



## Webinar onsdag 7 april 2021 «RAMS og sikring i et mer digitalisert jernbanesystem»

### **12:45 - 13:00 (0) MEET AND GREET**

*Bjørn Axel Gran, IFE og styreleder av ESRA*

### **13:00 - 13:10 (1) VELKOMMEN OG INFORMASJON OM ESRA**

*Bjørn Axel Gran, IFE og styreleder av ESRA*

### **13:10 - 13:20 (2) INFORMASJON OM TEKNA JERNBANE**

*Atle William Heskestad, Jernbanedirektoratet og styremedlem i Tekna Jernbane*

### **13:20 - 13:50 (3) Cyber securitys betydning for regelverk og godkjenning innen jernbane**

*Eivind Okstad, SINTEF Digital*

### **13:50 - 14:20 (4) Gir økt digitalisering på rullende materiell nye muligheter for optimalisering av vedlikehold?**

*Emil Hansen, Norske Tog AS og*

*Terje Nilsen, Vysus Group Norway (Tidligere Lloyds Register)*

### **14:20 - 14:50 (5) Simulering av RAM og togtrafikk - Et verktøy for beslutningsstøtte i jernbanen.**

*Stefan Isaksen, Safetec Nordic AS*

### **14:50 - 15:20 (6) Sporovervåkingsappen i Bane NOR**

*Kenneth Andersen, Bane NOR SF*

### **15:20 - 15:30 Oppsummering og avslutning**

*Bjørn Axel Gran, IFE og styreleder av ESRA*

Samarbeidspartner i



Fagnettverket Tekna Jernbane

## Har du forslag til et ESRA arrangement og / eller tema?

Bruk [«Forslagskassen til ESRA»](#).

Eller send en mail til [esra@tekna.no](mailto:esra@tekna.no)



**ESRA Norge**  
Norsk forening for risiko-  
og pålitelighetsanalyse



# Om ESRA Norge

08.09.2020

Tekna – Teknisk-naturvitenskapelig forening



## ESRA Norge – Norsk forening for risiko- og pålitelighetsanalyse

- Stiftet i 1994
- Norsk avdeling av ESRA - European Safety and Reliability Association (<http://www.esrahomepage.eu/>)
- Tilknyttet Tekna – Teknisk naturvitenskapelig forening (<https://www.tekna.no/>)

<https://esra.no/>

## «RAMS og sikring i et mer digitalisert jernbanesystem»

Webinar onsdag 7 april 2021 kl. 12:45 – 15:30. Sett av ettermiddagen til faglig påfyll innen skinnegående trafikk! De neste årene vil signalsystemene på både jernbanen og T-banen byttes ut med nye, digitale ... Les mer →

## «Er det bare flaks at det går bra?»

Webinar 9. februar 2021 kl. 13:00 – 15:00 Hvordan være best forberedt hvis hendelser inntreffer? Hvordan forbereder vi oss og hva er kritiske faktorer? Nyhetsbildet har den siste tiden vært preget av saker hvor ... Les mer →

En forening tilknyttet



## Nyhetsbrev

Meld deg på vårt nyhetsbrev for å få siste nytt fra foreningen.

➤ Abonner på nyhetsbrev

Støttebedrifter

# Formål

- **ESRA-Norge** skal holde en klar og avgrenset **faglig profil** med hovedvekt på analytiske metoder, anvendelser, verktøy og data i tilknytning til **risiko- og pålitelighetsanalyse**.

## Aktuelle aktiviteter:

- **Samle fagmiljøet** innen risiko- og pålitelighetsanalyse og styrke samarbeidet mellom fagpersoner innenfor industri, myndigheter, forskere, konsulenter, rådgivere m.v.
- **Arrangere møter og miniseminarer** som belyser ett eller et fåtall faglige temaer slik at det blir tid til fordypning.
- Informere medlemmene om:
  - "Nyheter", f.eks. gjennomførte utviklingsprosjekter, sentrale anvendelser m.v.
  - Møter, seminarer og konferanser.
  - Andre nyheter av interesse for medlemmene
- Samarbeide med andre beslektede faggrupper/foreninger i Norge og internasjonalt.

## Styret

- Bjørn Axel Gran, IFE (leder)
- Marie Saltkjel, Conoco Phillips (nestleder)
- Terje Dammen, Safetec Nordic AS
- Inge Alme, Alme Solutions AS
- Joar Dalheim, Vysus Group
- Kinga Wasilkiewicz Edwin, Sintef Digital
- Linn Ingrid Berggård, Bane NOR
- Marianne Fauskanger, Lilleaker Consulting AS
- Morten Bjerke, Tekna (Sekretær/Kontaktunkt)

# Medlemskap

<https://esra.no/bli-medlem/>

- Personlig medlem: 250 NOK
  - Student medlem: 0 NOK
  - Støttebedrift: 3000 NOK
- 
- Medlemskap i ESRA Norge gir ikke medlemskap i European Safety and Reliability Association (ESRA) eller omvendt



BANE NOR



ConocoPhillips



GLOBAL MARITIME



vår energi

SAFETEC



Vysus Group



FUTURE TECHNOLOGY



# Vi arrangerer seminar

10.03.2021

Webinar 9. februar 2021 – «Er det bare flaks at det går bra?»

09.12.2020

Webinar 9. desember 2020 – «Øker faren for storulykker i olje- og gassindustrien? Bør vi være bekymret nå?»

24.11.2020

Webinar 24. november 2020 – «Risikomodellering og kommunikasjon»

09.09.2020

Webinar 8. september 2020- «Erfaring etter større ulykker og hendelser samt høringsutkastet til revidert NS 5814»

09.09.2020

Årsmøtewebinar 26. mai 2020, tema: Erfaringer fra Hydrogeneksplosjonen i Sandvika juni 2019"

## Mange snakker om sikkerhet

Safety

«...Viktig å fokusere på sikkerhet...»

Security

«...Viktig å fokusere på sikkerhet...»



På ESRA seminarer utfordrer vi det offentlige, akademia og personer fra industrien til å dele på erfaringer og forventninger.



# Informasjon om Tekna Jernbane

Atle William Heskestad

**RAMS og sikring i et mer digitalisert jernbanesystem**  
ESRA webinar, onsdag 7. april 2021 kl. 12:45-15:30

1

## Informasjon om Tekna Jernbane

- Tekna Jernbane er ett av flere nettverk i Tekna
  - Styre som er bredt sammensatt av medlemmer fra **skinnegående sektor** (jernbane, trikk og T-bane)
  - I overkant av 1.000 medlemmer, som alle er interesserte i transportsystemet som **jernbane** er en del av
  - Et faglig fellesskap som jobber med kompetanse, samt politisk påvirkning
    - Partipolitisk uavhengig fagforening
    - Politikk som gagnar medlemmenes interesser
    - Forbereder høringsinnspill på Nasjonal transportplan 2022-2033 (NTP)
- Fordeler med å delta i Tekna Jernbane:**
- Dagsaktuelle tema identifiseres, fra overordnet til detaljert og spesifikt
  - Enkle og målrettede presentasjoner
    - Hva er viktig, og hvorfor dét er viktig
  - Runde rundt bordet: Synspunkter og meninger
    - (Forberedte innlegg)
  - Oppsummering og oppfølging

2

## Gjennomførte seminarer / webinarer

2020:

- Nullutslipp på ikke-elektrifiserte baner
- Bimodale tog
- Krav til informasjonsmodellering (KIM)
- Tekna Jernbane inviterer til gjennomgang av jernbanesektoren
- Tekna Jernbane presenterer sikkerhet i jernbanesektoren

2021:

- Tekna Jernbane presenterer banerådgiverens hverdag og RIFs blikk på jernbanens vedlikeholdsetterslep
- Årsmøte med fagmøte («Konkurransenutsetting av togdrift - Storbritannia»)

3



### Tekna Jernbane

Nettverket for Tekna medlemmer som engasjerer seg i jernbanens samfunnsmessige betydning som del av transportsystemet og jernbanetekniske problemstillinger.

#### Bli medlem i fagnettverket

Er du Tekna-medlem, er det gratis og uforpliktende å melde seg inn. Du får da e-post om relevante aktiviteter. Du kan også sende SMS med kodeord JERNBANE til 2007 for å bli medlem.

[Bli med i fagnettverket](#)

↓ Mer om nettverket

4

## Tekna Jernbane styre

Reza Sharkanloo	Bane NOR SF (Oslo)
Lars Grande	O.J. Dahl AS (Oslo)
Razieh Nejati Fard	Norske tog AS (Oslo)
Kristine Tveitan	Multiconsult AS (Oslo)
Øyvind Teodor Lavoll	Multiconsult AS (Oslo)
Kristoffer Bjornes	Sweco (Oslo)
Atle William Heskestad	Jernbanedirektoratet
Muzammil Navid Sheikh	Cowi AS
Dharun Arulthas	Sporveien AS
Kasserer	
Sigmund Sunde	Pensjonist Mantena AS, Trondheim



Tekna – Teknisk-naturvitenskapelig forening

// Side 5



SINTEF

# Cybersikkerhet og betydning for regelverk og godkjenning innen jernbane

ESRA-seminar, 7. mars 2021

Eivind Okstad, SINTEF Digital



(kilde: ENISA, 2020)



SINTEF

# Innhold

- Hvordan håndteres cybersikkerhet i Norsk jernbanesektor i dag?
- Er det mulige effekter på sikkerhet og effektivitet, og i hvilken grad fanges dette opp i dagens godkjenningsregime.
- Hva skjer fremover på området?
  
- *Merk: Cybertrusler endres i et raskere tempo enn rene sikkerhetstrusler.*



SINTEF

# Type trusler/trusselbilde vi tenker på

- **Utsiktet skade** i digitaliserte systemer i form av påført avbrudd, svikt eller funksjonsfeil. Hendelsene kan også være resultat av menneskelige feilhandlinger. Feil kan her gjøres av utviklere og testere ved innføring av nye systemer og software applikasjoner, eller av egne ansatte og brukere under drift/operasjon.
- **Tilsiktet skade** er trusler som inneholder cyberangrep og forsettlige aktiviteter, og/eller misbruk rettet mot jernbanesystemets eiendeler påført gjennom digitale systemer og kommunikasjonsplattformer.
  - Slik skade kan påvirke jernbanesystemets integritet og stabilitet, og derav også sikkerheten (*Safety*).
  - Det skilles på IT (adm. systemer) og OT (operative systemer) i regelverket. Denne presentasjonen fokuserer på OT.





SINTEF

# Litt om gjeldende regelverk

- **Jernbaneloven**

- Om godkjenningsordninger for planlegging/bygging av-, og tillatelser for å ta i bruk ny kjørevei og rullende materiell på Norsk jernbane.

- **EU-regelverk**

- Interoperability Directive 2016/797 (EU) -> Technical Specifications for Interoperability (TSI'er)
- Standardisering: Sikkerhet og RAMS (CENELEC), Cybersikkerhet og sikring (IEC 62433/ISO 27000-serien)

- I kraft av EØS-avtalen har dette bl.a. medført:

- Forskrift om samtrafikkvevnen i jernbanesystemet – *Samtrafikkforskriften* (om TSI'er - *Technical Specification Interoperability*)
- Forskrift om nasjonale tekniske krav m.m. for jernbaneinfrastruktur på det nasjonale jernbanenettet – *Jernbaneinfrastrukturforskriften*
- Forskrift om kjøretøy på jernbanenettet – *Kjøretøyforskriften*



SINTEF

# Sikkerhetsgodkjenning i Norsk jernbanesektor

- Sikkerhetsgodkjenning baseres på CENELEC standardene:
  - EN 50126-1/2:2017, EN 50128:2011, EN 50129:2018 og EN 50159:2010
- Cybersikkerhet er delvis omhandlet i EN 50129:2018 (sikkerhet ved signal- og kontrollsystemer) og EN 50159:2010 (sikkerhet ved kommunikasjon og transmisjon)
  - Krav ivaretar cybersikkerhet ved tilsiktede handlinger som kan påvirke sikkerhetsfunksjoner, eller ramme sikkerhetsrelatert utstyr.
- EN 50129:2018 krever at kvalitets- og sikkerhetsbevisene fra leverandører og jernbaneselskap samles i et toppdokument - "*Safety Case*".
  - Uavhengig sikkerhetsassessor (ISA)\* foretar vurdering av "*Safety Case*" og utgir egne rapporter som underlag for sikkerhetsgodkjenning.

(\*ISA er normalt utpekt av stedlig tilsynsmyndighet, dvs. Statens Jernbanetilsyn i Norge)



SINTEF

# Sentrale aktører og aktiviteter i EU

- **EU-kommisjonen**
  - *Directive (EU) 2016/797 on the interoperability of the rail system within the European Union*
  - *NIS-Directive on the security of network and information systems*
- **ERA** - European Union Agency for Railways
  - Informasjon, webinar: 2020-2021
  - TSI CCS in 2022 og 2025 med bl.a. *Generic cybersecurity architecture for coming products and rail automation systems*
- **ENISA** - European Union Agency for Network and Information Security
  - *ENISA Study Report (2020): Railway Cybersecurity - Security measures in the Railway Transport Sector.*
    - *Inneholder en spørreundersøkelse om håndtering av cybersikkerhet innen jernbanesektoren i EUs medlemsland som følge av NIS-Direktivet.*
    - *Status, og håndtering av cybersikkerhet (measures) innen ERTMS.*



SINTEF

# Utfordringer med cybersikkerhet i jernbanen

- Fra ENISA-rapporten (ENISA, 2020):
  - *Railway stakeholders must strike a balance between operational requirements, business competitiveness and cybersecurity, while the sector is undergoing digital transformation which increases the need for cybersecurity.*
  - *Railway stakeholders depend on suppliers with disparate technical standards and cybersecurity capabilities, especially for operational technology.*



SINTEF

# Håndtering av sikkerhet og cybersikkerhet (ERA, 2021)

- To **monitor** all activities related to cybersecurity in the railway context
  - Identify and promote adoption of native security features in **future radio communication and signaling systems**
- To cover safety requirements of the rail system, including the assessment of **safety consequences originated by security threats**
  - Security threats based on physical access to assets are outside of scope
  - Radio link inherent threats are considered
  - Safety AND Security Management Systems
- To reflect the above in the **EU railway regulation**
  - **TSIs** (TAF/TAP, OPE, CCS) : technical requirements to guarantee interoperability, e.g., increase the cyber robustness of ERTMS
  - **CSMs (Common Safety Method)**: process-oriented requirements to guide the acknowledgement of cybersecurity issues that might influence safety

# Relevante aktiviteter i EU som ERA nevner



## *TC9X - Working Group 26*

- *Draft Technical spec.: “Railway Applications – Cybersecurity” - prTS 50701 (2021)*
  - *Consistent approach to introduce requirements and recommendations for cybersecurity within the railway sector*



## *Technical Committee CYBER*

- *Technical Report: “Implementation of the NIS Directive”*
  - *Guidance on considerations for incident notification; best practices in cyber security risk management*



## *IP2 - Technical Demonstrator 2.11*

- *Definition of a security by design system, dedicated to railways (e.g., Protection Profiles Specification)*
  - *Application of the methodology to railways (demonstrator)*



SINTEF

## Cybersikkerhet aksept iht. prTS 50701 (TC9X-WG26)

- *prTS 50701: Railway applications – Cybersecurity (final draft, January 2021)*

*Purpose: "..when a railway system is compliant to TS 50701, it can be demonstrated that this system is at the state of the art in terms of cybersecurity, that it fulfils its targeted Security Level (SL-T) and that its security is maintained during its operation and maintenance".*

*TS 50701 applies to Communications, Signalling and Processing domain, to Rolling Stock and to Fixed Installations domains.*

- prTS 50701 gir veiledning og spesifikasjoner for hvordan cybersikkerhet skal håndteres i sammenheng med EN 50126-1, RAMS – livssyklusfasene.
- Endelig versjon TS 50701 planlegges utgitt juni 2021. Mulig EN 50701 innen 2-3 år.



SINTEF

# Intensjon med prTS 50701

- Skal være kompatibel og i samsvar med EN 50126-1 når den brukes på "*System under Consideration*" (*SuC*), som er en systembetegnelse/inndeling hentet fra IEC 62443.
- Skal skille prosessene med sikkerhetsgodkjenning og cybersikkerhets-aksept så mye som mulig fordi det er forskjell i hvordan sikkerhet og cybersikkerhet håndteres gjennom prosjektets faser.
- Identifiserer nødvendige synkroniseringstrinn (aktiviteter og leveranser) relatert til cybersikkerhet mellom systemintegrator (selskap som setter sammen delsystemer til en helhet) og eier av infrastrukturen eller rullende materiell.

*Cyber security in context of prTS 50701 is to protect the railway systems' essential functions, where safety is one of them, in case they are threatened by malicious cyber attackers.*





SINTEF

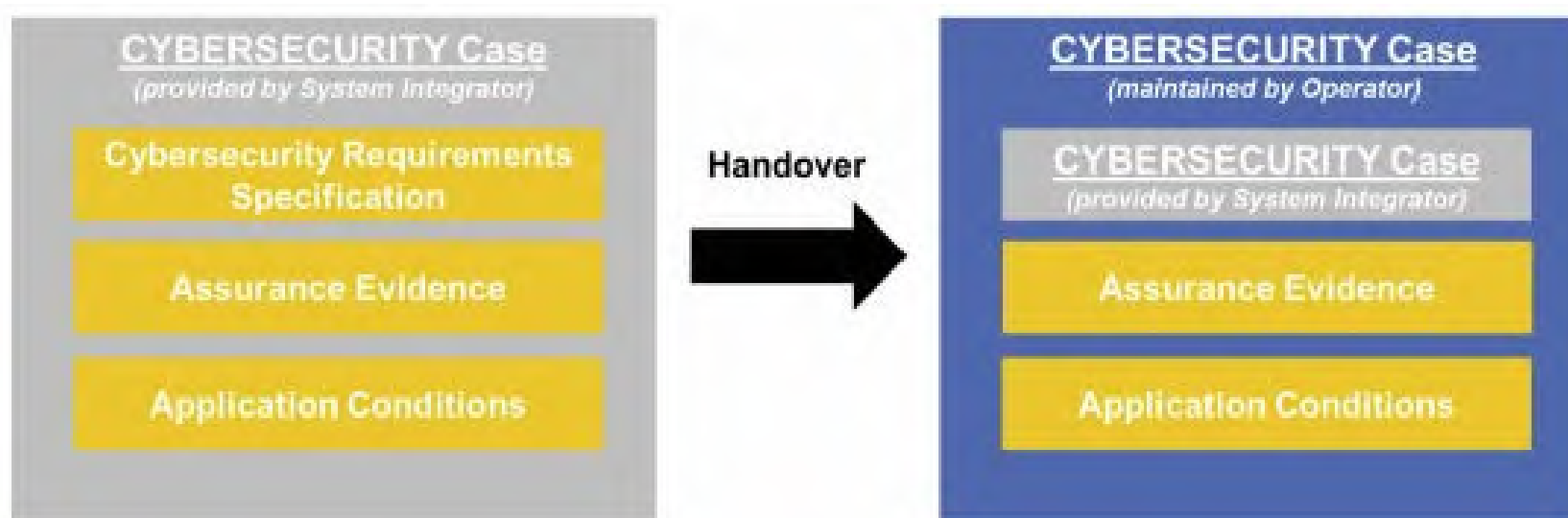
# Mål for cybersikkerhet

- Forslag i prTS 50701 er å definere et begrenset antall koordinerte cybersikkerhetsmål (og på et høyt nivå) som skal implementeres med *Cybersecurity Case*.
  - Ønsket med dette er å oppnå nødvendig nivå for separasjon og koordinering mellom RAMS- og cybersikkerhets-prosessene.



SINTEF

# Cybersecurity Case



(kilde: prTS 50701)

- Cybersecurity Case fra systemintegrator oppdateres når SuC er validert for den tiltenkte bruken. Når dette foreligger godtar operatør/infrastruktureier den oppdaterte Cybersecurity Case under SuC "Handover" som illustrert i figuren.
  - Merk: Med Cybersecurity Case følger "Security Related Application Conditions" (SecRAC), noe tilsvarende (SRAC) for Safety.



SINTEF

# Drift og vedlikehold

- prTS 50701 gir råd for kontinuerlig vurdering og administrasjon av sårbarheter og håndtering av software oppdateringer, eller "patcher". Sikkerhetsoppdateringer som påvirker sikkerhetsfunksjonene skal koordineres med sikkerhetsstyringen.
- Det er kunngjort at senere versjoner av TS 50701 vil innbefatte aktiviteter som overvåking av cybertrusler, håndtering av hendelser og sikring av virksomheten i krisesituasjoner.



SINTEF

# *Safety and Security (prTS 50701, Appendix D)*

- *Complementary goals: safety mainly seeks to protect people or the environment from malfunctions of automation systems, while security aims to protect the technical systems from attacks from the environment.*
- *Eight management principles follows:*
  1. *Safety and security are different and should be treated as such.*
  2. *The security environment should protect "essential functions", including safety as one of them.*
  3. *Cybersecurity Threat and Risk Analysis is the main interface with the Safety Analysis.*
  4. *Separate security and safety as far as possible but coordinate them effectively.*
  5. *Security should be evaluated on the basis of international standards, e.g. IEC 62443.*
  6. *It is infeasible to evaluate the Security Risk probabilistically.*
  7. *Safety and Security Target measures should not be coupled.*
  8. *Security is a collaborative continuous effort.*



SINTEF

Teknologi for et  
bedre samfunn