RAMS in the Railway sector, including assessment

Delimited to signalling systems

RAMS 2016-11-18

Venue: VG 11 (ground floor), Valgrinda, S.P. Andersens veg 5, Department of Production and Quality Engineering, NTNU

Thor Myklebust

Thor.myklebust@sintef.no

https://no.linkedin.com/in/thormyklebust

SINTEF ICT

Topics

- SINTEF groups: Functional safety & System safety
- Signalling projects in Norway
- EN 50126 the RAMS standard
  - Safety Case and The Agile Safety Case
- Roles
- Kick off meeting
- Different assessor roles
- Duty to provide guidance
- Assessor tasks

Competence and services

- Research, innovation and development
- SafeScrum
- SW process
- Certification
- Pre-assessment
- Analysis
- FMEDA (Failure Mode Effect Diagnostic Analysis)
- Training, courses and workshops
- Embedded HW/SW development
- RAMS (Reliability Availability Maintainability Safety)
- Safety Case

1. **IEC 61508 Generic safety standard Committee Member**
2. ISO 26262 series Automotive domain
3. ISO 13849-1 Machinery
4. IEC 62061 Machines
5. IEC 60601 Medical
6. IEC 61511 series Process industry
7. IEC 60880 and IEC 61513 Nuclear industry
8. DO 178C Avionics
9. MIL STD 882E Military standard
10. IEC 60730 White goods
11. IEC 60335 White goods
12. IEC 61800-5-2 Adjustable speed electrical power drive systems
13. EN 5012x series Railway domain
14. EN 50495 Safety devices ….. explosion risks
15. EN 50402 Fixed gas detection
16. IEC 50156 Furnaces

SINTEF: general information

- Technical evaluations of CCS systems since 1975

- ISA projects since 1994
- Appointed as NoBo in 2003
- CSM assessment body since 2012
  - Accredited 2016
- DeBo in Finland since 2015
- DeBo in Norway since 2016

- Participate actively in NB-Rail
  - Plenary meetings (3X/year)
  - ERTMS sub group meetings (3X/year)
  - Issue “ERTMS sub group User guide”

Books to be issued by Springer

SafeScrum 2017

SafeScrum

The Agile Safety Case 2017

Research project

Supported by:

- Sporveien
- Jernbaneverket
- Budget 2017: Transportstyrelsen

Signalling projects in Norway

Copy from Jernbaneverket:

The whole Norwegian railway network will be in service with ERTMS by 2030.

The speed of the rollout is aligned with the financing given in the National Transportation Plan 2014-2023.

GSM-R has been in service on the complete network from 2007.

The total cost of the Norwegian ERTMS implementation is estimated to be between 1,7 and 2,2 billion Euros.

CBTC in Oslo:

Sporveien expects funds for the project to be available from 2017 and intends to sign a contract in 2017.

RAMS standard EN 50126

EN 50126-1:1999 Railway applications – The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

Example: Maintainability

- In phase 11 "operation and maintenance" EN 50126-1 edition it is required that "Operation and Maintenance Procedures including all the relevant information for providing spare parts, particularly safety related items, shall be produced within this phase."

RAMS standard EN 50126

6.4 Phase 4: System requirements

c) maintainability, including:

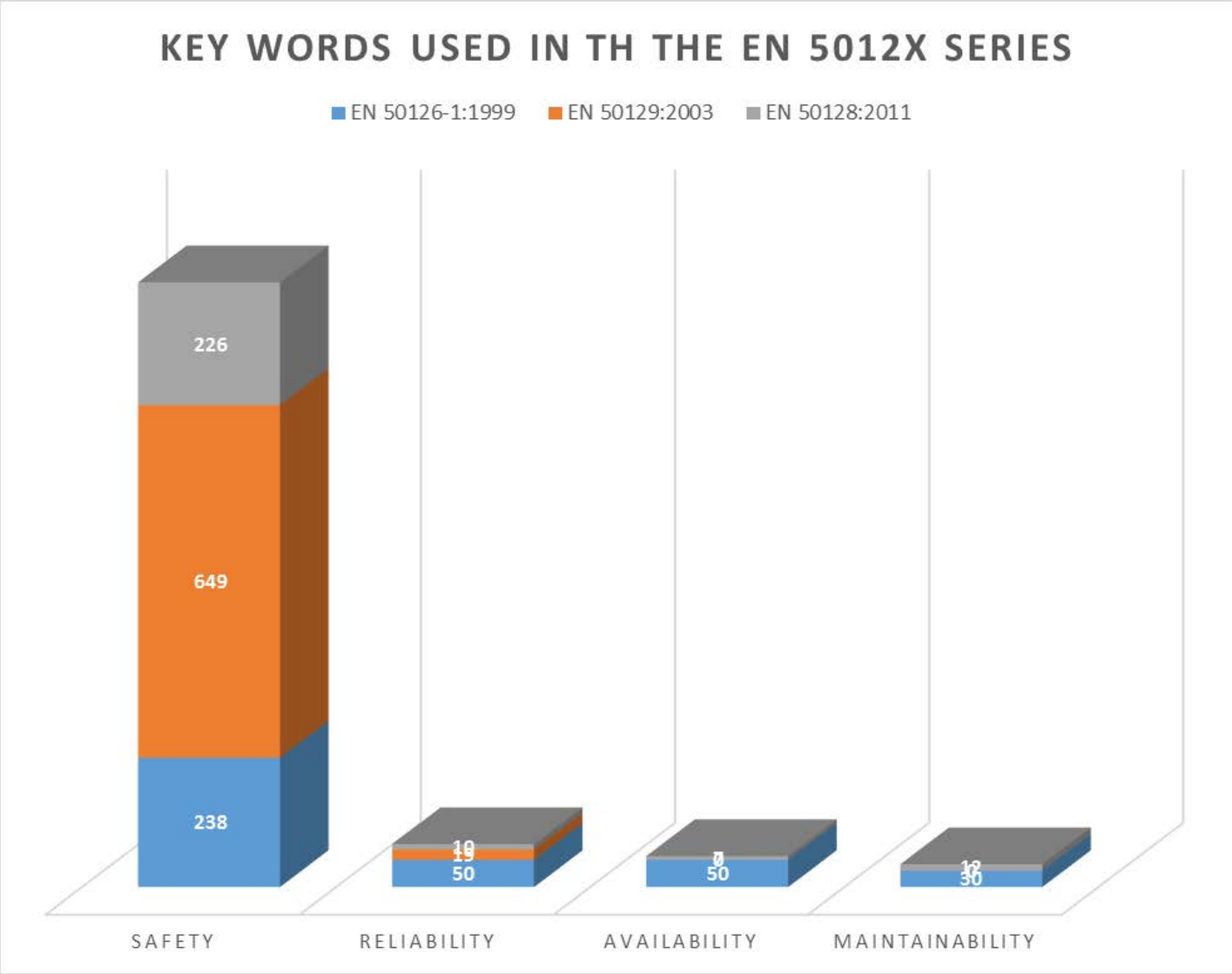
- maintainability analysis and prediction, including:
- maintainability analysis and verification;
- maintenance task analysis;
- ease-of-maintenance studies and testing;
- human factors maintainability considerations.

maintainability planning, including:

- maintainability design review programme;
- establishment of the maintenance strategy;
- review of reliability centred maintenance options;
- software maintenance programme.

No requirements are given for the content of the procedures in the standards

EN 5012X series



EN 50126-1:1999 and Reliability

reliability: The probability that an item can perform a required function under given conditions for a given time interval (t1, t2)

reliability growth: A condition characterised by a progressive improvement of a reliability performance measure of an item with time

EN 50126-1:1999 and Reliability

6.4 Phase 4: System requirements

reliability analysis and prediction, including:
- functional analysis and system failure definition;
- top down analysis, for example fault tree analysis and block diagram analysis;
- bottom up analysis, for example Failure Modes Effects Analysis (FMEA);
- common cause failure or multiple failure analysis;
- sensitivity analysis and trade-off studies;
- reliability apportionment;
- human machine interface analysis;
- stress analysis;
- worst case prediction and tolerance analysis

reliability planning, including:
- reliability design review programme;
- component reliability assurance programme;
- software quality/reliability assurance programme.

reliability testing, including:
- reliability growth testing, based on failure generation;
- reliability demonstration testing, based on expected failure modes;
- environmental stress screening;
- life testing of components;
- system life testing during early operation.
- reliability data acquisition and assessment;
- data analysis for reliability improvement

Safety Case

Railway EN 50126-1:1999 safety case:

The documented demonstration that the product complies with the specified safety requirements

Automotive ISO 26262-1:2011 safety case

Argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development

The contents of a safety case

- The safety case shall contain documentary evidence of quality management, safety management and functional and technical safety.
- Its structure:
  - *Definition of system*
  - *Quality management report*
  - *Safety management report*
  - *Technical safety report*
  - *Related safety cases*
  - *Conclusion*

Definition of System

- shall contain
  - *an overview of the system*
    - the product structure
    - interfaces (internal, external)
  - issue/revision resp. version data for all relevant
    - documents
    - sub-systems/products

Quality Management Report

- shall describe (or reference)
  - the quality requirements
  - the quality management system
  - ***a summary of the quality controls***
    - what you planned to do
    - what you actually did
  - what evidence you have e.g.
    - quality audit reports
    - minutes of meetings
    - procedures etc.
    - signatures on documents, drawings ...

Safety Management Report

- shall describe (or reference)
  - ***the safety requirements***
  - the safety management system
  - ***a summary of the safety controls***
    - what you planned to do
    - what you actually did
  - what evidence you have e.g.
    - ***safety assessment and safety audit tasks***
    - risk analyses
    - procedures etc.
    - hazard log

Technical Safety Report

- How did you achieve safety
  - *safety engineering techniques employed within the system*
- What did you achieve
  - technical properties, evidence (test results etc.)
- Structure of the report:
  - *Introduction*
  - *Assurance of correct functional operation*
  - *Effects of faults*
  - *Operation with external influences*
  - *Safety related application conditions*
  - *Safety qualification tests*

Related Safety Cases

- Hierarchy of system/subsystem/equipment...
  - "parts" or "components" of a more complex system
- Safety cases of those parts, components etc.
  - certificates, licenses, ...
- ***summary of any limitations and constraints***
  - = ***Safety related application conditions***
  - "we guarantee safety, provided that ..."
    - from the related safety cases
    - REPEAT THEM! Don't just make a reference.

The Conclusion

This shall summarise the

- **evidence presented in the previous parts of the Safety Case,**
- **argue that the relevant system/subsystem/equipment is adequately safe**

subject to compliance with the specified application conditions.

The Agile Safety Case

Purpose of a Safety Case:

The purpose of a Safety Case is to develop structured arguments supported by evidence, intended to justify that a product or system is acceptably safe for a specific application in a specific operating environment

Purpose of "The Agile Safety Case" (TASC): As the SC above but also including: Adaptability, flexibility and effective solutions

The TASC are developed alongside the product development

It is efficient to build the safety case by inserting information when it becomes available – an agile approach also resulting in increased safety awareness and understanding

The Agile Safety Case

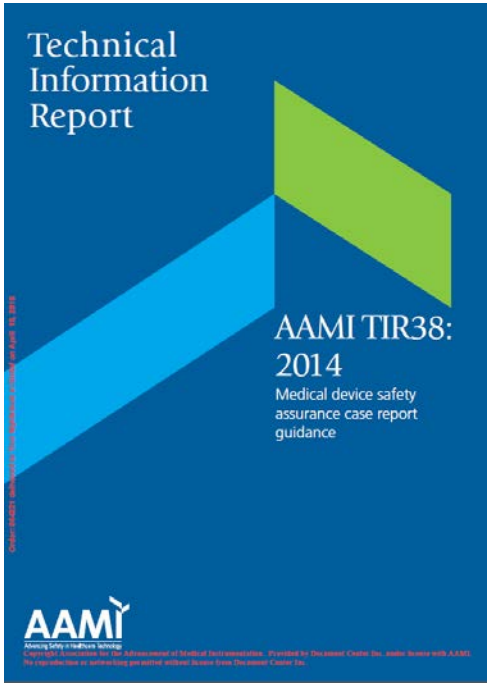
SC and domains

- EN 50129 Railway standard includes several requirements for a SC

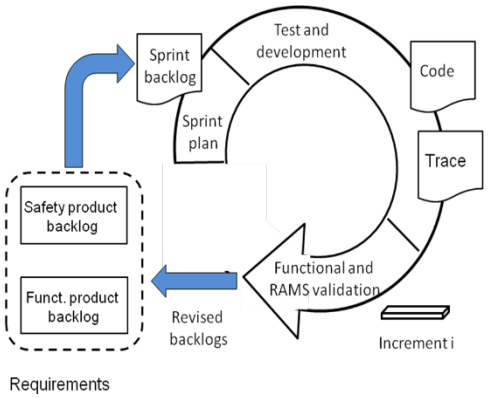
These standards includes requirements for a SC

- ISO 26262 automotive
- Def. 00-55 defence
- DO-178C avionics

- Discussions are being made to include SC requirements in IEC 61508 ed.3 Generic standard



From last Sprint to the Safety authority



Finished product

Independent tests

SC Author

Analysis Inspections

TASC

SAR

Communication between SC author and the assessor

SAR: Safety assessment report

Domain dependent

Safety authority

Assessors

- NoBo: Notified Body - Teknisk Kontrollorgan
- ABo: Assessment Body - Assesserende enhet
- DeBo: Designated Body - Utpekt organ
- ISA: Independent Safety Assessor - Uavhengig sikkerhets bedømmer

Assessor

EN 50126:1999 Definition of assessment: The undertaking of an investigation in order to arrive at a judgement, based on evidence, of the suitability of a product

EN 50129:2003 Definition of assessment

the process of analysis to determine whether the design authority and the validator have achieved a product that meets the specified requirements and to form a judgement as to whether the product is fit for its intended purpose

Tasks, the key tasks are:

- Acquiring an appreciation of the scope and context of the assessment
- Selecting and planning a cost-effective assessment strategy
- Gathering relevant evidence
- Forming a judgement
- Managing any outcomes

Different assessor roles and appointment

- Independent Safety Assessor, ISA according to the CENELEC standards EN 5012X
  - Accepted by the Norwegian Railway Authority for each project
  - CVs evaluated
- Assessment Body (Commission regulation)
  - Latest issue of the regulation (1136/2015) came into force august 2015
- NoBo Assessor (Directive 2008/57/EC)
  - Appointed organisation
- DeBo Assessor (EC Directive 2008/57/EC, article 17(3))
  - Appointed organisation

Assessor

Duty to provide guidance (copy from the appointment of SINTEF as NoBo)

In compliance with the Administration Act's §11

- a NoBo has a general duty to provide guidance

E.g. SINTEF ICT shall through its guidance point out

- possible faults or
- shortcomings of a product

so that the manufacturer can bring the product into line with the requirements from regulations.

It is however the manufacturer's responsibility to find the actual technical solutions.

ISA (CENELEC)

- Independent Safety Assessor
- National Safety Authority
  ISA organisation
- The ISA base the work on the CENELEC standards
  - EN 50126: RAMS
  - EN 50128: Software
  - EN 50129: Hardware and Safety Case
  - EN 50159:2010 Communication

Foto: San Francisco international airport

Assessor)

What we do

- Preliminary meeting
- Kick off meeting
- Scrutiny of documents
- Provide guidance
- Safety meetings
- Technical meetings
- Audits
- Witness testing
- On-site inspection of systems

Deliverables

- ISA plan
- Audit reports
- Safety Assessment Reports

ISA (CENELEC)

Kick off meeting

- Scope
- Involved parties
  - Responsibilities
- Safety plan
- GPSC, GASC and SASC
  - Schedule, document flow and deliverables
  - References
- SW development
- Language, SIL etc

Assessor (CENELEC, CSM and NoBo)

Scrutiny of documents (1 av 3)

- Prosedyre "SJS Granskingsprosedyre"
  - Kopi fra prosedyren:

- En gransking av dokumenter har til hensikt å vurdere om dokumentene oppfyller visse krav som er stilt i
  - standarder,
  - forskrifter
  - regelverk.
- Derfor må dokumentene som skal vurderes identifiseres nøyaktig.
- Kravene som dokumentene skal vurderes mot må også identifiseres, enten gjennom eksplisitt oppføring eller gjennom en referanse til et annet dokument som inneholder kriteriene (f.eks. en sjekkliste). I begge tilfeller må kravene kunne identifiseres f.eks. med et nummer, slik at referanser til enkelte krav kan gis.

Assessor (CENELEC, CSM and NoBo)

Scrutiny of documents (2 av 3)

- Metoden som blir brukt for å avgjøre om kravene er oppfylt kan være f.eks. grundig gjennomlesing, analyse, sammenligning med tidligere versjoner, sjekkliste...

- Resultatet av granskingen er en skriftlig redegjørelse for om kravene er oppfylt eller ikke. Dersom et krav ikke er oppfylt, bør de nødvendige endringer i dokumentet for å oppfylle kravet skisseres og forventet frist (dato eller utgave av oppdatert dokument) angis.

LooP template forteller om hvilke Funn-typer man kan bruke

Assessor (CENELEC, CSM and NoBo)

Scrutiny of documents (3 av 3): LooP (List Of Open Points)

Category	Classification level	Description
A	Major	A safety/interoperability related deviation to the standards which was found in the Design, and which probably will cause a project change.
B	Minor	A safety/interoperability related deviation to the standards which was found in the Documentation and has probably no impact on Design. This will lead to a new revision of the inspected document.
C	Marginal	A deviation to the standards which was found in the Documentation, which do not lead to a document or design change. A new revision is not necessary.
D	Formal	A formal deviation to the standards which was found in the Documentation, which do not lead to a document or design change. A new revision is not necessary.

NoBo/Teknisk kontrollorgan

The appointment of SINTEF was done by the:

Norwegian Ministry of Transport and Communications.

SINTEF is Notified Body #1278

NB-Rail

Topics:

- Common application
- Common practice
- Explanation
- Interpretation
- Guides (together with ERA)

Internet page: http://nb-rail.eu/home_en.html

Assessment Body

What we do

- Scrutiny of documents related to changes
  - Definition of the system
  - Risk/hazards (risk management process, safety relevant information)
  - Evidence from the risk management process
- Safety meetings

Significant changes (Article 4, CSM)
If there is no notified national rule for defining whether a change is significant or not in a Member State, the proposer shall consider the potential impact of the change in question on the safety of the railway system.

Deliverables

- CSM assessor plan
- Safety Assessment Reports

Assessment Body

Annex I

the risk assessment process, which shall identify

- the hazards,
- the risks,
- the associated safety measures and
- the resulting safety requirements

to be fulfilled by the system under assessment

Assessment Body

Accredited 2016

NORSK AKKREDITERING

Norsk akkreditering

Stiftelsen SINTEF
SINTEF IKT – Systemutvikling og sikkerhet
Strindveien 4
7034 Trondheim

Att: Narve Lyngbø

Deres ref./Your ref. | Vår ref./Our ref. PBH/15/0379 | Dato/Date 16.09.16

Vedtak om akkreditering

Norsk akkreditering har vedtatt at INSP 059 Stiftelsen Sintef er akkreditert etter NS EN ISO 17020 som beskrevet i vedlagt akkrediteringsomfang, med virkning fra 16.09.16. Vedtaket er gjort med hjemmel i Lov om det frie varebytte i Europa (EØS-vareloven) av 14.4.2013, kapittel II, art 5.1.

Vedtaket innebærer at Norsk akkreditering har funnet at organisasjonen oppfyller kravene til akkreditering, jf. Vilkår for å være akkreditert (NA Dok. 25/31).

Nytt akkrediteringsomfang for INSP 059 Stiftelsen Sintef etter NS EN ISO 17020 er tilgjengelig på Norsk akkrediterings nettsider www.akkreditert.no.

Akkrediteringen forutsetter regelmessig oppfølging og er gyldig til 16.09.21. Gyldigheten av akkrediteringen forutsetter at organisasjonen oppfyller alle vilkår for å være akkreditert kontinuerlig frem til akkrediteringen utløper.

Vedtak om akkreditering kan påklages innen 3 uker etter at vedtaket er kommet frem, jf. Lov om behandlingsmåten i forvaltningssaker av 10. februar 1967 (forvaltningsloven) § 29, jf. forvaltningsloven § 28. Klage på vedtak om akkreditering behandles av Norsk akkrediterings klageutvalg, i henhold til Lov om det frie varebytte i EØS (EØS-vareloven) av 14.04.2013 § 3 andre ledd. Klager sendes Norsk akkreditering.

Med vennlig hilsen

Pia Backe-Hansen
Sjefingeniør
Norsk akkreditering

Inger Cecilie Laake
Avdelingsdirektør
Norsk akkreditering

Norsk akkreditering
Postboks 155
Lillestrøm bedriftssenter
2001 Lillestrøm
Norge

Tlf.: (+47) 64 84 86 00
E-post: akkreditert@akkreditert.no
Web: www.akkreditert.no

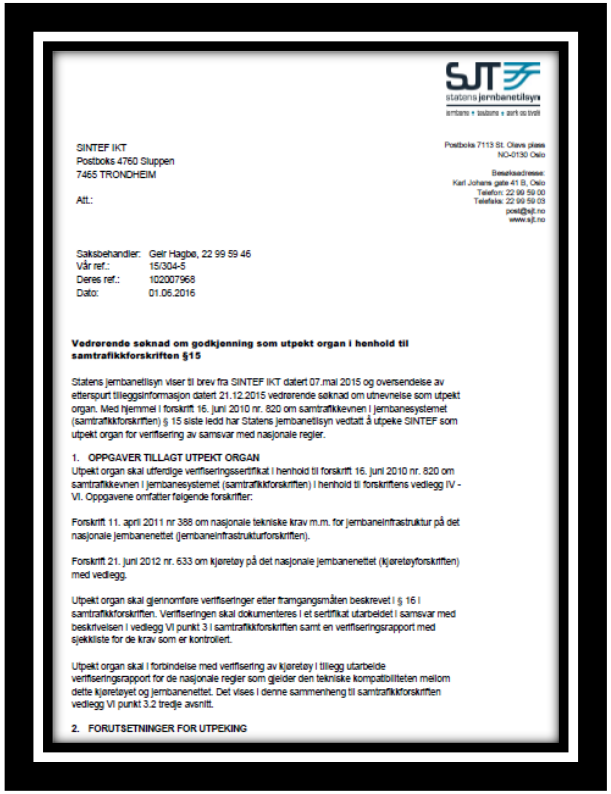
Bank: 7694 05 10763
Navn: DnB
Swift: DNBANOKK
IBAN: NO19 7694 05 10763

Norsk akkreditering / Norwegian Accreditation | Sign.: ICL | Dok.ID: 000508 | Ver.: 1.06 / 20.07.2016 | Side./Page: 1| 2|

DeBo

SINTEF has been appointed Designated Body 2016

DeBo evaluates the national requirements



SJT
statens jernbanetilsyn

SINTEF IKT
Postboks 4760 Sluppen
7465 TRONDHEIM

Att.:

Postboks 7113 St. Olavs plass
NO-0130 Oslo

Besøksadresse:
Karl Johans gate 41 B, Oslo
Telefon: 22 99 59 00
Telefaks: 22 99 59 03
post@sjt.no
www.sjt.no

Saksbehandler: Geir Hagbø, 22 99 59 46
Vår ref.: 15/304-5
Deres ref.: 102007968
Dato: 01.06.2016

Vedrørende søknad om godkjenning som utpekt organ i henhold til samtrafikkforskriften §15

Statens jernbanetilsyn viser til brev fra SINTEF IKT datert 07.mai 2015 og oversendelse av etterspurt tilleggsinformasjon datert 21.12.2015 vedrørende søknad om utnevnelse som utpekt organ. Med hjemmel i forskrift 16. juni 2010 nr. 820 om samtrafikkevnen i jernbanesystemet (samtrafikkforskriften) § 15 siste ledd har Statens jernbanetilsyn vedtatt å utpeke SINTEF som utpekt organ for verifisering av samsvar med nasjonale regler.

1. OPPGAVER TILLAGT UTPEKT ORGAN

Utpekt organ skal utferdige verifiseringssertifikat i henhold til forskrift 16. juni 2010 nr. 820 om samtrafikkevnen i jernbanesystemet (samtrafikkforskriften) i henhold til forskriftens vedlegg IV - VI. Oppgavene omfatter følgende forskrifter:

Forskrift 11. april 2011 nr 388 om nasjonale tekniske krav m.m. for jernbaneinfrastruktur på det nasjonale jernbanenettet (jernbaneinfrastrukturforskriften).

Forskrift 21. juni 2012 nr. 633 om kjøretøy på det nasjonale jernbanenettet (kjøretøyforskriften) med vedlegg.

Utpekt organ skal gjennomføre verifiseringer etter framgangsmåten beskrevet i § 16 i samtrafikkforskriften. Verifiseringen skal dokumenteres i et sertifikat utarbeidet i samsvar med beskrivelsen i vedlegg VI punkt 3 i samtrafikkforskriften samt en verifiseringsrapport med sjekkliste for de krav som er kontrollert.

Utpekt organ skal i forbindelse med verifisering av kjøretøy i tillegg utarbeide verifiseringsrapport for de nasjonale regler som gjelder den tekniske kompatibiliteten mellom dette kjøretøyet og jernbanenettet. Det vises i denne sammenheng til samtrafikkforskriften vedlegg VI punkt 3.2 tredje avsnitt.

2. FORUTSETNINGER FOR UTPEKING

Questions?

thor.myklebust@sintef.no
https://no.linkedin.com/in/thormyklebust
www.researchgate.net/profile/Thor_Myklebust

www.sintef.no/IEC61508 (Research, Certification and Consultancy)
www.sintef.no/sjs (Railway)
www.safescrum.no (Software development)