For å vurdere dette kan informasjon om kritikalitet for utstyret som alarmer mottas fra bidra til vurderingen.
- Forventet ledetid fra alarmer oppstår til avviket den varsler om får konsekvenser for produksjonen av tjenester samt hvor mye tid det vil ta for personell å tilbake stille situasjonen som forårsaker alarm.

Med i konsekvensvurderingen bør også togtetthet vurderes.

Jernbaneverket skal benytte følgende prioriteringsnivåer for alarmer:

Prioritetsnivå (kritikalitetsnivå)	Definisjon
1 Catastrophical	Feil/avvik på <b>sikkerhetsfunksjon eller sikkerhetsrelatert funksjon eller på andre hendelser som medfører en betydelig risikoøkning for at topphendelse</b> inntreffer. (Alle sikkerhetsalarmer)
2 Critical	Feil/avvik som har <b>direkte og umiddelbar</b> innvirkning på Jernbaneverkets evne til å tilby samfunnet et pålitelig og tilgjengelig transportsystem.
3 Major	Feil/avvik som <b>ikke har direkte og umiddelbart</b> innvirkning på Jernbaneverkets evne til å tilby samfunnet

	<p>et pålitelig og tilgjengelig transportsystem, <b>men som vil ha det om ikke tiltak iverksettes raskt</b> dvs. kan få konsekvens for Jernbaneverkets evne til å oppfylle fastsatte mål for punktlighet og oppetid.</p> <p>Feil/avvik som medfører høy risiko for at Jernbaneverket ikke oppnår fastsatte mål f.eks. krav til oppetid for IKT systemer.</p>
4 Minor	Feil/avvik som kan medføre redusert ytelse på en tjeneste. Eventuelt med langt P-F intervall.

✓ *Alarmer bør kunne få endret prioritet basert på tid.*

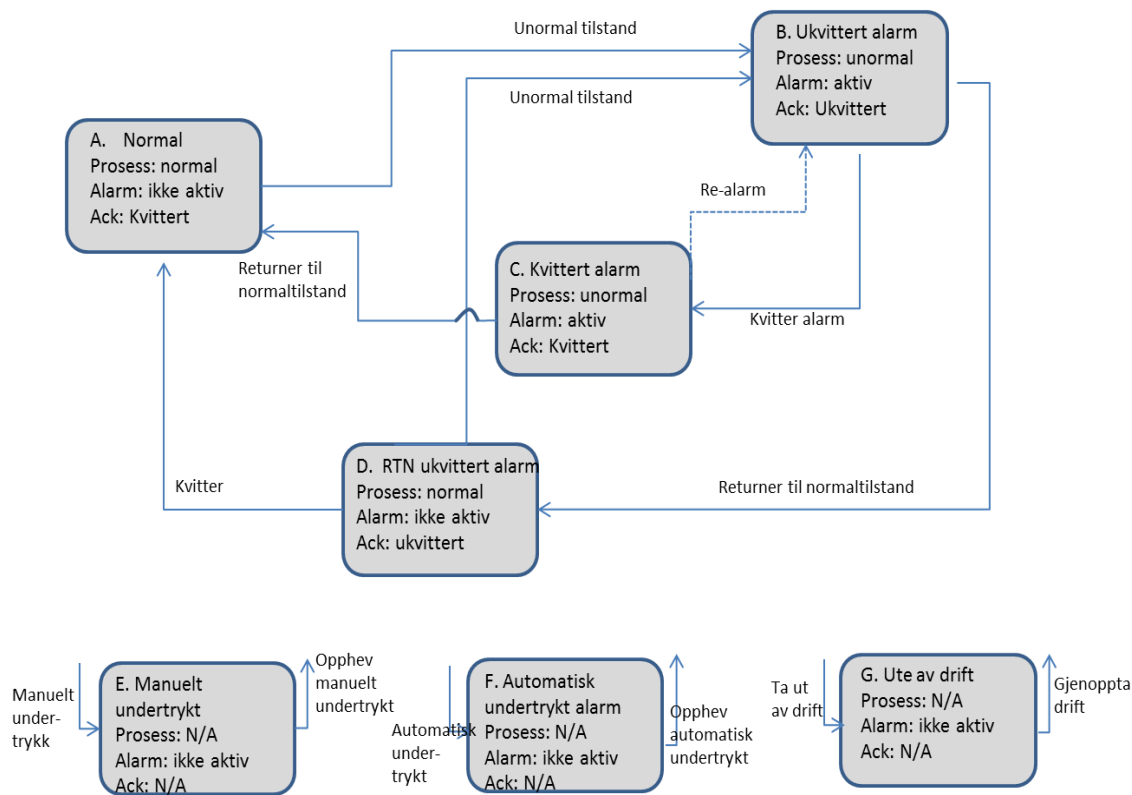
Dersom en alarm har ligget lenge uten at operatør har reagert på den, kan den få oppgradert prioritet. Dette skal i så fall være vurdert og beskrevet før implementering av alarmer i alarmsystemet.

## 9. Designprinsipper for alarmsystemet

### 9.1 Tillatte tilstander

Følgende tilstander skal benyttes (se Figur 3):

- Normal (dvs. ingen alarm).
- Kvittert alarm.
- Ukvittert alarm.
- Manuelt undertrykt alarm.
- Automatisk undertrykt alarm.



Figur 3 Tilstander i alarmsystemet

Figur 3 viser tilstander og tillatte overganger mellom disse. De grå firkantene representerer tilstander. Bokstaven identifiserer tilstanden sammen med navnet til tilstanden. «Ack» viser status for kvittering av alarm fra operatør. Overgang til/fra tilstandene E, F og G skal kunne gå fra/til alle eksisterende alarmtilstander i systemet.

**A Normal** - er normaltilstand dvs. når prosessen (utstyret, systemet) opererer innenfor de normale spesifikasjonene, det er ingen alarm og de siste alarmene er kvittert ut.

**B Ukvittert alarm** – er starttilstanden når prosessen (utstyret, systemet) opererer utenfor de normale spesifikasjonene og har sendt en alarm. Alarmen er ikke kvittert ut av operatør ennå. Tidligere kvitterte alarmer kan designes slik at de returnerer til denne tilstanden etter en tid.

**C Kvittert alarm** – tilstand hvor det er sendt en alarm og operatør har kvittert ut denne.

**D RTN ukvittert alarm (RTN er Returner til normal)**. - prosessen (utstyret, systemet) har returnert til normaltilstand (opererer ikke lenger utenfor de normale spesifikasjonene) og alarmen har forsvunnet før operatør har rukket å kvittere den ut.

**E Manuelt undertrykt** – alarm er undertrykt (blokkert) ved hjelp av funksjon utført av operatør. Alarm varsler ikke lenger til operatør. Manuelt undertrykte alarmer hentes frem igjen av operatør eventuelt – hvis dette er utviklet i systemet – automatisk basert på gitte betingelser.

**F Automatisk undertrykt** – alarm er undertrykt basert på programmert logikk i alarmsystemet. Alarmen varsles ikke til operatør.

**G Ute av drift** – alarmen er undertrykt enten manuelt eller ved hjelp av en funksjon når prosessen (utstyret/systemet) som overvåkes er til vedlikehold. Alarmene varsles ikke til operatør.

Regler for håndtering av tilstander, fremgår av 9.3.

## 9.2 Fastsetting av alarmterskel (Set point)

Der Jernbaneverket har fastsatte vedlikeholdsnivåer [7], skal alarmterskelen i størst mulig grad reflektere disse.

Dette kan f.eks. være grenser for når

- Togfremføringsmessige tiltak må ivaretas inntil tilstand er utbedret (dvs. feilretting må skje umiddelbart).
- Feil blir sikkerhetskritisk og krever umiddelbar stans av trafikk.

Der slike grenser ikke er definert, skal alarmterskel settes på et nivå som balanserer behovet for å unngå falske alarmer med behovet for tidsnok varsling til at operatør og vedlikeholdspersonell får tilstrekkelig tid til å reagere på alarmen.

## 9.3 Funksjonalitet og brukergrensesnitt HMI

### 9.3.1 Føringer for alarm design

Kapittelet skal beskrive regler og metodikk for design av alarmer under gitte betingelser hvor konsistens er viktig, ref. 6.2.23 [2]. Kapittelet anses ikke relevant i denne omgang da Jernbaneverket allerede har alarmsystemer.

Dersom det legges opp til omfattende endring evt. nyanskaffelse (for eksempel i forbindelse med alarmkorrelering), skal dette kapittelet utarbeides og ny versjon av alarmfilosofien godkjennes som grunnlag for kravspesifikasjon.

### 9.3.2 Kvittering av alarm

Regler for kvittering av alarm bør utarbeides i neste revisjon av alarmfilosofien.

### 9.3.3 Undertrykking av alarm

Regler for undertrykking av alarm bør utarbeides i neste revisjon av alarmfilosofien. Reglene bør hensynta at alarmene har ulik kritikalitet.

### 9.3.4 Presentasjon av alarmer (HMI design prinsipper)

Kapittelet skal dokumentere metode, format og «koding» (f.eks. fargevalg, symbolkatalog etc.) for alarmpresentasjon til operatør samt etablere prinsipper for presentasjon og varsel (ref.6.2.10 i [2]).

Kun overordnede prinsipper er definert i denne utgaven av alarmfilosofien ettersom Jernbaneverket

allerede har alarmsystemer.

Dersom det legges opp til omfattende endring evt. nyanskaffelse, skal dette kapittelet utarbeides som grunnlag for kravspesifikasjon. De overordna prinsippene beskrevet nedenfor, skal da legges til grunn.

- ✓ *Alarmene skal presenteres i et antall og format som tar hensyn til menneskelig evne til å behandle mengde og type informasjon.*
- ✓ *Alarmene skal presenteres på en måte som gjør det enklest mulig for operatørene raskt å gjenkjenne, forstå og reagere på alarmen.*

Ifølge [1], klarer den menneskelige hjerne kun å holde på 7 +/- 2 informasjonsenheter samtidig. Det er derfor viktig at operatørene ikke blir presentert for flere alarmer enn vedkommende kan håndtere i en presset situasjon. Selv om operatøren kun skal videreformidle alarmen til en annen instans for feilretting krever dette tid. F.eks. hvis operatøren må gjøre ulike oppslag for å identifisere hvilken vakttelefon som skal motta alarmen og forskjellige instanser skal koordineres.

Dette skal reflekteres i hvilke skjermbilder som lages og hvor mange alarmer som presenteres i det skjermbildet som benyttes for kontinuerlig overvåking.

- ✓ *Alarm skal presenteres til operatør uten opphold.*

Alarmer kan være kritiske og kreve umiddelbare tiltak. Det er derfor viktig at de presenteres umiddelbart når de oppstår.

- ✓ *En unik kombinasjon av varslingsmåter (visuelt og/eller akustisk) skal benyttes for å skille mellom prioritetsnivåer.*

Varslingsmåter og layout på skjermbilder skal utvikles med hensikt å gi operatør rask oversikt over status og tilstand for utstyret som overvåkes.

### **9.3.5 Alarmhistorikk**

Historikk med utgangspunkt i alarmlogg skal lagres som grunnlag for trendanalyser, feilstatistikker og ytelsesmålinger.

Alarmloggen bør inneholde alarm ID, alarmtekst, utstyr som er opphav til alarmen, tidspunkt for når alarmen oppstår og når den opphører, prioritet/kritikalitet samt informasjon om undertrykking og varighet av denne.

## **10. Opplæring, instruks og dokumentasjon**

### **10.1 Opplæring**

Prinsipper som skal ligge til grunn:

- ✓ *Operatør skal kun behandle alarmer som vedkommende har mandat og kunnskap til å behandle.*
- ✓ *Operatøren skal ha klar instruks om hvordan alarmer som vedkommende mottar skal håndteres.*



- ✓ *Operatøren skal ha opplæring og systematisk trening i all realistisk bruk av alarmsystemet og handlinger som vedkommende skal utføre basert på mottatt alarm.*

Alle operatører av alarmsystemet skal ha opplæring i:

- Funksjonalitet og bruk av alarmsystemet. Operatørene skal ha kunne forstå betydningen av symboler, fargevalg og lignende i HMI og kunne utnytte funksjonaliteten i systemet effektivt. Dette gjelder både generell funksjonalitet og spesifikk bruk i Jernbaneverket.
- Alarmene og instruksene i tilknytning til alarmene. Operatørene skal ha tilstrekkelig kunnskap til at de kan gjøre de riktige vurderingene og iverksette nødvendige aksjoner.
- Systemkunnskap dvs. å ha overordnet forståelse for hvordan utstyret som avgir alarmer inngår i et overordnet system og hvilken rolle utstyret har i dette.

Opplæringen skal inneholde både en teoretisk del og praktisk «on-the-job» opplæring under veiledning fra erfaren operatør.

Overordnet leder for operatørene har ansvar for at det finnes en opplæringsplan som konkretiserer hvilken opplæring ulike operatørfunksjoner skal ha for at ovenstående prinsipper og føringer ivaretas. Han/hun har også ansvar for at opplæring er gjennomført før operatøren blir satt til selvstendige overvåkingsoppgaver.

## 10.2 Instrukser

Instrukser for håndtering av alarmer skal være utarbeidet og tilgjengelig (se 10.3). Dersom det finnes eksisterende alarmer uten instrukser, skal det finnes en generell instruks for hvordan disse skal behandles (Den generelle instruksjonen skal bidra til at alarmene over tid får en mer spesifikk prosedyre eller fjernes fra systemet).

For følgende instrukser henvises til systemansvarlig for alarmsystemet:

- Loggføring av alarmer.
- Endring av alarmsystemet.
- Vedlikehold av alarmsystemet.

## 10.3 Dokumentasjon

Alarmsystemet skal være dokumentert og dokumentasjon for systemet bør omfatte:

- Alarmfilosofi (dette dokumentet).
- Strategi for alarmdesign (skal som minimum omfatte metodikk for utvikling av systemet og involvering av operatører/ytelseskrav, veiledning til leverandører av systemer som genererer alarmer, ordliste og definisjoner for bruk i alarmmeldinger). Kan innarbeides i alarmfilosofien.
- Brukermanual for alarmsystemet skal lagres i ProArc.
- Teknisk manual for alarmsystemet skal lagres i ProArc.

- Læreplaner for operatører.
- Rapporter fra KPI-målinger og revisjonsgjennomganger (skal lagres i Saksrom på Sak opprettet av Systemansvarlig).
- Alarmdokumentasjon:
  - o Dokumentasjon fra utvelgelse av alarmer.
  - o Instruks for håndtering av alarm.

Alarmdokumentasjon skal foreligge elektronisk og gjøres enkelt tilgjengelig for operatør.

Det skal finnes en oversikt over dokumenter og hvor disse er lagret (indeksring). Ved endringer skal det legges til rette for mest mulig sømløs knytning mellom alarm og alarmdokumentasjon.

## 11. Implementering og idriftsetting

Systemansvarlig for alarmsystemet skal kontaktes av tiltakshaver/prosjektansvarlig straks det er klart at de vil ha behov for å overvåke alarmer.

Tiltakshaver/prosjektansvarlig må på tidlig tidspunkt planlegge og å følge opp aktiviteter som sikrer at kontrollspørsmålene nedenfor er ivaretatt ved implementering og idriftsetting av nye alarmer.

Kontrollspørsmål	Kommentar
Er det laget en oversikt over alt utstyr (med plassering) som avgir alarmer?	
Er utstyret registrert i Banedata?	Alt utstyr skal være registrert i Banedata (det finnes noen unntak- for disse skal annet, godkjent register for registrering benyttes)
Benytter andre fagområder samme type utstyr?	Dersom tilsvarende utstyr allerede finnes og overvåkes i JBV bør standardisering tilstrebes.
Er utvelgelsesprosessen gjennomført?	
Er det etablert transmisjon for å overføre alarmer til sentral overvåking?	
Er systemansvaret for utstyret besluttet og er Single Point of Contact hos systemansvarlig pekt ut?	
Er ansvaret for feilretting avklart?	
Har systemansvarlig for utstyret tilgang til riktig	Systemansvarlig vil fungere som 2. linje og

verktøy til å kunne gjennomføre rotårsaksanalyse og feilanalyse?	vil måtte bistå overvåkingsfunksjon med feilanalyse.
Er avtaler SLA/OLA utarbeidet og signert?	
Er det implementert grensesnitt for integrasjon mellom systemer?	
Er ende-til-ende test gjennomført?	Verifisere at alarm kommer frem og presenteres som forventet
Er relevante prosedyrer oppdatert?	
Er nødvendig dokumentasjon oppdatert?	
Er behov for opplæring av overvåkingspersonell identifisert og gjennomført?	
Er alle stående alarmer og kjente feil lukket før idriftsetting?	

Tabell 3 Kontrollspørsmål ved implementering og idriftsetting av alarmer

## 12. Drift og vedlikehold av alarmsystemet

### 12.1 Vedlikehold

For generelle retningslinjer for vedlikehold av alarmdatabase etc., henvises til systemansvarlig for det aktuelle systemet.

Alarmer fra utstyr under vedlikehold og testing skal kunne fjernes fra operatørens alarmoversikt i perioden dette pågår for å unngå at disse alarmene tar oppmerksomhet fra andre, viktige alarmer.

Dette kan implementeres på ulike måter. Hvordan dette gjøres og prosedyrer for dette skal være definert og implementert før alarmer fra utstyret implementeres i alarmsystemet.

### 12.2 Endringshåndtering

Følgende defineres som en endring:

- Endring i alarmattributt.
- Integrasjon av nye alarmer i alarmsystemet.
- Fjerning av alarm.
- Ny, eller endret alarmfunksjonalitet.
- Nytt eller endret bilde.

Endringer skal godkjennes av systemansvarlig for alarmsystemet.

Konsekvenser for endringen for det eksisterende alarmsystemet, operatørene (bemanning, opplæring) og prosedyrer skal være vurdert for endringen og berørte parter skal være informert.

Relevant dokumentasjon skal oppdateres og operatørene skal ha fått opplæring på endringen før denne idriftsettes.

### 13. Overvåking og optimalisering av alarmsystemet

#### 13.1 Måling av kvalitet og effektivitet for alarmsystemet

Kvaliteten til alarmsystemet kan endres over tid. Faktorer som kan påvirke dette er f.eks.:

- At underliggende systemer genererer «falske alarmer» dvs. varsler om noe som ikke krever utbedring.
- Utstyr er feil konfigurert og sender alarmer uten riktig informasjon, eller ikke relevante alarmer.
- Rotårsak for alarmene er ikke håndtert.
- Alarmer på grunn av feil i felles infrastruktur (f.eks. strømforsyning, transmisjon) medfører følgealarmer fra systemer som er tilknyttet infrastrukturen.

For å identifisere faktorer som skaper utfordringer for operatør og påvirker hans/hennes evne til å oppdage og reagere på alarmer, skal ytelsen til systemet vurderes og måles. Resultatene for målingene skal benyttes for å foreslå og å iverksette forbedringstiltak.

- *Det skal etableres et måleregime for å måle kvalitet og effektivitet av alarmsystem.*

Forbedringer kan kreve endringer i tilgrensede systemer eller prosedyrer på tvers av organisasjonsheter samt i instruksjer. Det er derfor viktig at systemforvalter for fagsystemene (alarmgivende systemer) deltar i analysen av resultatene og iverksetter nødvendige tiltak i egne systemer, prosedyrer og instruksjer.

Det skal gjennomføres regulære, kvartalsvise møter for gjennomgang av KPI-er og generelle problemstillinger rundt alarmer. I tillegg skal det gjennomføres møter ved behov.

- Systemansvarlig for alarmsystemet har ansvar for å innkalle til og administrere møtene. Dette innebærer også referatføring og saksbehandling knyttet til å fremme tiltak i etterkant.
- Deltakere på møtene skal være operatører, systemansvarlig for alarmsystemet og systemansvarlig for relevante fagsystemer (avhengig av hvilke problemområder som skal diskuteres).
- Tema skal være KPI-er og utvikling av disse, generelle problemstillinger i tilknytning til alarmovervåking som identifisert av operatør, systemansvarlig for alarmsystem eller systemansvarlig fagsystem.
- Tiltak skal identifiseres og gjennomføres dersom det er innenfor mandat til deltakerne. Alternativt skal systemansvarlig for alarmsystemet fremme tiltak oppover i organisasjonen.

Det skal gjennomføres en kvartalsvis rapportering av KPI-er (månedlig for S-1) og utvikling av disse

til Infrastrukturdirektør. Rapporten skal synliggjøre resultat for måling, utvikling av KPI i løpet av året, tiltak gjennomført og anbefalte tiltak. Det er systemansvarlig for alarmsystemet som har ansvar for at rapport utarbeides.

### 13.2 Revisjon av alarmsystemet

Det skal gjennomføres revisjon av alarmhåndteringssystemet og prosessene ved behov – f.eks. etter store endringer, eller dersom det er signaler som tilsier at operatørene ikke får tilstrekkelig støtte for å gjøre oppgavene sine og KPI-ene ikke gir tilstrekkelig svar.

Revisjonen skal blant annet avdekke om:

- Alle alarmer som presenteres til operatør krever reaksjon.
- Alarmprioriteringen oppfattes som riktig.
- Alarmene varsler tidlig nok til at nødvendig aksjon kan gjennomføres før konsekvens inntreffer
- Operatørene opplever at de har tilstrekkelig opplæring
- Operatøren har tilstrekkelig støtte for analyse
- Alarmene er godt nok dokumentert

Revisjonen skal gjennomføres basert på intervjuer med operatørene.

Systemansvarlig for alarmsystemet har ansvaret for å iverksette revisjon.

## 14. Referanser

[1] Prinsipper for utforming av alarmsystemer, februar 2001, YA-710, Oljedirektoratet.

[2] NEK EN 62682:2015 Management of alarms systems for the process industries.

[3] STY-601058 Håndbok for vedlikehold.

[4] STY-601128 Instruks for RCM-analyse.

[5] EEMUA Publication 191 – Alarm systems: a guide to design, management and procurement.

[6] EN 50126 siste revisjon.

[7] [https://trv.jbv.no/wiki/Felles\\_bestemmelser/Generelle\\_bestemmelser#Tid\\_til\\_utbedring\\_av\\_feil](https://trv.jbv.no/wiki/Felles_bestemmelser/Generelle_bestemmelser#Tid_til_utbedring_av_feil).

[8] STY- 602165 Strekningsbeskrivelse for Jernbaneverkets nett del 8. tunneloversikt og særskilte brannobjekter.

[9] Forskrift om nasjonale tekniske krav m.m. for jernbaneinfrastruktur på det nasjonale jernbanenettet (Jernbaneinfrastrukturforskriften) (FOR-2011-04-11-388).

[10] Teknisk Regelverk, Signal/Prosjektering/betjeningsanlegg, kap 3.7.

[11] 0901410201 Referat fra ledermøtet 17.09.2015.

[12] STY-602279 Trafikkregler for Jernbaneverkets nett.

[13] Operativ regelsamling, <http://10.251.36.130/tswiki/doku.php>.

[14] STY-601563 Instruks for tiltak ved mistanke om- eller avdekket sikkerhetsfeil i signalanlegg, vedlegg 1.

[15] STY-601529 Instruks for tiltak ved mistanke om sikkerhetsfeil i over- / underbygning, vedlegg 5.

[16] STY-600095 Krav til dokument og dokumenttype.

## **15. Vedlegg**

Vedlegg 1 KPI-er for Fjel og TeMip

Vedlegg 2 Samsvarstabell mellom krav til innhold i alarmfilosofi som definert i [2] og alarmfilosofi for JBV.

## VEDLEGG 1- KPIer for Fjel og TeMip

I vedlegget defineres et sett av KPI-er for å måle og følge opp kvalitet og effektivitet i TeMip og Fjel. KPI-ene er gitt en unik ID og et navn.

KPI-er med ID som består av Y og et nummer, er KPI-er som måler om alarmer presenteres på en effektiv måte.

KPI-er som er benevnt S og et tall, er KPI-er som sier noe om den tekniske kvaliteten til alarmsystemet samt effektiviteten i feilretting av alarmsystemet.

Y-1 til Y-3 samt S-1 skal måles fra start, mens systemansvarlig vurderer behovet for å måle Y-4 og Y-5.

### Y-1 Gjennomsnittlig alarmrate per operatør

<b>KPI-ID</b>	Y-1
<b>KPI-navn</b>	Gjennomsnittlig alarmrate per operatør
<b>Hensikt</b>	Avdekke om operatør får presentert for mange alarmer til håndtering i gjennomsnitt over tid.  Verdien anses å gi en god indikator på om alarmsystemet fungerer tilfredsstillende og bør ses i sammenheng med PY-2. Vedvarende overskridelser av anbefalt maksgrense indikerer at alarmsystemet presenterer flere alarmer enn det operatørene kan behandle. Perioder med flere alarmer enn operatør kan behandle, øker sannsynlighet for tapte alarmer selv om gjennomsnitt for alarm er akseptabelt.
<b>Målemetode</b>	Gjennomsnittlig antall alarmer presentert per operatør i overvåkingsbildet per døgn målt over en periode på 30 dager. Med operatør forstås her en person kontinuerlig i 24 timer.
<b>Måltall</b>	Antatt akseptabelt 144 alarmer/døgn Maksgrense 288 alarmer/døgn
<b>Angitt i måleenhet</b>	Antall alarmer/døgn
<b>Datakilde</b>	Alarmbehandlingssystemene (separate målinger gjøres for Fjel og TeMip)
<b>Eier av KPI</b>	Infrastrukturdirektør
<b>Ansvarlig for målinger</b>	Systemansvarlig alarmsystem
<b>Måleperiode</b>	Månedlig – 1. i hver måned
<b>Rapporteringsperiode</b>	Kvartalsvis (1. desember – 1. mars, 1. mars – 1. juni, 1.juni - 1.august, 1.august – 1. desember). Første dato i periode er «fra og med», siste dato i periode er «til».



<b>Dato for endring av KPI</b>	
<b>Endringslogg</b>	
<b>Kommentar</b>	Måltall hentet fra EEMUA 191

**Y-2 Fordeling alarmprioritet**

<b>KPI-ID</b>	Y-2
<b>KPI-navn</b>	Fordeling av prioritet
<b>Hensikt</b>	Avdekke om fordelingen av alarmer på ulike prioritetsnivå er slik at operatør får støtte til å oppdage Critical og Major alarmene. Stor andel Critical og Major alarmer, vil medføre økt risiko for at operatør ikke reagerer på kritiske alarmer.
<b>Målemetode</b>	Antall alarmer med gitt prioritet (ref. 8.2) i forhold til totalt antall alarmer presentert for operatør i en 30 dagers periode.
<b>Måltall</b>	Critical: 5 % Major 15 % Minor 80%
<b>Angitt i måleenhet</b>	% av totalt antall alarmer presentert for operatør (operatør er
<b>Datakilde</b>	Alarmbehandlingssystemene (separate målinger gjøres for Fjel og TeMip)
<b>Eier av KPI</b>	Infrastrukturdirektør
<b>Ansvarlig for målinger</b>	Systemansvarlig alarmsystem
<b>Måleperiode</b>	Kvartalsvis (1. desember – 1. mars, 1. mars – 1. juni, 1.juni - 1.august, 1.august – 1. desember). Første dato i periode er «fra og med», siste dato i periode er «til».
<b>Dato for endring av KPI</b>	
<b>Endringslogg</b>	
<b>Kommentar</b>	Måltall hentet fra EEMUA 191

**Y-3 alarmrush**

<b>KPI-ID</b>	Y-3
<b>KPI-navn</b>	Alarmrush
<b>Hensikt</b>	<p>Avdekke om operatør i perioder får presentert alarmrater på mer enn 10 alarmer i løpet av 10-minutters periode.</p> <p>Verdien anses å gi en god indikator på om alarmsystemet fungerer tilfredsstillende og bør ses i sammenheng med PY-1.</p>
<b>Målemetode</b>	<p>Antall perioder med mer enn 10 innkomne alarmer per operatør. 1 periode er 10 minutter. Antallet alarmer for de 2 største alarmrushene</p> <p>Med operatør forstås her en person kontinuerlig i 24 timer.</p>
<b>Måltall</b>	Fastsettes etter måling av baseline
<b>Angitt i måleenhet</b>	%
<b>Datakilde</b>	Alarmbehandlingssystemene (separate målinger gjøres for Fjel og TeMip)
<b>Eier av KPI</b>	Infrastrukturdirektør
<b>Ansvarlig for målinger</b>	Systemansvarlig alarmsystem
<b>Måleperiode</b>	Kvartalsvis (1. desember – 1. mars, 1. mars – 1. juni, 1.juni - 1.august, 1.august – 1. desember). Første dato i periode er «fra og med», siste dato i periode er «til».
<b>Dato for endring av KPI</b>	
<b>Endringslogg</b>	
<b>Kommentar</b>	Forutsetter at alarmsystemet kan måle i 10 minutters perioder.

**Y-4 Gjennomsnittlig antall stående, aktive alarmer**

<b>KPI-ID</b>	Y-4
<b>KPI-navn</b>	Gjennomsnitt antall stående, aktive alarmer
<b>Hensikt</b>	Avdekke om det er alarmer som egentlig ikke burde være alarmer (f.eks. alarmer som ikke krever reaksjon)
<b>Målemetode</b>	Måle antallet alarmer som blir stående aktivt mer enn 24 timer.

<b>Måltall</b>	Måltall settes etter måling av baseline
<b>Angitt i måleenhet</b>	Gjennomsnittlig antall/år
<b>Datakilde</b>	Alarmbehandlingssystemene (separate målinger gjøres for Fjel og TeMip)
<b>Eier av KPI</b>	Infrastrukturdirektør
<b>Ansvarlig for målinger</b>	Systemansvarlig alarmsystem
<b>Måleperiode</b>	Kvartalsvis (1. desember – 1. mars, 1. mars – 1. juni, 1.juni - 1.august, 1.august – 1. desember). Første dato i periode er «fra og med», siste dato i periode er «til».
<b>Dato for endring av KPI</b>	
<b>Endringslogg</b>	
<b>Kommentar</b>	

#### Y-5 Manuelt undertrykte alarmer

<b>KPI-ID</b>	Y-5
<b>KPI-navn</b>	Manuelt undertrykte alarmer
<b>Hensikt</b>	Avdekke om det er alarmer som egentlig ikke burde varsles som alarm (f.eks. støyalarmer) eller om alarmer blir glemt
<b>Målemetode</b>	Antallet manuelt undertrykte alarmer i % av totalt antall alarmer over 30 dagers periode Varighet alarm er undertrykket (over 30 dager) Gjennomsnitt varighet alarm er undertrykket over 30 dager
<b>Måltall</b>	Måltall settes etter måling av baseline
<b>Angitt i måleenhet</b>	% Tid (timer)
<b>Datakilde</b>	Alarmbehandlingssystemene (separate målinger gjøres for Fjel og TeMip)
<b>Eier av KPI</b>	Infrastrukturdirektør
<b>Ansvarlig for målinger</b>	Systemansvarlig alarmsystem

<b>Måleperiode</b>	Kvartalsvis (1. desember – 1. mars, 1. mars – 1. juni, 1.juni - 1.august, 1.august – 1. desember). Første dato i periode er «fra og med», siste dato i periode er «til».
<b>Dato for endring av KPI</b>	
<b>Endringslogg</b>	

**Y-6 Alarmer per fagsystem**

<b>KPI-ID</b>	Y-6
<b>KPI-navn</b>	Alarmer per fagsystem
<b>Hensikt</b>	Avdekke om det er systemer som genererer forholdsvis stor andel av totalt alarmvolum
<b>Målemetode</b>	Antallet alarmer per fagsystem per 30 dager i % av det totale antallet alarmer i perioden
<b>Måltall</b>	Måltall settes etter måling av baseline
<b>Angitt i måleenhet</b>	%
<b>Datakilde</b>	Alarmbehandlingssystemene (separate målinger gjøres for Fjel og TeMip)
<b>Eier av KPI</b>	Infrastrukturdirektør
<b>Ansvarlig for målinger</b>	Systemansvarlig alarmsystem
<b>Måleperiode</b>	Kvartalsvis (1. desember – 1. mars, 1. mars – 1. juni, 1.juni - 1.august, 1.august – 1. desember). Første dato i periode er «fra og med», siste dato i periode er «til».
<b>Dato for endring av KPI</b>	
<b>Endringslogg</b>	
<b>Kommentar</b>	

**S-1 Tilgjengelighet**

<b>KPI-ID</b>	S1
<b>KPI-navn</b>	Tilgjengelighet
<b>Hensikt</b>	Måle om tilgjengeligheten av systemet er tilstrekkelig

<b>Målemetode</b>	<p>Tilgjengelighet A defineres som (Ref. Teknisk Regelverk sannsynligheten for at systemet er i stand til å utføre sin tiltenkte funksjon, forutsatt at de eksterne rammebetingelsene er oppfylt.</p> <p>Tilgjengelighet A beregnes som følger:</p> $A = ((MTBF-MTTR)/MTBF)*100$ <p>Gjennomsnittlig tid til reparert MTTR (Mean Time to Restoration; Mean Time to Repair) er spesifisert som tiden fra en feil blir detektert til feilen er ferdig reparert. MTTR inkluderer gjennomsnittlig logistisk forsinkelse MLD (Mean Logistic Delay) (typisk reisetid) og MRT (Mean Repair Time) gjennomsnittlig tid for reparasjon.</p> $MTTR = MLD + MRT$ <p>MTBF er <math>1 / \text{feilrate}</math></p>
<b>Måltall</b>	<p>99.985 % for TeMip<sup>1</sup></p> <p>99,98 % for Fjel</p>
<b>Angitt i måleenhet</b>	%
<b>Datakilde</b>	Alarmbehandlingssystemene (separate målinger gjøres for Fjel og TeMip)
<b>Eier av KPI</b>	Infrastrukturdirektør
<b>Ansvarlig for målinger</b>	Systemansvarlig alarmsystem
<b>Måleperiode</b>	Ved utgangen av hver måned
<b>Dato for endring av KPI</b>	
<b>Endringslogg</b>	
<b>Kommentar</b>	<p>Måltall kan være ulike for Fjel og TeMip.</p> <p>For sammenligning har Fjernstyringssystemer (CTC) systemene krav til 99,98 % tilgjengelighet.</p> <p>Det kan være hensiktsmessig å stille krav til transmisjon og underliggende systemer for alarmer med høy kritikalitet og som krever umiddelbar reaksjon.</p>

<sup>1</sup> Krav fra ERTMS prosjektet

## VEDLEGG 2 Samsvarstabell mellom krav til innhold i alarmfilosofi som definert i [2] og alarmfilosofi for JBV.

NEK EN 62682:2015			Alarmfilosofi for Jernbaneverket	
Innhold	Påkrevd/anbefalt	Kapittel i standard	Kapittel i alarmfilosofi	Kommentar
Purpose of alarm system	Påkrevd	6.2.2	5.1	
Definitions	Påkrevd	6.2.3	4.1	
References	Påkrevd	6.2.4	14	
Roles and responsibilities for alarm management	Påkrevd	6.2.5	5.2	
Alarm design principles	Påkrevd	6.2.6	9.3.1	
Rationalization	Påkrevd	6.2.7	0	
Alarm class definition	Påkrevd	6.2.8	7	
Highly Managed alarms	Anbefalt	6.2.9	Ikke inkludert	
HMI design principles	Påkrevd	6.2.10	9.3.4	Ikke definert siden JBV allerede har etablerte alarmsystemer
Prioritization method	Påkrevd	6.2.11	8	
Alarm setpoint determination	Anbefalt	6.2.12	9.2	Definert prinsipielt
Alarm system performance monitoring	Påkrevd	6.2.13	13	

Alarm system maintenance	Påkrevd	6.2.14	12	
Testing of alarms	Påkrevd	6.2.15	7.1	Kun behandlet ifbm sikkerhetsalarmer
Approved enhanced and advanced alarming techniques	Anbefalt	6.2.16	Ikke inkludert	
Alarm documentation	Påkrevd	6.2.17	10.3	
Implementation guidance	Påkrevd	6.2.18	11	Henviser til eksisterende systemer
Management of change	Påkrevd	6.2.19	12.2	
Training	Påkrevd	6.2.20	10.1	
Alarm history preservation	Påkrevd	6.2.21	9.3.5	
Related site procedures	Anbefalt	6.2.22	Ikke inkludert	
Specific alarm design considerations	Anbefalt	6.2.23	9.1.4	Ikke spesifisert ettersom JBV allerede har eksisterende alarmsystemer
Alarm system audit	Påkrevd	6.2.24	13.2	