

Veileder til forskrift om sikring på jernbane

Utvalgte tema, bransjemøte 12. juni 2019



Statens **jernbanetilsyn**

Utvalgte tema – tilsynserfaring

- Styringssystem
 - o Informasjonssikring
 - Identifisere informasjon
 - Nødvendig kontroll med informasjon
- Risikovurderinger
 - o Risiko i grensesnitt mellom aktører
 - o Normal- og beredskapssituasjoner



Formål og virkeområde (§§ 1-1, 1-2)

- ... arbeide systematisk og proaktivt for å unngå tilsiktede uønskede handlinger og begrense konsekvensene av dem.
- ... uønsket hendelse som forårsakes av en aktør som handler med hensikt, begrenset til terror og sabotasje og trussel om dette samt hærværk og tyveri med særlig stort skadepotensial.

Styringssystem for sikring



- Noen virksomheter erfarer at det er en fordel å integrere styring av sikring i sikkerhetsstyringssystemet
- Det skal være et godt samsvar mellom det dokumenterte styringssystemet og en felles praksis i virksomheten

Vurder å skjerme informasjon ...

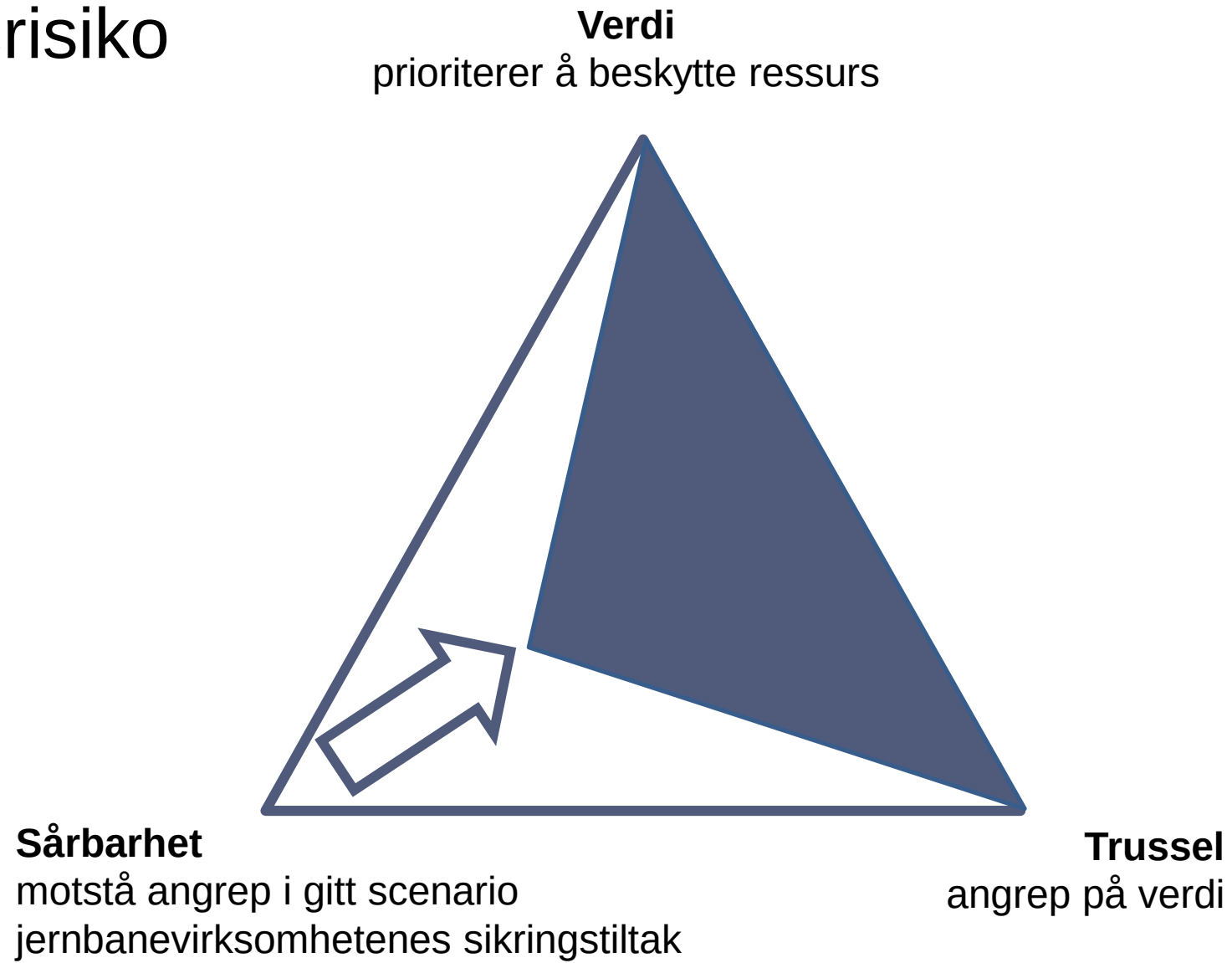
- om verdier, trusler og sårbarheter
- om sikringstiltak
- om sikringsrelaterte hendelser
- om sammenstilling og bekreftelse av informasjon som er åpent tilgjengelig
- som gjør det enkelt å finne informasjon som er skjermet

... som noen kan utnytte

Nødvendig kontroll – skjermet informasjon

- Merking av skjermet informasjon, for eksempel *skjermet jf. sikringsforskriften §§ 3-3 og 3-4*
- Rutiner for å håndtere informasjon som er skjermet
 - For eksempel i henhold til ISO 27001/27002
- Vurdere behov for godkjenning av personell med hensyn til å håndtere skjermet informasjon
 - Merk at innsidetrussel kan oppstå etter en første godkjenning
- Det er taushetsplikt, jf. § 3-4

Sikringsrisiko



Om verdivurderinger

- Ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen, jf. forskriften § 1-3 bokstav n
- Verdier kan omfatte utenforstående (tredjeparters) verdier for eksempel mennesker, symbolbygg, infrastruktur og ytre miljø – forbundet med jernbanen
 - Slike verdier bør inkluderes i jernbanevirksomhetens risikovurderinger, dersom jernbanevirksomheten har kunnskap om slike verdier og kan bidra til å redusere risikoen

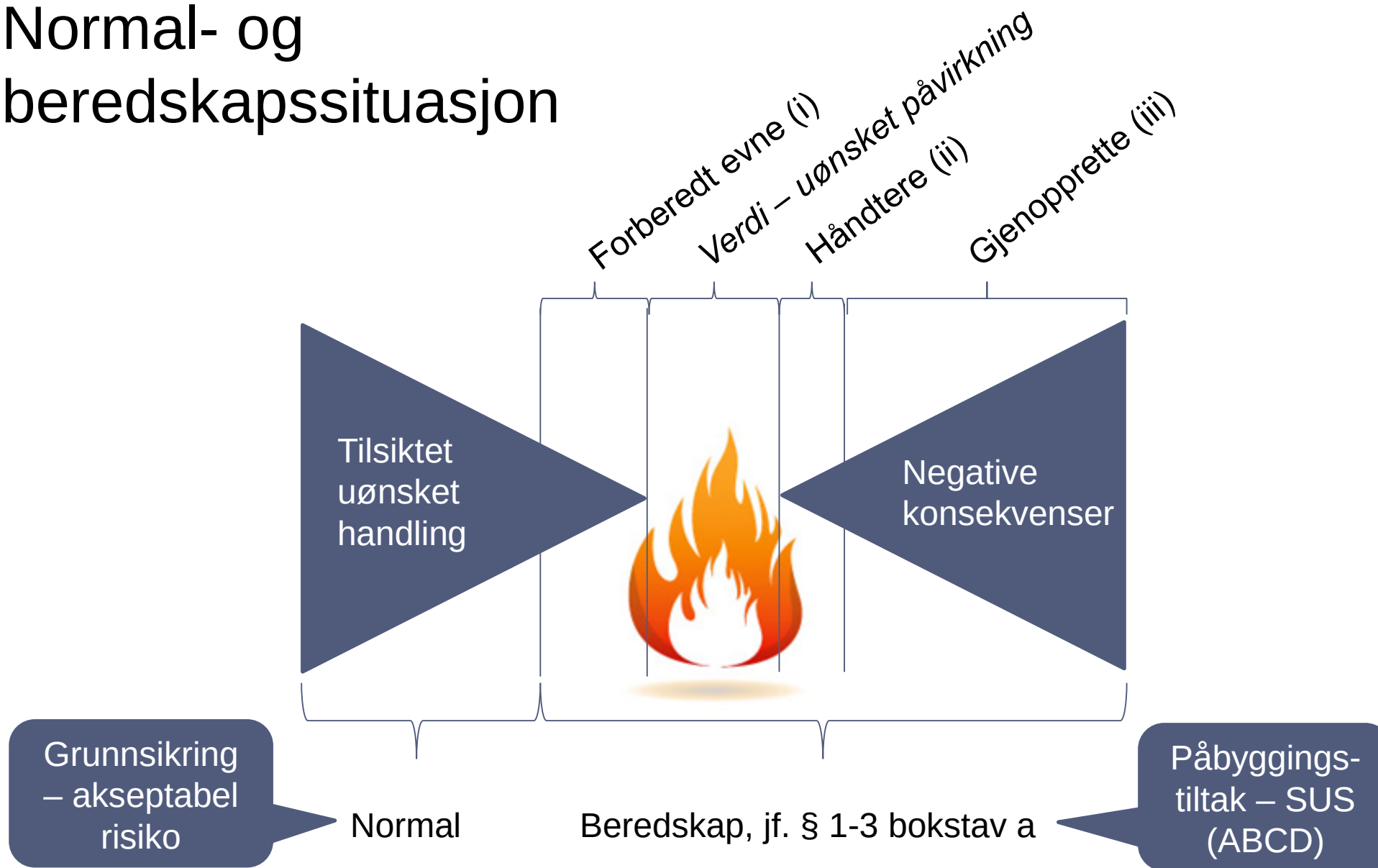
Mine og dine verdier ...? Grensesnitt



Relevante risikoer kan omfatte

- Passasjerenes liv og helse
- Eget og leverandørers personell
- Opprettholdelse av driften
- Gods
- Konsekvenser av angrep kan ramme utenforstående
- Angrep på andre kan få negative konsekvenser for jernbanevirksomheten
- Ressurser som andre eier/forvalter, for eksempel infrastrukturforvalter, som et jernbaneforetak drar fordel av
- Jernbanevirksomheten kan utnyttes for å skade andre

Normal- og beredskapssituasjon



Spørsmål og kommentarer?

- Informasjonssikring
- Grensesnitt mellom aktører
- Normal- og beredskapssituasjoner
 - Grunnsikring
 - Påbyggingstiltak
- Veiledningsbehovet?



Flere spørsmål? Kontakt SJT på e-post: post@sjt.no

Evaluering av sikringsforskriften

- SJT skal evaluere sikringsforskriften
 - Arbeidet påbegynnes i løpet av høsten 2019
 - Ved revidering av forskriften planlegger vi å sende ut høringsnotat med forslag til endringer i løpet av våren 2020
- Vi ønsker å involvere bransjen så tidlig som mulig!
 - Send deres innspill til post@sjt.no



Styring av sikringsrisiko – risikovurderinger i praksis

Bransjemøte sikring – Statens jernbanetilsyn
12. juni 2019

Anne-Kari Valdøl



PREPARED.

I dag



- Er det håndterbart? Hva må til?
- Praktisk bruk sikringsrisikovurderinger
 - Verdivurdering
 - Scenarioer
 - Grunnsikring
- Status for NS 583x-serien

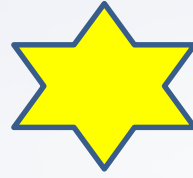


Er det håp?

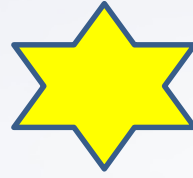


Tilbakevendende strategier...

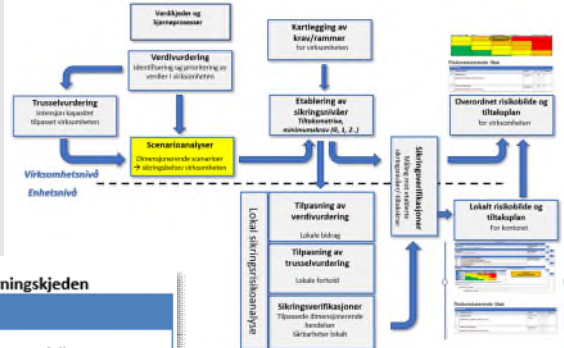




Tør å prioritere



**Stol på fornuftige vurderinger – vær
forsiktig med tall og indekser...**

Trusselvurdering for
virksomheten AS

Dimensjonerende scenarioer



Scenario

Beskrivelse av scenario/trusler

1. En eller flere personer som har autorisert tilgang til forsyningskjeden benytter seg av tilgangen og stjeler, ødelegger eller manipulerer materiellet enten på base, lager eller under transport.
2. En eller flere personer som ikke har autorisert tilgang til forsyningskjeden tar seg ulovlig inn/bryter seg inn på base eller lager, og stjeler, ødelegger eller manipulerer materiellet.
3. En eller flere personer tar seg inn og stjeler, ødelegger eller manipulerer materiellet mens det er under transport fra et punkt til et annet.
4. En eller flere personer bryter seg inn i eller stjeler transportmiddelet hvor materiellet oppbevares, mens det står i ro.

Trusselvurdering

Virksomheten har materiell på flere forskjellige lagre. En del av dette materialet er av stor viktighet i forbindelse med operasjonene som selskapet utfører, og tap av slikt materiell kan påføre selskapet store kostnader både i form av tap av materialet og ved eventuell utsettelse av arbeidet.

Materiell har i seg selv en økonomisk verdi som kan være av interesse for enkeltpersoner/kriminelle som ser muligheten for vinning ved videresalg. Xxxx.....

Samtidig ser norske sikkerhetsmyndigheter med bekymring på den økte aktiviteten fra utenlandske selskaper og stater som opererer i Norge. Mange av disse statene og private selskapene ønsker å skaffe seg tilgang til materiell som norske selskaper innen bransjen har utviklet og benytter i operasjoner. Russland er. soxxxxxx....

Kina kom i 2018 med xxxxxx hvor satsningsområdene ble beskrevet. Målet med satsningen er blant annet å få større tilgang til xxxx. xxxxxxxxxxxx

Både Russland og Kina har kapasitet til å skaffe til veie teknologi som er etterspurt ved bruk av ulovlige metoder. XXXKonkret bransjeeksempelXXX

Det er registrert større interesser fra utenlandske aktører rettet mot Norge og norske selskaper som besitter teknologi eller naturressurser som har strategisk betydning. Behovet for tilgang til teknologi trenger nødvendigvis ikke være knyttet opp mot XXX, men å benytte teknologien/materiellet til utvikling av våpen. Slike interessante er XXX osv...

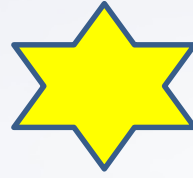
Forventet utvikling i trusselbildet

Det er få trekk i utviklingen som tyder på at interessen for høyteknologi og avansert materiell vil reduseres i fremtiden. XXXX.....etterspurt. Samtidig er det en økende sannsynlighet for at statlige eller private aktører forsøker å rekruttere personer som har kompetanse eller tilgang til utstyr som er ønsket.

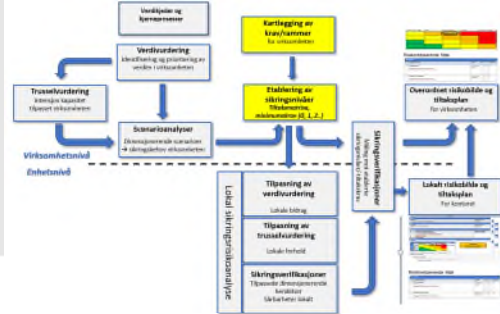
Tall fra politiet (Strasak) viser at det har vært en reduksjon XXXX

Mulige konsekvenser

Forsinkelse eller stans i produksjon som følge av at kritisk materiell blir tapt. XXX osv...



**Det enkle er det...
viktigste**



- Personkontroll som dekker forsyningskjeden
 - o Leverandører
 - o Egne ansatte
- Overvåking (kamera etc.)
- Kontrollrutiner/registrering
- Adgangsstyring – bare nødvendig
- Materiellkontroll – sjekkklister, tagging/sporing
- Adgangskontroll – inkludert gjerder, porter, vakthold osv. (soneinndelingen) – alarmer, lys
- Rutiner for transport (låsing, hensetting, vakthold/opsyn
- Sporing av transporten
- Leverandørstyring – spesifiserte krav

Med tanke på trusselbildet og kjente hendelser er det en usikkerhet knyttet til i hvilken grad selskaper varsler/anmelder tap av kritisk materiell videre da det kan peke på lite eller dårlig sikkerhetsfokus
XXXX...

Nr	Kategori	Tiltaksbeskrivelse	Kommentarer	Hensikt	M	T	O	Sikringsnivå	Referanse
FS01	Fysisk sikkerhet			Forhindre		X		1	
FS02	Fysisk sikkerhet			Forhindre		X		1	
FS06	Fysisk sikkerhet			Kontrollere			X	1	
FS07	Fysisk sikkerhet			Forebygge			X	1	
FS11	Fysisk sikkerhet			Oppdage		X		1	
FS13	Fysisk sikkerhet			Overvåke		X		1	
IS01	Informasjonssikkerhet			Forebygge			X	1	
PS01	Personellsikkerhet			Forebygge			X	1	
PS05	Personellsikkerhet			Overvåke			X	1	

Når Hendelse	Overvåke	Forebygge	Oppdage	Forhindre	Håndtere	Kontrollere
1	PS05, FS13, FS14, IS18	PS01, PS02, PS03, PS04, PS06, PS07, FS07, FS08, FS09, FS10 IS01, IS02, IS03, IS04, IS05, IS06, IS15, IS16, IS22, G1, G2, G3	FS11, FS12, FS15, IS17	FS01, FS02, FS03, FS04, FS05, IS07, IS08, IS09, IS10, IS11, IS12, IS13, IS14, IS21	IS19, IS20, G04	FS08
2		G05, G06, G07, G08, G09	G12, IS25 FS16, FS20, FS21, FS22	IS23, IS24, FS16, FS17	G10, G11	FS18
3		G14, G15, G16, G17, G18, G19, G20, FS23	IS26, FS25, FS26, FS27, FS29	G21, IS27, IS28, IS29, FS28	G22	G13, FS24

Nr	Tiltaksbeskrivelse	Kommentarer	Sikrings -nivå	Gjennomført I/N - begrunnelse/kompenserende hvis nei
FS01			1	
FS02			1	
O-G01			1	
O-G02			2	
O-IS05			1	
O-IS07			2	
O-PS01			1	
O-PS02			3	

Status NS 5830-32



- Revisjon
- Andre initiativer
- Ønsker innspill fra ulike bransjer og virksomheter

Tilbakemeldinger NS 583x eller spørsmål?



Anne-Kari Valdal
Telefon: 99004026
E-post: akv@proactima.com

proactima.com

Prepared.