

Safety en Compliance Plan

ERTMS Noordelijke Lijnen



Lijst met aanpassingen

Versie	Datum	Beschrijving van de wijziging	Herzien	Vrijgegeven door
Nul	23 feb 2023	Nulversie, voor commentaar	Krijn Rabouw	
P01.02	9 mei 2023	Commentaar verwerkt in eerste volledige concept	Krijn Rabouw	
P01.03	22-05-2023	Review en modereren van review verwerking	Jaap Ton	
P01.04	24 mei 2023	Resterend commentaar verwerkt	Krijn Rabouw	
P01.05	24-05-2023	Wijzigingen geaccepteerd	Jaap Ton	
P01	24 mei 2023	Vrijgave		Michiel Blaauboer

Sweco Nederland B.V.

Onderwerp

Projectnummer

Klant

Auteur

Datum

Document referentie

30129769

ROVK Treinbeveiliging ERTMS

51006352

ProRail B.V.

Krijn Rabouw

24-05-2023

51006352-SWECO-RHSF-XX-MS-ZS-00001

ProRail projectnummer

ProRail document referentie

D-003122

ENL_9.1_Sw_01_001

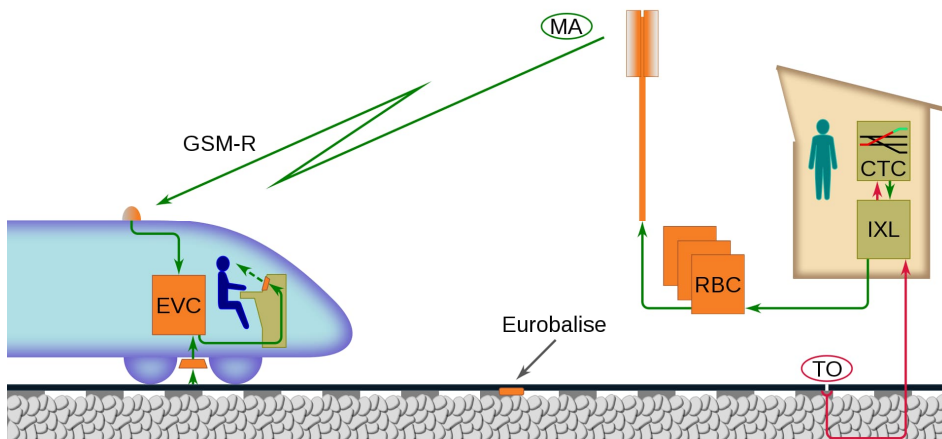
Inhoudsopgave

1	Inleiding	5
1.1	Doel	6
1.2	Afbakening	7
1.2.1	Specifieke Applicaties	7
1.2.2	Fasen van de levenscyclus.....	7
1.2.3	Subsystemen	8
1.2.4	Generieke Applicatie	8
1.3	Voorbehoud	9
1.4	Relatie met andere plannen	9
1.5	Structuur van dit plan	9
1.6	Gebruikte afkortingen	10
2	Systeem en context	12
2.1	Generieke Applicatie	12
2.2	Specifieke Applicaties	12
2.3	Wettelijke context	13
2.4	Stakeholders	14
2.4.1	Context.....	14
2.5	Levenscycli	16
3	Strategie	19
4	Kwaliteitsmanagement	20
4.1	Ontwerpen met IMX data	20
4.2	Verificatie.....	21
4.3	Validatie.....	22
4.3.1	Validatie tegen klanteisen.....	22
5	Veiligheidsorganisatie	23
5.1	Interne veiligheidsorganisatie.....	23
5.1.1	Project Management.....	23
5.1.2	Designers	24
5.1.3	Verifiers.....	25
5.1.4	Validator	25
5.2	Externe veiligheidsorganisatie	25
5.2.1	Safety tafel	25
5.2.2	Raakvlakken	25
5.2.3	Independent assessor	25
5.2.4	Vergunningen.....	26
5.2.5	Toestemming voor gebruik	26
6	Activiteiten en producten	27

6.1	Specifieke Applicaties	27
6.2	Configuratiedata	29
6.3	Systeemdefinitie	30
6.4	Risicomanagement	30
6.5	(Sub) System Requirements Specifications	30
6.6	Systeemontwerp	31
6.7	Specific Application Safety Cases	31
6.7.1	Structuur van de Safety Cases	31
6.7.2	Iteraties van de SASC	33
6.7.3	Safety Argument	33
6.7.4	Verband met de GASC	34
6.7.5	Verband met andere SASCs	34
6.8	Application Preparation Plan	35
6.9	Tools	35
6.10	Decommissioning bestaande systemen	35
7	Hazard management	36
7.1	Wat is een hazard?	37
7.2	Hazard identificatie	37
7.2.1	Oorzaken en gevolgen	38
7.3	Hazard classificatie	38
7.4	Algemeen aanvaarbare risico's	39
7.5	Risicoaanvaardingsbeginselen	39
7.6	Risico evaluatie	40
7.7	Hazard Log	40
7.8	Safety audits	40
7.9	Independent Safety Assessment	41
8	Compliance management	42
8.1	TSI compliance	42
8.2	EG Verificatie door een NoBo	43
8.3	TSI compliance dossier	46
8.4	Technisch Dossier	47
	Referenties	49
	Bijlage 1 – Van toepassing zijnde TSI's	51
	Bijlage 2 – Uitgangspunten	53
	Bijlage 3 – Risicomatrix	55
	Bijlage 4 – Audit programma	56
	Bijlage 5 – Checklist eisen safety plan	57

1 Inleiding

ProRail vervangt de komende jaren het huidige treinbeveiligingssysteem ATB door het European Train Control System (ETCS) van de fabrikant Thales. Als consequentie daarvan moeten vele andere systemen ook aangepast of vervangen worden, zoals de treindetectie, interlocking, object controllers voor wissels en overwegen, het verkeersleidingsysteem (Post21) en bijbehorende voedings- en communicatiesystemen. De huidige lichtseinen worden daarna verwijderd.



Figuur 1 - De basiselementen van ERTMS (bron: Wikipedia)

ETCS is een onderdeel van het European Rail Traffic Management System (ERTMS). Een ander onderdeel van ERTMS is GSM-R, dat is het draadloze communicatienetwerk dat gebruikt wordt voor de data communicatie tussen een "Radio Block Centre" (RBC) en de ETCS treinapparatuur (o.a. de EVC). En ook voor de spraakcommunicatie tussen machinist en verkeersleiding. In het dagelijks spraakgebruik wordt de term "ERTMS" gebruikt voor het totale besturings- en seingevingssysteem (Control-Command and Signalling).

Het eerste vervangingsproject is nu *ERTMS Noordelijke Lijnen* (ENL). Dit project bestaat uit 7 percelen in Groningen en Friesland, waaraan door 3 ingenieursbureaus (IB's; Arcadis, Nexus en Sweco) wordt gewerkt.

Sweco werkt aan 3 percelen:

4. Groningen – Eemshaven / Delfzijl;
5. Groningen – Bad Nieuweschans (Duitse grens) / Veendam;
6. Emplacement Groningen.



De andere percelen van ENL zijn:

- Harlingen Haven – Leeuwarden (perceel 1 - Arcadis);
- Stavoren – Leeuwarden (perceel 2 - Nexus);
- Leeuwarden – Groningen (perceel 3 - Nexus);
- Emplacement Leeuwarden (perceel 7 - Arcadis).

De eerste lijn waarop volgens de huidige planning ERTMS wordt geïnstalleerd, de *Early Deployment Lijn*, is de lijn Leeuwarden – Harlingen Haven.

Tegelijkertijd met ENL lopen er nog drie projecten: ERTMS Kijfhoek – Belgische grens (EKB), ERTMS Hanzelijn (EHL) en ERTMS Schiphol – Amsterdam – Almere – Lelystad (ESAAL). De IB's werken nauw samen in twee Kennis Allianties om ervaring op te doen met ERTMS en om tot een gelijke werkwijze te komen. Doel hiervan is ook om te komen tot "open engineering", zodat ProRail verschillende IB's kan inschakelen in plaats van afhankelijk te zijn van de ontwerpdiensten van 1 fabrikant. In de Kennis Alliantie ENL/EHL/ESAAL werken 5 IB's samen (Arcadis, Movares, Nexus, Royal Haskoning DHV en Sweco); in de Kennis Alliantie EKB de 4 oorspronkelijke IB's.

1.1 Doel

Doel van dit Safety en Compliance Plan is om alle werkzaamheden te beschrijven die nodig zijn om te komen tot 3 ontwerpen en 3 gerealiseerde "specifieke applicaties" (zie verderop), die aan alle veiligheidseisen en wettelijke eisen voldoen, opdat een Vergunning voor Indienststelling kan worden verkregen. Daarnaast omschrijft dit de te leveren documenten en ook de organisatie die ingericht wordt om voldoende veiligheid te waarborgen.

Dit plan is bedoeld voor diverse stakeholders (zie ook § 2.4):

- voor het projectteam van Sweco,
- voor ProRail, en dan met name het safety en compliance management,
- tot op zekere hoogte voor de andere IB's,
- voor de externe assessor (AsBo/NoBo) en
- mogelijk ook voor de Inspectie Leefomgeving en Transport (ILT).

Omdat een deel van de doelgroep niet dagelijks te maken heeft met safety en/of compliance management wordt er in dit plan soms uitgebreide uitleg gegeven over bepaalde onderwerpen. Lezers met meer ervaring kunnen deze stukken gemakkelijk overslaan.

1.2 Afbakening

Dit plan betreft het safety management en compliance management voor de 3 percelen waarbij Sweco verantwoordelijk is voor de engineering, de uitvoeringsbegeleiding en een deel van de testen. Het gaat hierbij specifiek over spoorwegveiligheid en TSI Compliance (zie § 2.3 voor het wettelijk kader). Arbeidsveiligheid wordt behandeld in het V&G Management Plan [18].

1.2.1 Specifieke Applicaties

Het treinbeveiligingssysteem van ieder perceel wordt (in CENELEC termen) gezien als een "Specifieke Applicatie". De afbakening, het doel en de functies van deze Specifieke Applicaties zijn in detail vastgelegd in de Systeemdefinitie [17].

1.2.2 Fasen van de levenscyclus

Treinbeveiligingssystemen worden ontwikkeld volgens de CENELEC systeem levenscyclus (zie EN 50126-1 [10], § 2.5 en § 6.1). Iedere Specifieke Applicatie heeft dus haar eigen levenscyclus.

Sweco is verantwoordelijk voor de fasen 1 t/m 6 van de levenscyclus van de 3 Specifieke Applicaties, van *Concept* t/m *Design and Implementation*. In de eerste fasen wordt daarbij wel geleund op het werk van ProRail. ProRail is als opdrachtgever eindverantwoordelijk voor het bredere vervoerssysteem (bijvoorbeeld inclusief monitoring- en verkeersleidingsystemen) en heeft al een concept ontwikkeld en klanteisen opgesteld.

De fabrikanten van systemen, apparatuur en componenten zijn verantwoordelijk voor fase 7, *Manufacture*. Het is dus aan de fabrikanten om aan te tonen dat hun systemen, apparatuur en componenten aan de gestelde eisen voldoet. Hier zijn echter wel raakvlakken want een deel van deze bewijsvoering moet worden opgenomen in de Specific Application Safety Cases. Merk op dat deze systemen, apparatuur en componenten in de meeste gevallen als product ook hun eigen levenscyclus doorlopen, voordat ze worden toegepast in de Specifieke Applicaties.

Aannemers (en in sommige gevallen ook fabrikanten) zijn verantwoordelijk voor fase 8, *Integration*, het plaatsen en aansluiten van de systemen, apparatuur en componenten. Sweco heeft hier echter ook verantwoordelijkheden: Sweco wordt ingeschakeld voor de uitvoeringsbegeleiding en ook voor het uitvoeren van testen bij de in bedrijf stelling. De bewijzen van veiligheid die de aannemer en fabrikanten aanleveren moeten door Sweco worden verwerkt in de Specific Application Safety Cases.

Sweco is verantwoordelijk voor fase 9, de Validatie van de 3 Specifieke Applicaties. Uitgangspunt daarbij is wel dat de Generieke Applicatie al gevalideerd is.

Zie verder § 6.1 voor de verdere afbakening van deze activiteiten.

1.2.3 Subsystemen

Sweco is verantwoordelijk voor de subsystemen die “langs de baan” geïnstalleerd worden. Welke dat zijn is in detail vastgelegd in de Systeemdefinitie [17]. Het gaat in deze paragraaf om subsystemen in technische zin; niet specifiek om de Subsystemen van het Europees Spoorwegsysteem, zoals bedoeld in de TSI's.

Sweco levert wel data aan voor de interlocking en het RBC, maar is niet verantwoordelijk het laden van de juiste data in die systemen. Die verantwoordelijkheid ligt bij Thales. Sweco is ook niet verantwoordelijk voor aanpassingen aan de verkeersleidingssystemen. Die verantwoordelijkheid ligt bij RIGD Loxia. De integratie van baanapparatuur met de centrale apparatuur valt echter wel binnen de scope.

De verantwoordelijkheid voor de integratie van alle subsystemen van het vervoersysteem ligt bij het ProRail project ENL, dat wordt aangestuurd vanuit het cluster ERTMS Uitrol op Spoorse Infra (EUSI). EUSI op haar beurt valt binnen het cluster Implementatie ERTMS ProRail (IEP) (zie § 2.4 en het Veiligheidsmanagementplan ENL van ProRail [14]).

Waar de demarcatie van verantwoordelijkheden precies ligt moet nog worden uitgewerkt in de Data Preparation en Verificatie & Validatie Plannen. Mogelijk gaan de IB's ook nog een rol spelen in het testen van de totale systeemintegratie en de bijbehorende safety cases, maar op dit moment valt dat buiten de scope.

1.2.4 Generieke Applicatie

De Generieke Applicatie wordt ontwikkeld, aangestuurd door het cluster Ontwikkelen en Vrijgeven ERTMS Beveiliging (OVEB). Ook OVEB valt binnen het cluster IEP. Zie § 2.4 en het Veiligheidsmanagementplan ENL van ProRail [14] voor verdere informatie.

Hoewel Sweco dus niet verantwoordelijk is voor de ontwikkeling van de Generieke Applicatie, is zij daar wel van afhankelijk en ook indirect bij betrokken. Immers, op het niveau van de Generieke Applicatie worden tal van ontwerpvoorschriften, installatievoorschriften, checklists en testspecificaties ontwikkeld die van toepassing zijn op het ontwerp en de realisatie van de 3 Specifieke Applicaties waarvoor Sweco verantwoordelijk is.

Hoewel er met dit soort voorschriften en specificaties al ervaring is opgedaan bij eerdere ETCS en beveiligingsprojecten zijn deze versies nieuw. Bovendien moeten hier nu de ontwerp- en installatievoorschriften van Thales in zijn verwerkt en was er bij eerdere projecten sprake van andere leveranciers. ENL is het eerste project waarmee er ervaring wordt opgedaan met deze nieuwe versies. Het is te verwachten dat er vanuit ENL een terugkoppeling naar OVEB komt over de bruikbaarheid en correctheid hiervan.

De verbanden met generiek ontwikkelde ontwerpvoorschriften, installatievoorschriften, checklists en testspecificaties worden in hoofdstuk 6 toegelicht.

1.3 Voorbehoud

Dit plan omschrijft alle voorziene werkzaamheden en te leveren producten tot en met de Systeemvalidatiefase. Hierbij wordt het voorbehoud gemaakt dat ProRail stapsgewijs opdrachten verstrekt voor het uitvoeren van werkzaamheden.

De deelopdrachten omvatten het volgende:

1. FIS, RVTO;
2. Detail Ontwerp;
3. Vraagspecificatie;
4. Bouwmanagement;
5. Testen en in bedrijf stellen.

Op dit moment is alleen deelopdracht 1 ontvangen. Voor werkzaamheden in latere fasen geldt het voorbehoud dat deze alleen uitgevoerd worden indien ProRail daartoe opdracht verstrekt.

Hierbij wordt ook aangetekend dat het hier om een regieopdracht gaat. De omschrijvingen van de werkpakketten zijn nogal standaard en zijn niet erg specifiek ingevuld voor het ENL project. De specifieke invulling wordt onder ProRail's regie in overleg bepaald, bijvoorbeeld aan de Lead Engineers Tafel, de Systems Engineering Tafel, de Safety Tafel of de RAM Tafel. Als gevolg hiervan zijn de plannen aan verandering onderhevig.

1.4 Relatie met andere plannen

Safety management bouwt voort op kwaliteitsmanagement. Zowel safety management als compliance management zijn nauw verweven met systems engineering. Dat betekent dat allerlei te doorlopen processen en te leveren documenten (producten) al beschreven zijn in andere plannen. De belangrijkste daarvan zijn:

- Het Project Management Plan [18];
- Het Systems Engineering Werkplan [23];
- Het Verificatieplan¹ [21];
- Het Validatieplan [22].

Wanneer informatie al in een ander plan beschikbaar is wordt daar vanuit dit plan naar verwezen. Vanwege de leesbaarheid wordt die informatie soms kort samengevat in dit Safety en Compliance Plan.

Extern is er een relatie met het Veiligheidsmanagementplan ENL [14] en het V&V managementplan [16] van ProRail.

1.5 Structuur van dit plan

Dit hoofdstuk 1 geeft de inleiding op het Safety en Compliance Plan.

Hoofdstuk 2 presenteert het te realiseren systeem op hoofdlijnen en de wettelijke en organisatorische context.

In hoofdstuk 3 wordt de strategie gepresenteerd om tot geaccepteerde Specifieke Applicaties te komen op de 3 percelen.

¹ Het Verificatieplan en het Validatieplan zijn op dit moment nog niet geschreven.

Hoofdstuk 4 geeft een overzicht van het kwaliteitsmanagement en gaat gedetailleerd in op drie specifieke aspecten daarvan.

Hoofdstuk 5 presenteert zowel de interne veiligheidsorganisatie (binnen het Sweco project) als de externe (Sweco in relatie tot andere stakeholders). Hoofdstuk 6 legt het verband tussen enerzijds de activiteiten en te leveren producten die vereist zijn volgens de wetgeving (CSM-REA [3]) en de CENELEC normen EN 50126-1 [10] en EN 50128 [12] en anderzijds de werkpakketten. Op verschillende activiteiten en te leveren producten wordt een uitgebreidere toelichting gegeven.

Hoofdstuk 7 gaat in op alle aspecten van het hazard management en de beoordeling van de veiligheid door een Assessment Body.

Hoofdstuk 8 tenslotte gaat in op het aantonen van de compliance met de TSI's en andere wetgeving, en de externe beoordeling daarvan door een Notified Body.

1.6 Gebruikte afkortingen

ADSC	Application Design Safety Case
AsBo	Assessment Body
EKB	ERTMS Kijfhoek – Belgische grens
EHL	ERTMS Hanzelijn
ENL	ERTMS Noordelijke Lijnen
ERA	European Union Agency for Railways (vroeger: European Railway Agency)
ESAAL	ERTMS Schiphol – Amsterdam – Almere – Lelystad
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
EVC	European Vital Computer
FIS	Functioneel Integraal Systeemontwerp
GASC	Generic Application Safety Case
GPSC	Generic Product Safety Case
GSM-R	Global System for Mobile Telecommunication - Railways
HAZID	Hazard Identification (workshop)
IB	Ingenieursbureau
IEP	Implementatie ERTMS ProRail
ILT	Inspectie Leefomgeving en Transport
IXL	Interlocking
K&L	Kabels en leidingen
LCC	Life Cycle Costs
NoBo	Notified Body

OBE	Ontwerp(tekening) Baan en Emplacement
OC	Object Controller
OI	Ondergrondse Infrastructuur
OVEB	Ontwikkelen en Vrijgeven ERTMS Beveiliging
PISC	Physical Implementation Safety Case
RAM	Reliability, Availability, Maintainability
RBC	Radio Block Centre
RVT	Railverkeerstechniek
RVTO	Railverkeerstechnisch Ontwerp
SASC	Specific Application Safety Case
SE	Systems Engineering
SIL	Safety Integrity Level
SMB	Stop Marker Board
SRAC	Safety Related Application Condition
TB	Treinbeveiliging
TBB	TreinBeveiligings- en Beheersingsinstallaties
TO	Track Occupancy (spoorbezetting)
TSI	Technische Specificatie voor Interoperabiliteit / Technical Specification for Interoperability
TvG	Toestemming voor Gebruik
EUSI	ERTMS Uitrol op Spoorse Infra
V&G	Veiligheid en Gezondheid
Vvl	Vergunning voor Indienststelling

2 Systeem en context

Dit hoofdstuk presenteert het te realiseren systeem op hoofdlijnen en de wettelijke en organisatorische context.

2.1 Generieke Applicatie

De Generieke Applicatie wordt ook wel het generieke systeem genoemd. Dit omvat alle systeemelementen, onafhankelijk van de toepassing op een bepaalde spoorlijn of emplacement.

De ontwikkeling van de Generieke Applicatie wordt aangestuurd door het cluster OVEB. Van de Generieke Applicatie is weinig documentatie ontvangen; de informatie daarover is daarom vrij summier. De scope er van wordt geïllustreerd door de Technische Referentiearchitectuur Vervoersysteem [15]. Deze scope is echter veel ruimer dan de subsystemen waar Sweco mee te maken heeft, en bevat bijvoorbeeld ook de monitoringsystemen en het GSM-R netwerk.

Ons uitgangspunt is dat de Generieke Applicatie overeenkomt met het Central Safety System.

De belangrijkste subsystemen en componenten daarvan zijn:

- Interlocking (IXL);
- Radio Block Centre (RBC);
- Assentellers;
- Object Controllers (OC);
- Eurobalises;
- Signalling network (tussen IXL en OCs).

De belangrijkste externe interfaces zijn die met:

- Het GSM-R netwerk;
- ASTRIS en ETIS;
- De treinen inclusief ERTMS en andere relevante on-board apparatuur;
- Wissels;
- Overweginstallaties;
- Beweegbare bruggen;
- Seinen;
- Waarschuwinginstallaties;
- Spoor;
- Naburige interlockings;
- Naburige treinbeïnvloedingssystemen (ATB, PZB);
- Monitoringsystemen;
- Energievoorziening;
- Treindienstleiders;
- Servicemonteurs.

Zie de Systeemdefinitie [17] voor uitgebreidere informatie.

2.2 Specifieke Applicaties

Een Specifieke Applicatie is een locatiespecifieke toepassing van het generieke systeem; toepassing op een bepaalde spoorlijn of emplacement. De Specifieke Applicaties waar Sweco aan werkt bestaan dus uit de Generieke Applicatie, uitgelegd op de 3 percelen:

4. Groningen – Eemshaven / Delfzijl;
5. Groningen – Bad Nieuwesches (Duitse grens) / Veendam;
6. Emplacement Groningen.

De omvang en functies van de Specifieke Applicaties worden in detail beschreven in de Systeemdefinitie.

Wanneer de nieuwe systemen geïnstalleerd en in bedrijf zijn gesteld zullen de volgende oude systemen verwijderd worden:

- Treindetectie (assentellers en/of spoorstroomlopen);
- ATB apparatuur;
- Licht- en bordseinen;
- Object Controllers / aansluitkasten;
- Interlockings;
- Met alle bijbehorende bekabeling.

Dit brengt een aantal (overgangs-) situaties met zich mee:

1. Oude systemen in bedrijf;
2. Oude systemen in bedrijf, nieuwe worden gebouwd;
3. Oude systemen in bedrijf, nieuwe worden getest;
4. Nieuwe systemen in bedrijf; oude buiten bedrijf;
5. Nieuwe systemen in bedrijf, oude verwijderen, kabels omleggen;
6. Eindsituatie bereikt met alleen nieuwe systemen.

Dit betekent dat niet alleen de veiligheid van de nieuwe systemen aangetoond moet worden, maar ook van de tijdelijke situaties. Ook de risico's van het verwijderen van bestaande systemen zullen bekeken moeten worden, met name wat betreft onbedoelde effecten (denk bijvoorbeeld ook aan de interfaces met Post '21).

2.3 Wettelijke context

De wettelijke context wordt in de eerste plaats bepaald door 2 Europese Richtlijnen op spoorweggebied, met daaronder een aantal verordeningen:

- De Richtlijn voor spoorwegveiligheid [2];
- De Verordening betreffende de gemeenschappelijke veiligheidsmethode voor risico-evaluatie en -beoordeling [3] (CSM-REA in het Engels);
- De Interoperabiliteitsrichtlijn [1];
- De TSI Besturing en Seingeving [4];

Er zijn nog 3 TSI's van toepassing op het ProRail project, maar deze raken niet de scope van de IB's:

- TSI Exploitatie en verkeersleiding [5];
- TSI Telematicatoepassingen ten dienste van passagiers [6];
- TSI Telematicatoepassingen voor goederenvervoer [7].

Europese Richtlijnen worden overgenomen in nationale wetgeving. Bovenstaande Richtlijnen zijn daarom overgenomen in de Nederlandse Spoorwegwet [8]. De Verordeningen gelden direct in alle Lidstaten. Dit wettelijk kader stelt niet alleen eisen aan de techniek maar ook aan de processen die doorlopen moeten worden, zoals onafhankelijke beoordelingen door een AsBo en een NoBo en de vergunningverlening door ILT. Daarom richt dit plan zich op deze wetgeving.

Naast deze spoorweginstallatie specifieke wetgeving geldt er ook meer algemene wetgeving (zie ook de bestaande veiligheidsmaatregelen in hoofdstuk 5 van de Systeemdefinitie). Compliance met deze wetgeving wordt gemanaged door middel van opnamen van de wettelijke eisen in de SRS. Vanaf dat moment worden de eisen meegenomen in het ontwerp en in de realisatie en wordt met verificatie en validatie geborgd dat aan de wettelijke eisen wordt voldaan.

Omdat daar geen beoordeling door een onafhankelijke derde partij aan te pas komt wordt daar in dit plan verder geen speciale aandacht aan besteed.

Overigens ligt de verantwoordelijkheid voor het voldoen aan wettelijke eisen in de meeste gevallen bij de fabrikant van apparatuur. In die gevallen is de conformiteitsverklaring van de fabrikant voor het project voldoende bewijs van compliance. In sommige gevallen zal aangetoond moeten worden dat aan de ontwerp- en installatievoorschriften van de fabrikant is voldaan.

2.4 Stakeholders

De volgende stakeholders spelen een rol in dit project:

- ProRail: beheerder van de infrastructuur en opdrachtgever;
- Arriva, NS: gebruikers van de infrastructuur;
- ERA: beheerder van het ERTMS systeem; ERTMS trackside approval;
- ILT: vergunningverlener;
- N.t.b.: AsBo en NoBo;
- Arcadis: IB voor andere ENL percelen;
- Nexus: IB voor andere ENL percelen;
- Thales: fabrikant van de ETCS en interlocking apparatuur, inclusief assentelsysteem;
- RIGD Loxia: leverancier van de verkeersleidingsystemen;
- N.t.b.: leverancier van de Object Controllers;
- N.t.b.: aannemer voor de installatie van de baanapparatuur.

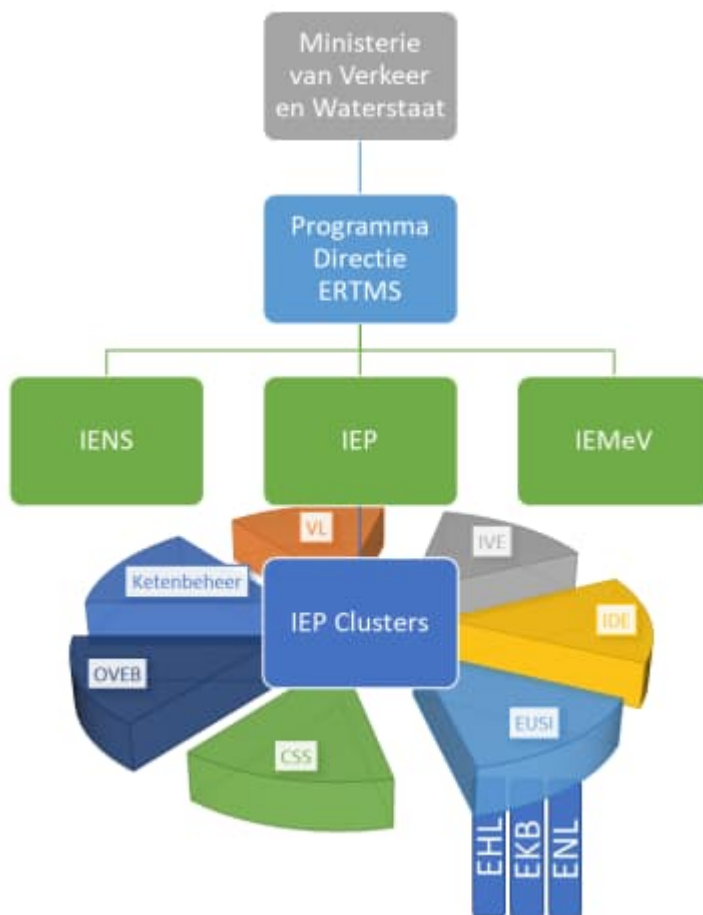
2.4.1 Context

Het Ministerie van Infrastructuur en Waterstaat is de opdrachtgever voor de uitrol van ERTMS in Nederland. Zij heeft de Programmadirectie ERTMS aangesteld, die de regie heeft over het realiseren van ERTMS in Nederland. De Programmadirectie stuurt 3 clusters aan:

- Implementatie ERTMS bij ProRail (IEP);
- Implementatie ERTMS bij NS (IENS);
- Implementatie ERTMS bij materiele eigenaren en vervoerders (IEMeV).

IEP kent binnen ProRail 7 clusters, elk vanuit hun eigen kennisgebied:

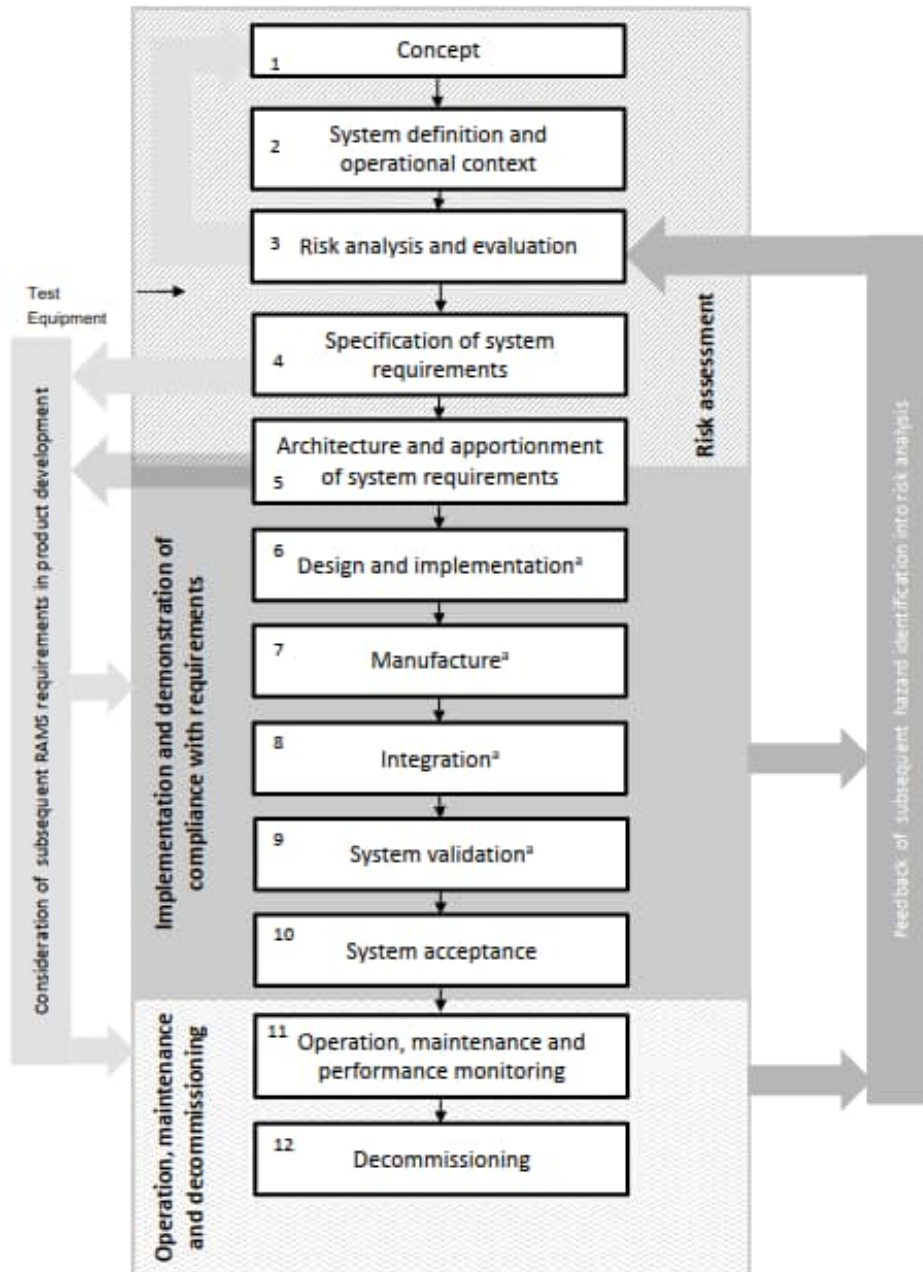
- Ketenbeheer (onderhoud/beheer);
- VL: Verkeersleiding;
- IVE: ICT voor ERTMS;
- IDE: InfraData voor ERTMS;
- EUSI: ERTMS Uitrol op Spoorse Infra;
- CSS: aanbesteding Central Safety System;
- OVEB: Ontwikkelen en Vrijgeven ERTMS Beveiliging.



Andere stakeholders waar ProRail m.b.t. ENL een relatie mee onderhoudt zijn de Provincie Groningen en de Provincie Friesland.

2.5 Levenscycli

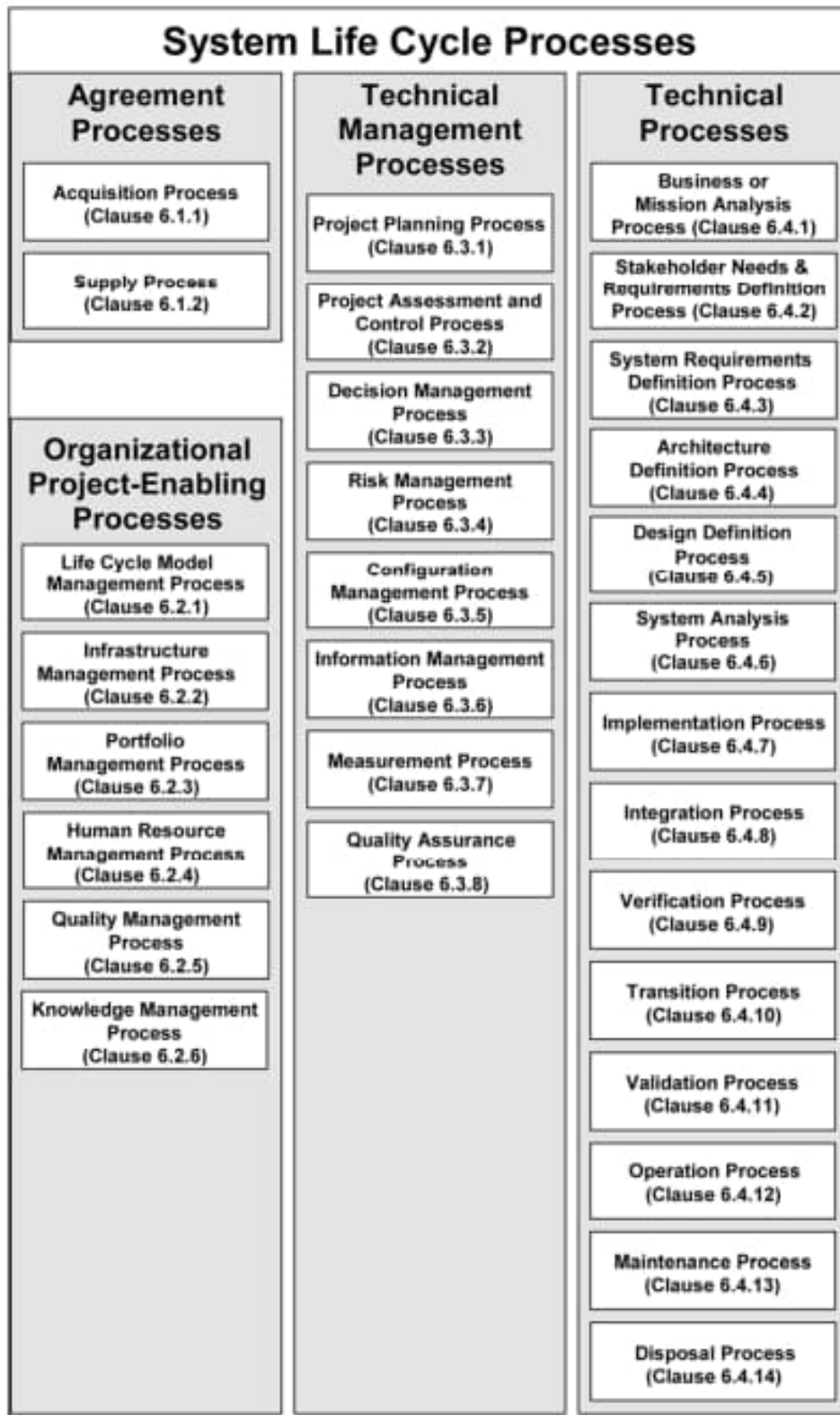
ETCS en de interlocking zijn SIL 4 systemen die de CENELEC system life cycle doorlopen:



Figuur 2: De CENELEC system life cycle

Daarnaast kent CENELEC een software life cycle volgens EN 50128.

De voeding en het signalling network zijn SIL 0 systemen, die meer volgens Systems Engineering worden ontworpen en gerealiseerd:



Figuur 3 - De processen volgens ISO 15288

Deze twee methoden zijn nauw verwant maar niet helemaal hetzelfde. ISO 15288 specificeert processen; EN 50126 specificeert fasen; beide specificeren

activiteiten, taken en resultaten. De relatie tussen Technische Processen van Systems Engineering en de CENELEC system life cycle wordt in de tabel hieronder geïllustreerd.

Systems Engineering process	CENELEC phase
Business or Mission Analysis	1. Concept
Stakeholder Needs and Requirements definition	2. System Definition and operational context
	3. Risk Analysis and Evaluation
System Requirements Definition	4. System requirements specification
Architecture Definition	5. Architecture and apportionment of system requirements
Design Definition	6. Design and Implementation
Implementation	7. Manufacture
Integration	8. Integration
Transition	
Validation	9. System validation
	10. System acceptance
Operation	11. Operation, maintenance and performance monitoring
Maintenance	
Disposal	12. Decommissioning

In dit Safety en Compliance Plan gaan we in de eerste plaats uit van de CENELEC system life cycle omdat die wordt voorgeschreven door de TSI CCS [4]. Bovendien is het zo dat wanneer deze CENELEC system life cycle correct doorlopen is, er voldaan is aan de eisen van CSM-REA [3].

3 Strategie

In dit hoofdstuk wordt de strategie gepresenteerd om tot geaccepteerde Specifieke Applicaties te komen op de 3 percelen.

Uitgangspunt voor het Safety en Compliance Management op het Specifieke Applicatie niveau is dat de Generieke Producten en Generieke Applicatie voldoen aan de wetgeving:

1. Alle veiligheidsrisico's zijn voldoende gemitigeerd, hetzij in het ontwerp van de producten en systemen zelf, hetzij door verwerking van veiligheidseisen (Safety Related Application Conditions) in ontwerpvoorschriften, installatievoorschriften, testvoorschriften en – specificaties, bedieningsvoorschriften en onderhoudsvoorschriften.
2. Relevante TSI-eisen zijn ofwel geadresseerd op het Generic Application (GA) niveau ofwel verwerkt in genoemde voorschriften.

De bewijsstukken hiervoor, die wij zullen verzamelen voor de 3 Specific Application Safety Cases dan wel de TSI compliance dossiers, zijn:

- De conformiteitsverklaringen van fabrikanten;
- De ondersteunende 'EG' certificaten van hun Notified Bodies;
- Het Independent Safety Assessment Report van de Generieke Applicatie, opgesteld door cluster OVEB's Assessment Body;
- Het Type Examination Certificate (of eventueel een Intermediate Statement of Verification) voor de Generieke Applicatie, uitgegeven door cluster OVEB's Notified Body.

Met deze bewijsstukken is straks voldoende aangetoond dat de Generieke Producten en de Generieke Applicatie voldoen aan de wetgeving, en dat, wanneer aan genoemde voorschriften wordt voldaan, de producten op een juiste manier worden toegepast en dat de veiligheid van het systeem in het algemeen voldoende geborgd is.

Op het niveau van de Specifieke Applicaties moeten dan nog de lijnspecifieke "hazards" (gevaarlijke situaties) in beeld gebracht en gemitigeerd worden. Evenals de hazards die ontstaan door het tegelijkertijd aanwezig zijn van het 'oude' en 'nieuwe' systeem en het verwijderen van het 'oude' systeem. Hiertoe wordt het CSM-REA risicobeheerproces [3] doorlopen.

Om aan te tonen dat de Specifieke Applicaties aan alle eisen voldoen wordt na iedere fase geverifieerd of a) het voorgeschreven proces correct is doorlopen en b) of de resultaten (output) in overeenstemming zijn met de input. Na realisatie wordt gevalideerd dat de Specifieke Applicatie voldoet aan de systeemeisen.

Alle stappen zullen onafhankelijk beoordeeld worden door een derde partij, in de rollen van Assessment Body (AsBo) en Notified Body (NoBo).

In de volgende hoofdstukken wordt deze strategie uitgewerkt naar concrete stappen.

4 Kwaliteitsmanagement

De basis van veiligheidsmanagement ligt bij kwaliteitsmanagement. Het kwaliteitsmanagement van dit project is gebaseerd op het managementsysteem van Sweco Nederland, dat ISO 9001 gecertificeerd is.

Voor de volgende aspecten van kwaliteitsmanagement wordt verwezen naar het Projectmanagementplan [18]:

- Kwaliteit in het algemeen;
- Samenwerking en organisatie;
- Planning;
- Informatiemanagement;
- Wijzigingsmanagement;
- Risicomanagement;
- Monitoring.

Voor de volgende aspecten wordt verwezen naar het Systems Engineering Workplan:

- Kennismanagement;
- Besluitvorming;
- Configuratiemanagement;
- Uitvoering.

Drie aspecten worden hieronder apart toegelicht.

4.1 Ontwerpen met IMX data

ProRail is bezig om van traditionele (ontwerp-) tekeningen over te stappen naar een ontwerp- en asset management methodiek die gebaseerd is op data in het IMX formaat. Alle gegevens over de assets die bij ProRail in beheer zijn, worden dan in dat formaat opgeslagen en beheerd. Tekeningen kunnen nog wel worden gegenereerd vanuit de IMX data omdat die nou eenmaal beter leesbaar zijn maar ontwerpen worden niet meer primair in tekeningen gemaakt.

De inrichting van alle benodigde processen valt onder het cluster IDE (InfraData voor ERTMS). De processen voor de uitgifte van de IMX data van het bestaande spoor en de inname van de IMX data van een ontwerp zijn nog in ontwikkeling.

Uitgangspunten voor Sweco zijn:

- De processen voor uitgifte en inname van IMX data worden ontwikkeld onder het cluster IDE;
- De processen voor uitgifte en inname van IMX data worden geaccepteerd door een Assessment Body (AsBo);
- Door ProRail aangeleverde IMX data is correct en voldoende nauwkeurig dan wel met behulp van andere (referentie) gegevens voldoende nauwkeurig en betrouwbaar te maken voor een veilig ontwerp.

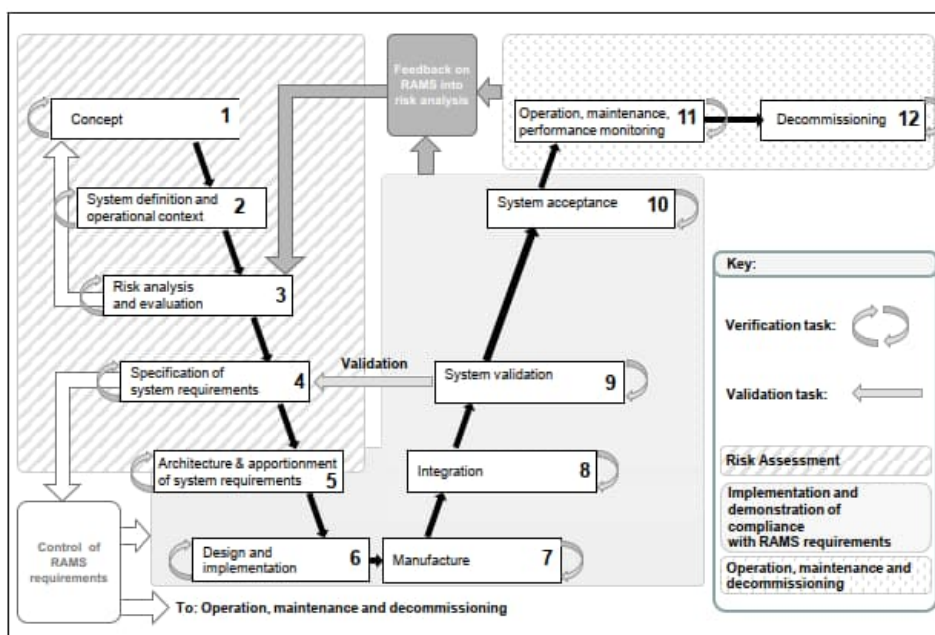
Tools voor het werken met IMX data (zowel ontwerpen als verifiëren) worden door Sweco zelf ontwikkeld buiten het project ENL om (zie ook § 6.9).

4.2 Verificatie

De definitie van verificatie volgens EN 50126 is: *confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.*

Deze definitie komt overeen met ISO 9001: *verificatieactiviteiten worden uitgevoerd om ervoor te zorgen dat de ontwerp- en ontwikkelingsoutputs aan de inpuisen voldoen.*

Verificatie is dus voorzien aan het eind van iedere fase. Daarbij wordt zowel getoetst of de producten voldoen aan de normeisen (EN 50126, EN 50128, CSM-REA) als aan de inpuisen. Onderstaande figuur (figure 7 uit EN 50126-2) illustreert dit.



Figuur 4: Verificatie en Validatie volgens het CENELEC V-model

De hoofdlijnen van de verificaties liggen vast in het *V&V managementplan* van ProRail [16]. Het nog te schrijven *Verificatieplan* [21] gaat de details geven over:

- welk (output) document wordt geverifieerd tegen welk (input) document;
- welke methoden zijn voorzien;
- wie doet wat en wanneer; en
- welke checklists en test specificaties worden uitgewerkt door het Verificatieteam en welke gaan we ontvangen van het cluster OVEB?

De meest gebruikelijke verificatiemethoden zijn document review, gebruik van checklists, inspecties en testen. Voor een deel van de testen bestaan er al test-specificaties van ProRail; voor een deel van de testen worden die door het project ontwikkeld. Uiteindelijk zal er voor iedere eis een verificatiestap gedefiniëerd worden met goed- en afkeurcriteria.

4.3 Validatie

EN 50126 definieert validatie als: *confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.*

Ook deze definitie sluit goed aan bij ISO 9001: *activiteiten voor validatie worden uitgevoerd om ervoor te zorgen dat de resulterende producten en diensten aan de eisen voor de gespecificeerde toepassing of het beoogde gebruik voldoen.*

EN 50126 vereist 2 validatiemomenten:

1. Validatie van de System Requirements Specification, aan het eind van fase 4;
2. Validatie van het systeem in fase 9.

De eisen hieraan staan in §§ 6.7.3, 7.5.4 en 7.10 van EN 50126-1.

Het voorziene Validatieplan [22] zal gedetailleerd ingaan op de aanpak.

4.3.1 Validatie tegen klanteisen

Naast deze validatie volgens de CENELEC standaard wordt de term validatie ook vaak gebruikt voor het met de klant nagaan of het systeem (-ontwerp) nog steeds aan de klanteisen en -wensen voldoet (“wordt het juiste gebouwd?”). Klanteisen zijn niet altijd even hard en voortschrijdend inzicht kan leiden tot aangepaste eisen en wensen, die in het project meegenomen moeten worden. Dat betekent dat de SRS, het ontwerp en het gerealiseerd systeem getoetst worden tegen de CRS.

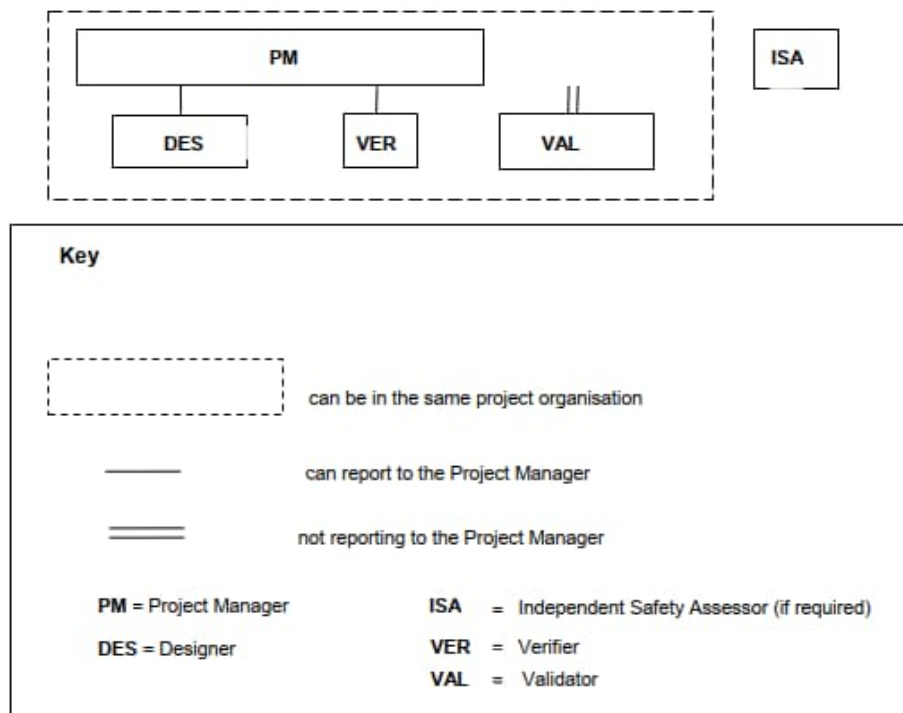
Dit is een belangrijk proces, maar dat is dus iets anders dan wat er in de CENELEC standaarden met validatie wordt bedoeld. Voor validatie tegen de klanteisen gelden dan ook niet de onafhankelijkheidseisen die in § 5.1 worden genoemd.

5 Veiligheidsorganisatie

Dit hoofdstuk presenteert zowel de interne veiligheidsorganisatie (binnen het Sweco project) als de externe (Sweco in relatie tot andere stakeholders).

5.1 Interne veiligheidsorganisatie

ETCS en de interlocking zijn SIL 4 systemen. Daarvoor stelt EN 50126-2 [11] eisen aan de onafhankelijkheid van de Verifiers en Validators. Verifiers en Designers moeten gescheiden zijn; een Verifier mag niet aan het ontwerp hebben gewerkt. Maar ze mogen wel allebei worden aangestuurd door de Project Manager (of een Lead Engineer). De Validator moet volledig onafhankelijk zijn.



De rollen in het projectteam worden als volgt ingedeeld in de 4 groepen. Deze indeling is moeilijk terug te zien in het organogram [19]. Daarom worden de rollen en namen hier apart benoemd.

5.1.1 Project Management

In deze groep vallen zowel de algemene management rollen als de technische management rollen.

Algemeen project management

- Projectmanager: Rudolf van Aken
- Financieel manager: Daniëlle Bode
- Informatiemanager: Roos Hoogendijk
- Risicomanager: Pieter de Heer Kloots

Technisch management

- Lead Engineer Techniek: Bouwie Bakker
- Lead Engineer SE en Omgeving / Conditionering: Bouke Stoker
- Adviseur Techniek: Gert-Jan van den Elzen
- Veiligheid en Gezondheid (V&G) manager: Hanneke Voordes
- RAM/LCC manager: Jaap Ton
- Safety manager: Krijn Rabouw

5.1.2 Designers

In deze groep vallen alle rollen die technisch inhoudelijk een bijdrage leveren aan het creatieve proces. Dat betreft niet alleen het ontwerp, maar bijvoorbeeld ook het uitvoeren van analyses en het opstellen van eisen in de vroege fasen en het installeren en integreren van het systeem in de latere fasen.

Designers worden aangestuurd door het technisch management.

Ontwerpfasen

- Adviseur ERTMS: Jari Klomp, Gert-Jan van den Elzen
- Adviseur overwegveiligheid: N.t.b.
- Adviseur RVT: N.t.b.
- Adviseur security: N.t.b.
- Adviseur voeding TBB: André Hirdes
- Configuratiemanager: Roos Hoogendijk
- Systems Engineer: Fazia Ghuman
- Ontwerpleiders FIS: Antonio Russo, Martin Vink
- Ontwerpers FIS 4 (Gn – Rde/Dz): Martijn Geertjes, Lucia Bloemendal
- Ontwerpers FIS 5 (Gn – Nsch): Bart van Assen, Benjamin Smakic
- Ontwerpers FIS 6 (Gn empl.): Hendrik Spek, Rommy Luitjens, Bart van Assen
- Ontwerpleider RVTO: Martin Vink
- Ontwerpers RVTO 4 (Gn – Rde/Dz): Rommy Luitjens, Martijn Geertjes, Lucia Bloemendal
- Ontwerpers RVTO 5 (Gn – Nsch): Antonio Russo, Bart van Assen, Benjamin Smakic
- Ontwerpers RVTO 6 (Gn empl.): Hendrik Spek, Bart van Assen
- Ontwerpleider/adviseur OI: Diederik Hoekman
- Ontwerper OI: Roy van Oudenaarden (two-b)
- Ontwerpleider/adviseur TB: Natan Gomes
- Ontwerper TB: N.t.b.

Realisatiefasen

- Ontwerpleider/adviseur uitvoering: N.t.b.

Designers zonder directe relatie met systeemveiligheid

- Adviseur Brondata/bestaande situatie: Bennie Zwartenkot
- Adviseur Conditionering: Bouke Stoker
- Adviseur Duurzaamheid: Fred Verwoerd
- Adviseur Ecologie: Rietje Klous
- Adviseur Vergunningen: Melanie Hirsch

5.1.3 Verifiers

In deze groep vallen de medewerkers die het werk van de designers formeel verifiëren.

Verifiers worden aangestuurd door het technisch management.

- Verifiers FIS 4 (Gn – Rde/Dz): Hendrik Spek, Rommy Luitjens
- Verifiers FIS 5 (Gn – Nsch): Rommy Luitjens
- Verifiers FIS 6 (Gn empl.): Rommy Luitjens

- Verifiers RVTO 4 (Gn – Rde/Dz): Alfons Oldenkamp, Jianxin Yuan
- Verifiers RVTO 5 (Gn – Nsch): Hendrik Spek, Rommy Luitjens
- Verifiers RVTO 6 (Gn empl.): n.t.b.

- Verifiers DO: n.t.b.

Sommige Verifiers werken ook als designer aan een FIS of RVTO, maar uiteraard nooit in beide rollen aan hetzelfde perceel.

5.1.4 Validator

De validator van het project is: **NTB**

De validator is **autonoom** en wordt niet aangestuurd door het technisch management.

5.2 Externe veiligheidsorganisatie

5.2.1 Safety tafel

Binnen het project ENL is er een safety tafel. Hierin overleggen de safety managers van ProRail, Arcadis, Nexus en Sweco over het veiligheidsmanagement met betrekking tot ENL.

Er bestaan 2 Kennis Allianties: ENL/EHL/ESAAL en EKB. Op dit moment is er geen gezamenlijke safety tafel ENL/EHL/ESAAL of afstemming met EKB, maar op verzoek van ProRail zou daaraan deelgenomen kunnen worden.

Op uitnodiging neemt Sweco's Safety Manager deel aan de Lead Engineers Tafel, Systems Engineering Tafel of aan de samenwerkingsdagen.

5.2.2 Raakvlakken

Het safety management van de kennisalliantie ENL heeft raakvlakken met het safety management van Thales, RIGD Loxia en eventueel de leverancier van de Object Controllers.

Uitgangspunt is dat deze raakvlakken gemanaged worden door de Safety Manager ENL van ProRail.

5.2.3 Independent assessor

Het Independent Safety Assessment, zowel tegen CSM-REA als tegen de CENELEC standaarden, wordt uitgevoerd door de AsBo. De 'EG' Verificatie m.b.t. de interoperabiliteitsrichtlijn wordt uitgevoerd door de NoBo (zie § 8.2). ProRail is voornemens voor de rollen van AsBo en NoBo dezelfde marktpartij te contracteren; 1 partij voor heel ENL. Hiertoe wordt een Europese

aanbestedingsprocedure doorlopen. Naar verwachting kan het contract met de AsBo/NoBo in augustus 2023 worden gesloten.

Sweco's Safety Manager is de eerste contactpersoon voor de AsBo/NoBo.

5.2.4 Vergunningen

Om de geharmoniseerde implementatie van ERTMS en interoperabiliteit in de hele Europese Unie te waarborgen, is een "ERTMS trackside approval" nodig van de ERA. De ERA controleert daarbij of de beoogde technische oplossingen volledig in overeenstemming zijn met de relevante TSI's.

ERTMS trackside approval wordt aangevraagd door ProRail. De IB's leveren hierbij zo nodig ondersteuning (werkpakket 9.5)

ERTMS trackside approval zou aangevraagd moeten worden voordat een aanbestedingsprocedure voor ERTMS apparatuur gestart wordt. Aangezien ProRail inmiddels een overeenkomst met Thales heeft gesloten is het niet duidelijk wat er op dit moment nog gedaan moet worden.

Voor het ERTMS systeem dient ProRail een Vergunning voor Indienststelling (VvI) aan te vragen bij ILT. De IB's leveren hierbij ondersteuning door benodigde stukken voor het aanvraagdossier aan te leveren aan ProRail (werkpakket 9.3).

5.2.5 Toestemming voor gebruik

Uitgangspunt is dat alle systemen en bijbehorende voorschriften worden vrijgegeven in parallel aan de goedkeuring van de Early Deployment Line. Daarom zijn Toestemmingen voor Gebruik (TvG's) van nog niet vrijgegeven ERTMS apparatuur (van ProRail) niet voorzien voor de latere percelen.

6 Activiteiten en producten

Dit hoofdstuk legt het verband tussen enerzijds de activiteiten en te leveren producten die vereist zijn volgens de wetgeving (CSM-REA [3]) en de CENELEC normen EN 50126-1 [10] en EN 50128 [12] en anderzijds de werkpakketten. Op verschillende activiteiten en te leveren producten wordt een uitgebreidere toelichting gegeven.

6.1 Specifieke Applicaties

De Specifieke Applicaties waar Sweco aan werkt bestaan uit de Generieke Applicatie, uitgelegd op de 3 percelen:

4. Groningen – Eemshaven / Delfzijl;
5. Groningen – Bad Nieuwesches (Duitse grens) / Veendam;
6. Emplacement Groningen.

Elk van de 3 Specifieke Applicaties doorloopt de CENELEC system life cycle. Hierin zitten een aantal gemeenschappelijke elementen: bijvoorbeeld dit *Safety en Compliance Plan* wordt maar 1 keer opgesteld en is geldig voor alle 3 de percelen.

Onderstaande tabel geeft de producten (deliverables) per fase van de levenscyclus en geeft aan in welk werkpakket die tot stand komen.

Fase	Belangrijkste activiteit / product	WP	Omschrijving
1. Concept	Documented results [De OCDs en CRS's van ProRail]		
2. System definition and operational context	Systeemdefinitie	3.1b	Systems Engineering
	FIS hoofdstuk 2	4.3	Functioneel Integraal Systeemontwerp
	Safety Plan	9.1	Safety management
	Verificatieplan	3.5a	Verificatie & Validatie
	Verificatierapport	3.5a	Verificatie & Validatie
3. Risk analysis and evaluation	Risk Assessment	3.16 3.17	Risico analyse overwegveiligheid Veiligheid: VMS 4.0
	Hazard Log	3.17	Veiligheid: VMS 4.0
	Verificatierapport	3.5a	Verificatie & Validatie
4. Specification of system requirements	SRS	3.3a	Opstellen System Requirement Specification
	Safety validation plan	3.5a	Verificatie & Validatie
	Verificatierapport	3.5a	Verificatie & Validatie
	Validatierapport fasen 1 - 4	3.5a	Verificatie & Validatie
	Systeemarchitectuur Specifieke Applicatie	3.3b	Opstellen Sub System Requirement Specification

Fase	Belangrijkste activiteit / product	WP	Omschrijving
5. Architecture and apportionment of system requirements	Allocation of RAMS requirements	3.3b	Opstellen Sub System Requirement Specification
	Acceptance criteria, processes and procedures	3.5a 8.6	Verificatie & Validatie Testen en indienststellen treinbeveiliging
	Verificatierapport	3.5a	Verificatie & Validatie
6. Design and Implementation	FIS	4.3	Functioneel Integraal Systeemontwerp
	RVTO	4.7	Rail Verkeerstechnisch Ontwerp
	DO	4.8a 4.8b 4.9 4.10 4.13 4.14	Ontwerp Treinbeveiligingsinstallaties Ontwerp Kabels en Leidingen Ontwerp Baan en Spoor Ontwerp Energievoorziening Ontwerp voeding TBB Ontwerp IXL-netwerk
	Vraagspecificatie	6.1	Vraagspecificatie
	Configuratiemanagement	3.22	Configuratiemanagement ontwerp
	Risk Assessment	3.16	Risico analyse overwegveiligheid
	Updated Hazard Log	3.17 3.24	Veiligheid: VMS 4.0 Afwijkingen OVS
	SASC part Application Design Safety Case	9.4	Opstellen SASC
	TSI compliance dossier / technisch dossier	9.1	Safety Management
	Verificatierapporten	3.5a	Verificatie & Validatie
	Independent Safety Assessment Report		AsBo
	Design Examination Certificate of ISV ²		NoBo
7. Manufacture	Producten		Fabrikanten
	FAT rapporten		Fabrikanten
	Conformiteitsverklaringen		Fabrikanten
8. Integration	Gerealiseerd systeem		Aannemer
	Installatierapporten		Aannemer
	Testrapporten		Aannemer
	Testrapporten	3.5a	Verificatie & Validatie
	In-bedrijf-stellingsrapporten	3.5a 8.6	Verificatie & Validatie Testen en in dienst stellen TB

² Dit is afhankelijk van het gekozen Assessment Module

Fase	Belangrijkste activiteit / product	WP	Omschrijving
9. Validation	Validatierapport	3.5a	Verificatie & Validatie
	SASC part Physical Implementation Safety Case	9.4	Opstellen SASC
	TSI compliance dossier / technisch dossier	9.1	Safety Management
	Verificatierapporten	3.5a	Verificatie & Validatie
10. Acceptance	Independent Safety Assessment Report		AsBo
	Veiligheidsverklaring		ProRail
	'EG' certificaten en NoBo technisch dossier		NoBo
	Technisch Dossier		ProRail
	'EG' Keuringsverklaring		ProRail
	Vergunning voor indienststelling		ILT

De meeste van bovenstaande producten worden geleverd door Sweco (tenzij anders aangegeven). Een aantal wordt ontwikkeld door de 3 IB's tezamen, waarbij dan onderscheid wordt gemaakt naar een gezamenlijk deel en een deel per IB of per perceel. Dit geldt bijvoorbeeld voor de Systeemdefinitie en het SRS.

6.2 Configuratiegegevens

Tot de scope van het project behoort het aanlevering van de configuratiegegevens (applicatiegegevens) voor het RBC, de interlocking, de balises en de Object Controllers (werkpakket 4.8a en 10.1). Op deze applicatiegegevens is hoofdstuk 8 van EN 50128 van toepassing (zie ook § 6.8).

De relatie tussen de "output documents" volgens § 8.3 van EN 50128 en de werkpakketten wordt gegeven in onderstaande tabel:

Nr.	Document	WP	Omschrijving
1)	Application Preparation Plan	4.8a	Ontwerp Treinbeveiligingsinstallaties
		10.1	Configureren ERTMS systeem
2)	Application Requirements Specification	3.3a	Opstellen System Requirement Specification
3)	Application Architecture and Design	3.3b	Opstellen Sub System Requirement Specification
		4.8a	Ontwerp Treinbeveiligingsinstallaties
		10.1	Configureren ERTMS systeem

4)	Application Test Specification	3.5a	Verificatie & Validatie
5)	Application Test Report	3.5a	Verificatie & Validatie
6)	Application Preparation Verification Report	3.5a	Verificatie & Validatie
7)	Source Code of Application Data/Algorithms	4.8a 10.1	Ontwerp Treinbeveiligingsinstallaties Configureren ERTMS systeem
8)	Application Data/Algorithms Verification Report	3.5a	Verificatie & Validatie

6.3 Systeemdefinitie

De systeemdefinitie [17] is het vertrekpunt voor de systeemontwikkeling en voor de RAM en Safety risicoanalyse. Hij moet voldoen aan de eisen uit § 2.1.2 van het CSM-REA risicobeheerproces en § 7.3.2.1 van EN 50126-1 [10].

6.4 Risicomanagement

Een uitgebreide toelichting op de risicoanalyse en -evaluatie wordt apart gegeven in het volgende hoofdstuk. Daar wordt ook ingegaan op de Hazard Log. Het gaat hierbij uitsluitend over de systeemveiligheid (spoorwegveiligheid).

6.5 (Sub) System Requirements Specifications

Parallel aan de analyse van de veiligheidsrisico's worden klanteisen (CRS) vertaald naar technische eisen (SRS) en worden RAM-, EMC-, Human Factors-, security, duurzaamheidsanalyses et cetera uitgevoerd. Resultante hiervan zijn systeem- en subsysteemeisen, die worden opgenomen in de SRS.

Overigens zijn dergelijke analyses al op uitgebreidere schaal uitgevoerd voor de Generieke Applicatie door het cluster OVEB. Die hebben geresulteerd in ontwerpvoorschriften, die naar verwachting al 80 – 95% van de eisen op Specific Application niveau bevatten.

Op het moment van schrijven is niet duidelijk of de ontwerpvoorschriften van de fabrikanten (zoals Thales) zijn verwerkt in de ontwerpvoorschriften van ProRail, of dat deze in parallel gelden. Ook is nog niet duidelijk in hoeverre de voorschriften op GA niveau door een AsBo worden ondersteund. Sweco gaat er echter van uit dat dit het geval zal zijn.

De System Requirements Specification (SRS) zal worden gevalideerd zoals omschreven in § 4.3.

Het Requirements Management wordt gedetailleerd omschreven in het Systems Engineering Werkplan [23].

6.6 Systeemontwerp

Het systeemontwerp zal worden gemaakt in de bij ProRail gebruikelijke stappen:

1. Functioneel Integraal Systeemontwerp (FIS);
2. Railverkeerstechnisch Ontwerp (RVTO);
3. Definitief Ontwerp (DO), en
4. Vraagspecificatie.

Deze stappen worden gedetailleerd omschreven in het Systems Engineering Werkplan[23].

Input voor het ontwerp is de data van het 'bestaande' spoor, zoals dat in 2025 zal bestaan. Dat is het huidige spoor, met daarbij alle voorziene wijzigingen tot 2025. De spoordata van de huidige situatie wordt door ProRail aangeleverd in IMX formaat; de voorziene wijzigingen tot 2025 dienen door Sweco zelf worden ingevoerd. De huidige data is echter niet gevalideerde data (met soms een grote onnauwkeurigheid), die nog vergeleken moet worden met andere bronnen, zoals OBE-bladen, luchtfoto's en visuele inspecties, om tot betrouwbare en dus veilige input data te komen.

6.7 Specific Application Safety Cases

De norm EN 50129 [13] geeft in § 7.4 de voorzieningen voor een Specific Application Safety Case (SASC). De volgende 2 aspecten moeten daarin aan de orde komen:

- a) *the application design, and*
- b) *the physical implementation.*

In overeenstemming met het Safety Plan van ProRail [14] (§ 2.6.3) zullen 2 aparte delen van de SASC worden geleverd:

- a) Een Application Design Safety Case (ADSC; voor fasen 1 t/m 6), en
- b) Een Physical Implementation Safety Case (PISC; voor fasen 7 t/m 9).

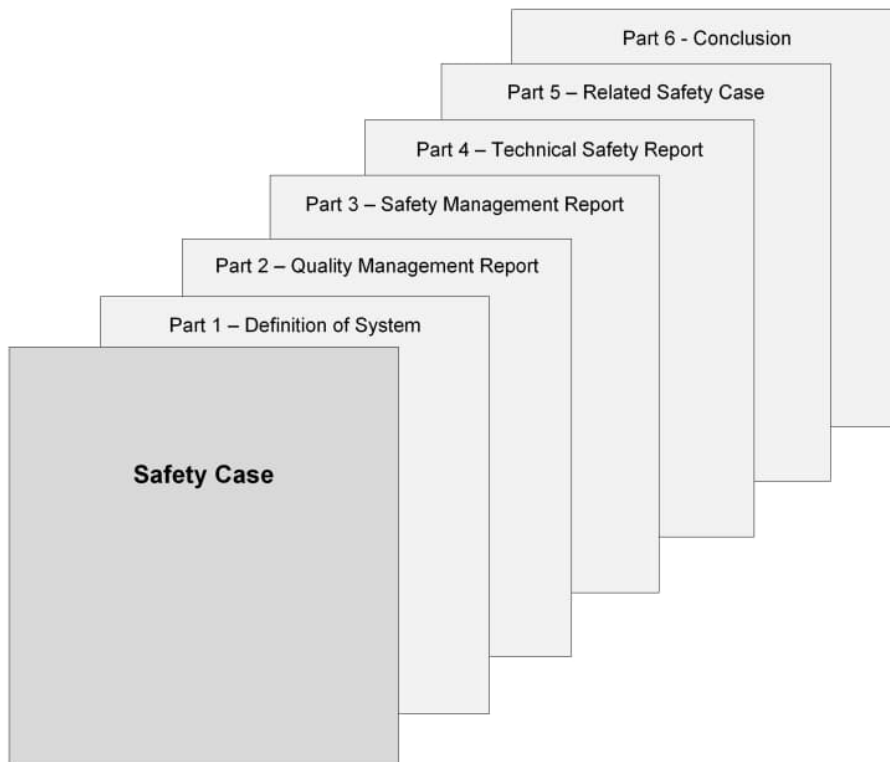
Zo'n 2-delige SASC wordt dus opgesteld voor elk van de 3 percelen:

4. Groningen – Eemshaven / Delfzijl;
5. Groningen – Bad Nieuwesches (Duitse grens) / Veendam;
6. Emplacement Groningen.

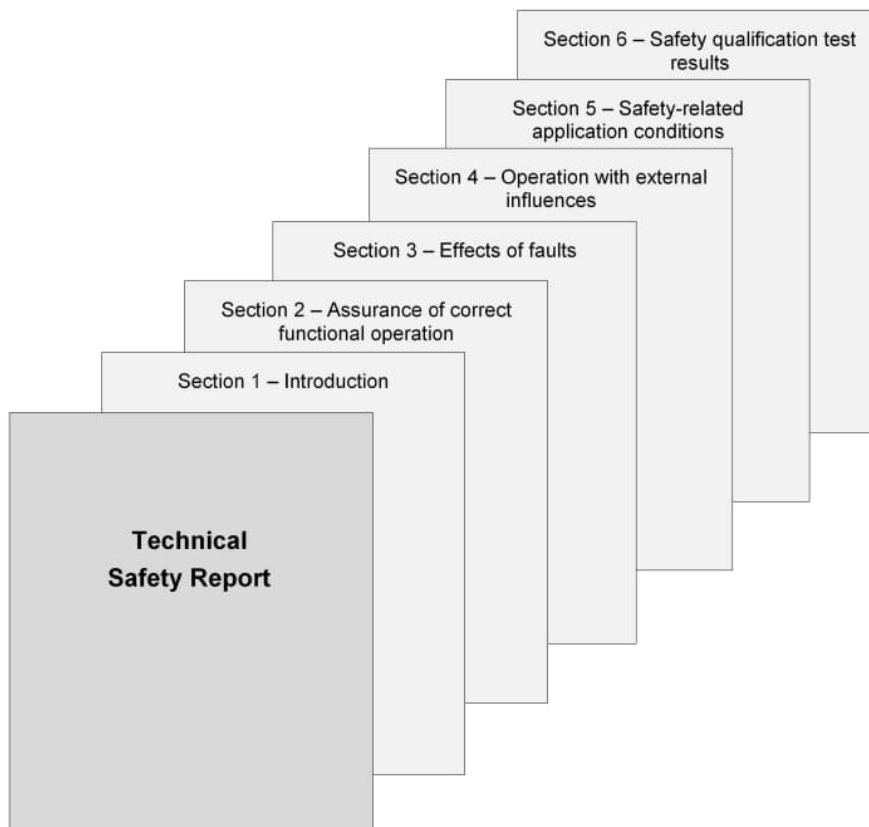
De scope van de Application Design Safety Case valt samen met Sweco's projectscope. Voor de Physical Implementation Safety Cases is Sweco afhankelijk van de fabrikanten en aannemer die test- en installatierapporten en andere bewijzen van veiligheid die moeten aanleveren. De precieze afspraken daarover zullen worden vastgelegd in een latere versie van dit plan.

6.7.1 Structuur van de Safety Cases

De Safety Case worden gestructureerd zoals omschreven in § 7.1 van de norm EN 50129:



Het Technical Safety Report wordt opgebouwd zoals omschreven in § 7.2 van EN 50129:



6.7.2 Iteraties van de SASC

Het is de bedoeling dat iedere SASC parallel aan de ontwerp- en realisatiewerkzaamheden wordt opgebouwd. Daarom zijn de volgende iteraties voorzien:

- SASC-ADSC:
 - o 1^e iteratie: bij het RVTO,
 - o 2^e iteratie: bij het DO;
- SASC-PISC:
 - o 1^e iteratie: na installatie, voor in-bedrijf-stelling;
 - o 2^e iteratie: na in-bedrijf-stelling.

Wanneer er meerdere versies van een RVTO of DO worden geleverd, wordt er bij iedere versie ook een versie van de SASC-ADSC voorzien.

6.7.3 Safety Argument

In de SASC zal een argument voor veiligheid worden gepresenteerd, dat wordt opgebouwd vanuit de volgende argumenten:

1. Het ERTMS systeem is voldoende veilig om operationeel gebruikt te worden ten behoeve van reizigers- en goederenvervoer;
 - 1.1. Alle hazards zijn gecontroleerd;
 - 1.1.1. Alle mogelijke hazards zijn geïdentificeerd.
 - 1.1.2. Mitigerende maatregelen voor iedere hazard zijn geformuleerd;
 - 1.1.3. Mitigerende maatregelen zijn verwerkt in eisen, ontwerp-, installatie- en testvoorschriften;
 - 1.1.4. Mitigerende maatregelen zijn geïmplementeerd;
 - 1.2. De toegepaste producten zijn voldoende veilig;
 - 1.2.1. De toegepaste producten voldoen aan de functionele eisen;
 - 1.2.2. De toegepaste producten voldoen aan de veiligheidseisen;
 - 1.2.3. De toegepaste producten zijn onafhankelijk beoordeeld door een AsBo, ISA en/of NoBo;
 - 1.3. Het ontwerp van het ERTMS systeem (FIS, RVTO, DO) voldoet aan de ontwerpvoorschriften en het systeem is volgens het ontwerp gebouwd;
 - 1.3.1. De ontwerp-, installatie en testvoorschriften bevatten alle SRACs vanuit de Generieke Applicatie;
 - 1.3.2. De ontwerp-, installatie- en testvoorschriften zijn geaccepteerd door een AsBo;
 - 1.3.3. De inputdata voor het ontwerp (o.a. locatie van het spoor, alignment) is correct en voldoende nauwkeurig;
 - 1.3.4. Er is aangetoond dat het ontwerp voldoet aan de ontwerpvoorschriften;
 - 1.3.5. Er is aangetoond dat het systeem is gebouwd en geconfigureerd volgens het ontwerp;
 - 1.3.6. Er is aangetoond dat het systeem is geïnstalleerd volgens de installatievoorschriften;
 - 1.4. De IMX data is correct;
 - 1.4.1. Angeleverde IMX data is correct en voldoende nauwkeurig;
 - 1.4.2. Gebruikte tools zijn geschikt voor hun toepassing (klasse T1, T2 of T3);
 - 1.4.3. Uitgeleverde IMX data is geverifieerd;
 - 1.5. Het systeem voldoet aan de systeemeisen;
 - 1.5.1. Er is aangetoond dat alle verificaties correct zijn uitgevoerd;
 - 1.5.2. Voor elke systeemeis (SRS) is een validatiemethode (test, analyse, inspectie, ...) en zijn er pass/fail criteria vastgesteld;

1.5.3. Voor elke systeemeis is er een positief validatieresultaat; eventuele afwijkingen zijn acceptabel.

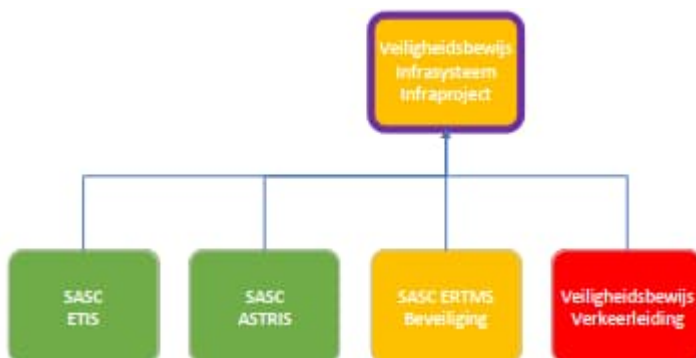
6.7.4 Verband met de GASC

De SASCs van Sweco zullen verwijzen naar de Generic Application Safety Case (GASC) van cluster OVEB voor het generieke systeem. Uitgangspunt daarbij is dat met de GASC en onderliggende documenten is aangetoond dat alle generieke hazards zijn gemitigeerd, hetzij in het generieke systeem zelf, hetzij door middel van Safety Related Application Conditions (SRACs) in ontwerp-, installatie-, test- en gebruiksvoorschriften, die door een AsBo worden ondersteund.

De GASC en het Independent Safety Assessment Report van OVEB's AsBo vormen dus een deel van de bewijsvoering van veiligheid. De verwachting is dat de GASC gecompliceerd en goedgekeurd wordt, parallel aan de ontwikkeling van de Early Deployment Lijn (EDL).

6.7.5 Verband met andere SASCs

Paragraaf 3.4.5.4 van ProRail's Veiligheidsmanagementplan ENL [14] geeft de structuur van de GPSCs, GASCs, SASCs en andere veiligheidsdossier weer. Onderstaand fragment daarvan geeft de SASCs weer:



De in geel weergegeven SASCs vallen onder de verantwoordelijkheid van cluster EUSI. Wat hier eenvoudig is weergegeven als *SASC ERTMS Beveiliging* bestaat in werkelijkheid uit de SASC-ADSC en de SASC-PISC van ieder van de 7 percelen. Deze worden door de IB's opgesteld.

Iedere SASC heeft raakvlakken met naburige percelen. Daarnaast moet het bewijs van veiligheid geleverd worden voor de configuratiedata van de centrale interlocking en de RBCs. De verantwoordelijkheid daarvoor ligt bij Thales. Mogelijk stelt Thales een eigen SASC op. Bij toevoeging van een perceel wijzigt de data. Er zijn daarom 7 iteraties voorzien.

Het opstellen en op elkaar aan laten sluiten van al deze Safety Cases vereist een nauwe samenwerking tussen de Safety Managers van ProRail, Arcadis, Nexus, Sweco en eventueel Thales.

Het Veiligheidsbewijs infrasysteem Infraproject is overkoepelend en wordt door ProRail opgesteld. Mogelijk vraagt ProRail hiervoor nog assistentie van de IB's maar dat is op dit moment niet in opdracht gegeven.

6.8 Application Preparation Plan

In het project hebben we te maken met 4 systeemelementen die met applicatie-data geconfigureerd worden:

- IXL;
- RBC;
- Balises;
- Object Controllers.

De (wettelijk verplichte) norm EN 50128 stelt in hoofdstuk 8 eisen aan de ontwikkeling van deze applicatiedata. Een eerste eis is dat een Application Preparation Plan wordt opgesteld. De eisen hieraan staan in § 8.4.1 van de norm.

Het opstellen van het Application Preparation Plan valt onder de verantwoordelijkheid van de Lead Engineers.

6.9 Tools

EN 50128 definieert 3 klassen tools:

- T1 – *generates no outputs which can directly or indirectly contribute to the executable code (including data) of the software;*
- T2 – *supports the test or verification of the design or executable code, where errors in the tool can fail to reveal defects but cannot directly create errors in the executable software;*
- T3 – *generates outputs which can directly or indirectly contribute to the executable code (including data) of the safety related system.*

Het is in dit project de bedoeling dat trackdata aangeleverd wordt in IMX formaat. De tools hiervoor zijn nog in ontwikkeling. Deze zullen (deels) als T2 of T3 geclassificeerd worden. De eisen aan T2 en T3 tools staan in § 6.7 van EN 50128.

Zoals gezegd in § 4.1 ontwikkelt Sweco de tools voor het werken met IMX data (zowel ontwerpen als verifiëren) zelf, buiten de projecten EKB en ENL om. Het aantonen dat de tools voldoen aan de eisen voor T2 of T3 tools valt dus buiten de scope het project ENL.

In het Application Preparation Plan moet echter wel onderbouwd worden dat de tools die in het ENL project gebruikt worden daarvoor geschikt zijn.

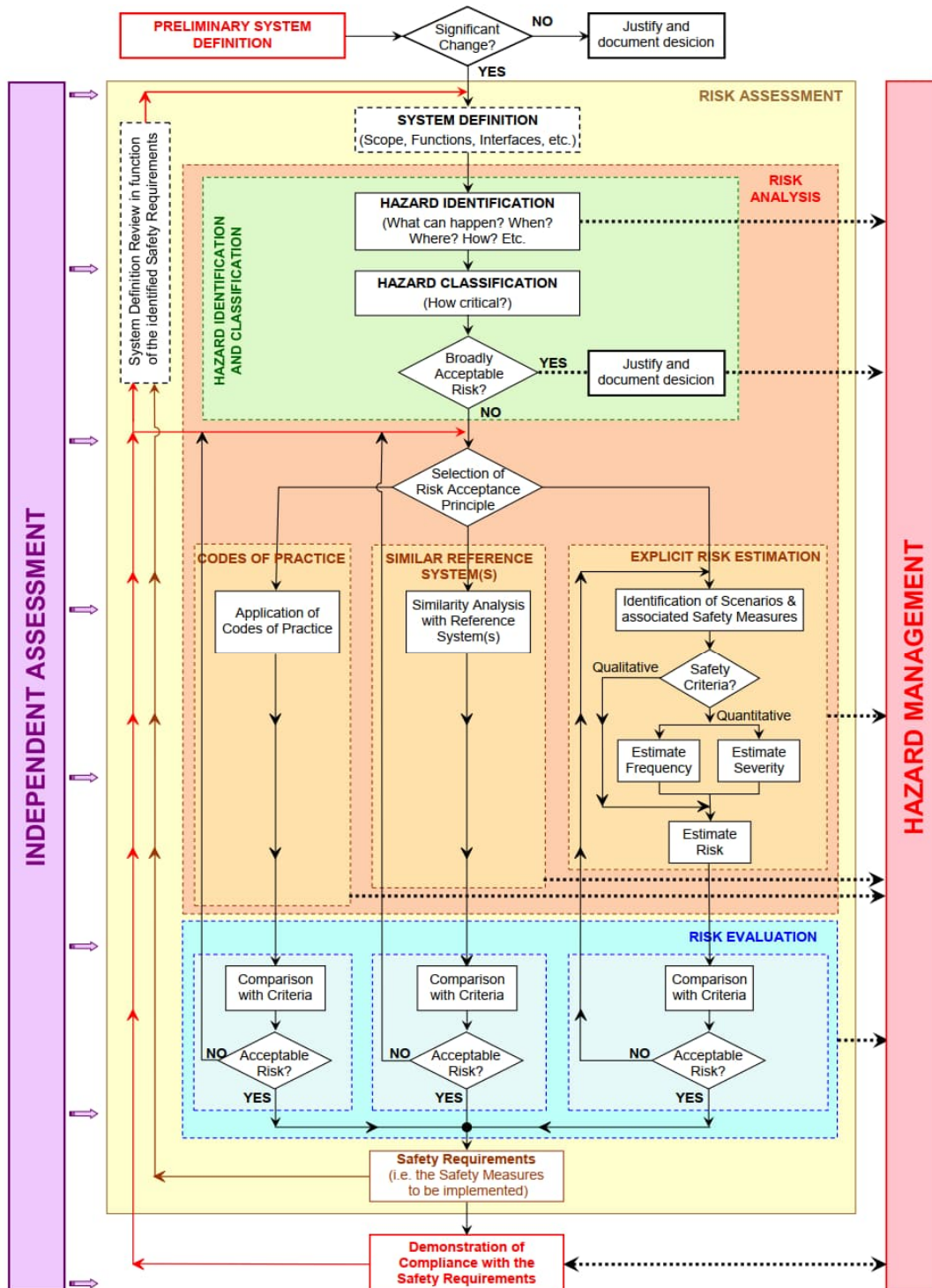
6.10 Decommissioning bestaande systemen

Na het in bedrijf stellen van de nieuwe systemen moeten de oude systemen (de Automatische Trein Beïnvloeding - Nieuwe Generatie (ATB-NG), de PrikSpanningSpoorStroomLoop (PSSSL) componenten, de Vital Processor Interlocking (VPI's), assentelsystemen en licht- en bordseinen) worden verwijderd. Het managen van de (eventuele) daarbij behorende spoorwegveiligheidsrisico's behoort tot de scope van het project.

7 Hazard management

Dit hoofdstuk gaat in op alle aspecten van het hazard management en de beoordeling van de veiligheid door een Assessment Body.

Voor het hazard management wordt een proces doorlopen dat zowel voldoet aan EN 50126 [10] als aan CSM-REA [3].



Omdat lang niet iedereen regelmatig bezig is met hazard management wordt de materie in dit hoofdstuk uitgebreider toegelicht. Deze extra informatie staat in een grijs kader en kan door een ervaren lezer worden overgeslagen.

7.1 Wat is een hazard?

Het begrip “hazard” is lang niet voor iedereen duidelijk. Vaak worden hazard en oorzaken van hazards door elkaar gehaald. Daarom volgt hier eerst meer uitleg.

Een hazard is een gevaarlijke situatie; een situatie waaruit schade of een ongeval uit zou kunnen ontstaan. Bijvoorbeeld: glad spoor.

Een hazard heeft altijd een oorzaak (of meerdere oorzaken) en mogelijke gevolgen. In dit voorbeeld is een oorzaak: blaadjes op de rails. Mogelijke gevolgen zijn:

- De machinist anticipeert op glad spoor en weet de trein voor het rode sein tot stilstand te brengen;
- De trein passeert een rood sein maar stopt nog voor het wissel;
- De trein passeert een rood sein en schiet door over het wissel, waar op dat moment geen andere trein (op af) rijdt;
- De trein passeert een rood sein en schiet door over het wissel, waar op dat moment een andere trein rijdt.

Een hazard treedt op aan de buitengrens van een systeem: als er 230 Volt op een ader in een snoer staat is dat geen gevaarlijke situatie; als er 230 Volt op de buitenkant van je wasmachine staat is dat wel een hazard.

7.2 Hazard identificatie

Hazards kunnen op verschillende manieren worden geïdentificeerd, bijvoorbeeld in een HAZID workshop maar ook tijdens het ontwerpproces.

Een HAZID workshop is een brainstormsessie met deelnemers met zo veel mogelijk verschillende achtergronden (een multidisciplinair team): de klant, ontwerpers, aannemers/installateurs, gebruikers, onderhoudsmonteurs, materiaaldeskundige, calamiteitenorganisatie, een leek die slimme vragen stelt, enzovoort.

Een HAZID workshop kan een vrije brainstorm zijn, maar kan ook op een gestructureerde manier aangepakt worden. Dan wordt er bij elke functionele en niet functionele interface van een systeem nagegaan wat er mis kan gaan. Gidswoorden daarbij zijn bijvoorbeeld: te veel, te weinig, te vroeg, te laat, omgekeerd.

Uitgangspunt bij dit project is dat alle generieke hazards al geïdentificeerd zijn door het cluster OVEB bij de ontwikkeling van de Generieke Applicatie. Waar er in dit project dan nog naar moet worden gekeken zijn gevaarlijke situaties die specifiek zijn voor een locatie op een spoorlijn of emplacement of die ontstaan door de wijzigingen.

Een voorbeeld hiervan is een station met te smalle perrons. De huidige interlocking werkt zo dat een trein nu altijd op een ‘stop’ tonend sein binnenkomt. Hij nadert en vertrekt dus altijd met lage snelheid. Met de introductie van ETCS wordt het mogelijk dat een (goederen-) trein het station met baanvaksnelheid passeert. Dit kan gevaarlijk zijn voor reizigers op het perron, dat smaller is dan tegenwoordig wordt geëist.

Omdat de scope beperkt is wordt in eerste instantie per perceel 1 interne HAZID workshop voorzien, met als input de systeemdefinitie. Deze zal voorbereid worden door de Safety Manager en alle interne disciplines zullen daarvoor uitgenodigd worden.

Daarnaast worden er door ProRail bredere HAZID workshops georganiseerd, waarin bijvoorbeeld ook de centrale systemen van Thales, de verkeersleidingssystemen van RIGD Loxia (Post 21) en de verkeersleiding zelf in scope zijn.

Tijdens het ontwerpproces (FIS, RVTO, DO) worden er door de ontwerpers vaak tal van hazards of oorzaken van hazards ontdekt. De Safety Manager zal daarom regelmatig met de ontwerpers mini HAZID workshops houden om deze door te nemen en vast te leggen (voor zover dat nog niet gebeurd is).

Alle geïdentificeerde hazards worden vastgelegd in een Hazard Log (zie verderop).

7.2.1 Oorzaken en gevolgen

Als aanzet naar de hazard classificatie worden de mogelijke oorzaken en gevolgen van iedere hazard geanalyseerd en vastgelegd in de hazard log.

Hierbij is het van belang de mogelijke scenario's zo goed mogelijk te beschrijven om die goed te begrijpen. Dat is niet alleen van belang om de kansen en mogelijke gevolgen goed te begrijpen, het is ook van belang op om in een latere stap de juiste mitigaties te kunnen bepalen.

Dus niet als mogelijk gevolg: "aanrijding", maar de verschillende scenario's zoals in het voorbeeld in § 7.1.

Voor iedere hazard worden tenminste 2 scenario's geanalyseerd:

1. Het meest waarschijnlijke scenario;
2. Het realistische worst-case scenario.

7.3 Hazard classificatie

Doel van de hazard classificatie is om te bepalen hoe acceptabel hazards zijn, oftewel hoe groot de risico's zijn. Dit gebeurt in het proces twee keer: voor en na het definiëren veiligheidseisen en/of mitigerende maatregelen. In het schema hierboven zien we de eerste keer in het groene blok; de tweede keer bij de 'risk evaluation' in het blauwe blok.

Bij hazard classificatie worden hazards ingedeeld in klassen, bijvoorbeeld:

- Zeer hoog – het risico is onacceptabel;
- Hoog – het risico moet worden gereduceerd;
- Gemiddeld – het risico zou verder verlaagd moeten worden;
- Laag – het risico is acceptabel.

Voor hazard classificatie zijn 2 stappen nodig:

1. Het bepalen van de kans en ernst;
2. Het bepalen van de risicoklasse.

Aan de hand van de oorzaken en gevolgen die bij de vorige stap bepaald zijn, wordt de kans op het optreden van een hazard en de kans op een ongewenste gebeurtenis ingeschat, evenals de ernst van de gevolgen. Bij de initiële hazard classificatie (in het groene blok) mag rekening worden gehouden met

bestaande veiligheidsmaatregelen. De bestaande veiligheidsmaatregelen zijn vastgelegd in de systeemdefinitie.

Kans wordt uitgedrukt in termen van kans per uur of van eens per periode (uur / week / maand / jaar / etc.). De ernst wordt uitgedrukt in aantallen gewonden en/of doden. Zie ook het voorbeeld in bijlage 3.

Voor de kans en ernst wordt gebruik gemaakt van de risicomatrix van ProRail, die langs de ene as de kans optreden en langs de andere as de ernst van de gevolgen weergeeft. Hierbij moet dus gekozen worden uit 1 van de stappen langs iedere as.

Als de kans en de ernst bepaald zijn dan kan in de matrix de klasse worden uitgelezen.

In de meeste gevallen zijn de kansen en de ernst van scenario's niet exact te bepalen. Het is nou eenmaal niet mogelijk om deze van alle hazards met wetenschappelijke experimenten te bepalen. Daarom moeten deze zo goed mogelijk worden ingeschat. Voor de classificatie maakt het in veel gevallen niet uit of men een stapje hoger of lager kiest. Bij twijfel dient altijd van de grotere kans en het ernstiger gevolg te worden uitgegaan.

7.4 Algemeen aanvaarbare risico's

Als bij de initiële hazard classificatie, rekening houdend met bestaande veiligheidsmaatregelen, het risico wordt geclassificeerd als 'Laag' dan is er geen verdere risicoanalyse nodig. De argumenten voor de classificatie worden vastgelegd in de Hazard Log.

Het is dan natuurlijk wel belangrijk dat geborgd wordt dat bestaande veiligheidsmaatregelen in de SRS terecht komen. Als dat het geval is dan wordt de hazard gesloten.

7.5 Risicoaanvaardingsbeginselen

Zowel volgens EN 50126 als volgens CSM-REA moet er gekozen worden uit 3 risicoaanvaardingsbeginselen:

1. de toepassing van praktijkcodes;
2. een vergelijking met soortgelijke systemen;
3. een expliciete risico-inschatting.

Een "praktijkcode" wil zeggen dat er ergens algemeen aanvaarde normen of handleidingen voor bestaan. Door een AsBo ondersteund ontwerpvoorschrift van ProRail of een fabrikant kunnen ook als een praktijkcode worden beschouwd.

Wanneer de hazard al bij een eerder project geïdentificeerd was, dan kunnen de veiligheidsmaatregelen en -eisen van dat project overgenomen worden. Daarbij moet wel aangetoond worden dat de context, kansen en mogelijke gevolgen vergelijkbaar zijn.

Het expliciet analyseren van de risico's kan altijd (maar kan veel werk betekenen).

Bovenstaande volgorde is ook de volgorde van voorkeur. Het toepassen van een bepaalde norm is nou eenmaal de gemakkelijkste oplossing. Het overnemen van eisen van een vergelijkbaar project wordt al ingewikkelder en het van

scratch af aan ontwikkelen van afdoende veiligheidseisen en -maatregelen kost de meeste moeite.

Veiligheidsmaatregelen en -eisen kunnen ingedeeld worden in 2 groepen: kans verlagende maatregelen en gevolg beperkende maatregelen. In de Hazard Log worden deze onderscheiden.

7.6 Risico evaluatie

Nadat de veiligheidsmaatregelen en -eisen op bovenstaande manier zijn bepaald wordt geëvalueerd of het restrisico aanvaardbaar is. Daarbij worden de restrisico's opnieuw geclassificeerd, zoals omschreven in § 7.3.

Als het restrisico geclassificeerd is als 'Zeer hoog' of 'Hoog' dan zijn aanvullende maatregelen noodzakelijk en moet de vorige stap opnieuw worden doorlopen. Daarbij kan er uit een ander risicoaanvaardingsbeginsel worden gekozen.

Als het restrisico geclassificeerd wordt als 'Gemiddeld' dan moet geanalyseerd worden of het risico nog tegen redelijke kosten verder gereduceerd kan worden. Alleen als deze kosten hoog zijn in verhouding tot de risicowinst, dan kan het acceptabel zijn geen verdere maatregelen te nemen.

7.7 Hazard Log

De Hazard Log wordt opgezet als module in de gezamenlijke Relatics van ENL (die wordt gefaciliteerd door Arcadis).

De Hazard Log bevat velden voor alle bovengenoemde informatie.

Hij is toegankelijk voor alle designers; zij kunnen daar hazards en mitigaties in vastleggen.

Hazards krijgen een status. De statussen moeten nog worden afgestemd met de andere IB's maar voorzien zijn in ieder geval:

- Open – er is een hazard geïdentificeerd en deze is in behandeling;
- Generiek – de hazard is al geïdentificeerd voor de Generieke Applicatie en mitigaties zijn daar vastgesteld;
- Gereed – de restrisico's zijn geëvalueerd als 'Laag', of als 'Gemiddeld', waarbij het restrisico redelijkerwijs niet verder gereduceerd kan worden;
- Gesloten – de veiligheidsmaatregelen en -eisen zijn vastgelegd in de SRS.

Als de restrisico's aanvaardbaar zijn en veiligheidsmaatregelen en -eisen zijn vastgelegd in de SRS dan wordt de hazard gesloten. Vanaf dat moment worden de eisen meegenomen in het ontwerp en in de realisatie en wordt met verificatie en validatie geborgd dat aan deze veiligheidseisen wordt voldaan. Daarom hoeft dat niet via de Hazard Log gemonitord te worden.

Alleen de Safety Manager kan hazards sluiten.

7.8 Safety audits

De Safety Manager zal interne safety audits organiseren en uitvoeren.

Een voorlopig auditprogramma is opgenomen in Bijlage 3.

7.9 Independent Safety Assessment

Een onafhankelijke derde party, een Assessment Body (AsBo), moet controleren of aan de eisen van CSM-REA is voldaan: zowel of het proces correct doorlopen is als of het systeem veilig in gebruik kan worden genomen.

Ongeveer hetzelfde eisen de CENELEC standaarden. Alleen wordt daar gesproken over een Independent Safety Assessor en is het toetskader niet CSM-REA maar EN 50126, EN 50128 en EN 50129.

Zoals gezegd is het zo dat wanneer er aan de CENELEC standaarden wordt voldaan er automatisch ook aan de eisen van CSM-REA wordt voldaan. Bovendien eist de TSI Besturing en Seingeving [4] dat het “CENELEC Independent Safety Assessment” wordt uitgevoerd door een AsBo. Er is dus sprake van 1 geïntegreerd Independent Safety Assessment.

De AsBo wordt gecontracteerd door ProRail, middels een Europese aanbestedingsprocedure. Naar verwachting kan het contract in augustus 2023 worden gesloten.

Dit is een lastige situatie omdat de plannen, FIS en RVTO ruim voor die tijd gereed zijn en eigenlijk direct beoordeeld zouden moeten worden. Dit brengt het risico met zich mee dat deze (en ook het DO) in een laat stadium nog gewijzigd moeten worden.

8 Compliance management

Dit hoofdstuk gaat in op het aantonen van de compliance met de TSI's en de externe beoordeling daarvan door een Notified Body.

Zoals gesteld in § 2.3 wordt compliance met andere wetgeving gemanaged door middel van opnamen van de wettelijke eisen in de SRS en het volgen van het normale ontwerpproces, verificatie en validatie. In dit hoofdstuk komt dat verder niet aan de orde.

8.1 TSI compliance

De TSI stelt eisen op 2 niveaus:

1. Op productniveau – 'Interoperability Constituents' genoemd;
2. Op systeemniveau – 'Subsysteem' (van het Europees spoorwegsysteem of van een spoorlijn) genoemd.

In dit project zijn enkele producten relevant: Eurobalises, Lineside Electronic Units, Stop Marker Boards (SMBs) (en eventueel andere marker boards), assentellers en RBCs. Marker Boards zijn overigens in de huidige TSI niet gedefinieerd als Interoperability Constituent maar ze moeten wel aan de TSI eisen voldoen.

Interoperability Constituents moeten aan de TSI en alle andere wettelijke eisen voldoen op het moment dat ze "op de markt geplaatst" worden. Dat is: op het moment dat de fabrikant ze levert. Het concept van "op de markt plaatsen" heeft in de Europese wetgeving een speciale betekenis. Het is van toepassing op individuele producten / systemen (zie de "Blauwe Gids" [9]). De fabrikant is hiervoor verantwoordelijk. Producten moeten geleverd worden met een conformiteitsverklaring die is gebaseerd op 'EG' certificaten die zijn afgegeven door hun NoBo.

Hierbij moet worden aangetekend dat op dit moment wordt gewerkt volgens ETCS Baseline 3 Release 2. Echter, op dit moment zijn ook de volgende versies van de TSI's in een ver gevorderd stadium. Naar verwachting moeten de Interoperability Constituents tegen de tijd dat het systeem gerealiseerd wordt, voldoen aan de eisen voor Baseline 4 (en mogelijk zelfs 5). Er wordt waarschijnlijk ook een overgangstermijn voorzien en er is normaal gesproken dispensatie voor project in een ver ontwikkelingsstadium. Wat de impact is op het project moet worden geëvalueerd wanneer de nieuwe TSI's gepubliceerd zijn.

Op het Subsysteem niveau moet alleen nog aangetoond worden dat de producten op een juiste manier worden toegepast. Bijvoorbeeld dat balises en SMB's op de juiste plaatsen liggen/staan en dat balises de juiste berichten aan een passerende trein geven.

Uitgangspunt hierbij is dat het cluster OVEB aantoont dat alle relevante TSI-eisen ofwel zijn geadresseerd op het Generic Application (GA) niveau ofwel zijn verwerkt in de ontwerpvoorschriften, testvoorschriften et cetera. Op projectniveau moet dan alleen nog aangetoond worden dat aan deze voorschriften is voldaan.

8.2 EG Verificatie door een NoBo

Dat een Substelsysteem aan alle eisen (inclusief de veiligheidseisen) voldoet moet worden bevestigd door een onafhankelijke derde partij, een Notified Body (NoBo).

De NoBo wordt gecontracteerd door ProRail, middels een Europese aanbestedingsprocedure. Omdat er de nodige overlap bestaat tussen de assessment scope van de AsBo (zie § 7.9) en de assessment scope van de NoBo wordt door ProRail 1 marktpartij gecontracteerd voor beide assessments.

Wat een NoBo voor een Baansubstelsysteem moet controleren staat in tabel 6.3 van de TSI Besturing en Seingeving. Deze tabel is hieronder overgenomen, opdat voor het hele projectteam duidelijk is welke informatie aan de NoBo verstrekt moet worden.

Het te leveren bewijs komt voor een deel van de Generieke Applicatie, die onder cluster OVEB wordt ontwikkeld, en voor een deel van de Specifieke Applicaties, die in de ERTMS projecten worden ontwikkeld onder cluster EUSI. De insteek is echter dat de NoBo voor de GA en de NoBo voor de SA's los van elkaar worden gecontracteerd door OVEB, respectievelijk het ENL project van ProRail. De verdeling van te leveren en te beoordelen bewijsvoering moet nog in detail worden afgestemd tussen OVEB en EUSI en moet nog worden geaccepteerd door beide NoBo's.

De insteek is verder:

- EG- typeonderzoek (module SB) voor de GA (OVEB);
- EG-keuring op basis van productkeuring (module SF) voor de SA's (EUSI).

Aspect	Wat te beoordelen	Ondersteunend bewijs
Gebruik van interoperabiliteits-onderdelen	Controleren of alle interoperabiliteitsonderdelen die in het subsysteem moeten worden geïntegreerd door een EG-verklaring van conformiteit en het overeenkomstige certificaat zijn gedekt	Aanwezigheid en inhoud van documenten
	Controleren hoe de beperkingen op het gebruik van interoperabiliteitsonderdelen zich verhouden tot de eigenschappen van het subsysteem en van de omgeving	Effectbeoordeling aan de hand van documenten
	Voor interoperabiliteitsonderdelen die zijn gecertificeerd volgens oudere versies van de TSI Besturing en seingeving controleren of het certificaat nog altijd overeenstemming waarborgt met de eisen van de momenteel geldende TSI	Effectbeoordeling door vergelijking van specificaties waarnaar in de TSI wordt verwezen en certificaten van de interoperabiliteitsonderdelen
Gebruik van trein-detectie-systemen	Controleren of de geselecteerde types voldoen aan de eisen van de TSI Besturing en seingeving	Documentcontrole

	— fundamentele parameters 4.2.10 en 4.2.11	
Integratie van interoperabiliteitsonderdelen in het subsysteem	Controleren of de interne interfaces van het subsysteem correct zijn geïnstalleerd en correct werken — fundamentele parameters 4.2.5 en 4.2.7	Controles volgens specificaties
	Controleren of de extra functies (die niet in deze TSI worden vermeld) de verplichte functies niet beïnvloeden	Effectbeoordeling
	Controleren of de waarden van de ETCS ID's binnen het toegelaten bereik vallen en, indien vereist door deze TSI, uniek zijn — fundamentele parameter 4.2.9	Ontwerpspecificaties controleren
Integratie met infrastructuur	Controleren of de apparatuur correct is geïnstalleerd — fundamentele parameters 4.2.3, 4.2.4 en installatievoorschriften van de fabrikant	Resultaten van controles (volgens specificaties waarnaar wordt verwezen in de fundamentele parameters en de installatievoorschriften van de fabrikant)
	Controleren of het baansubsysteem besturing en seingeving compatibel is met de omgeving van de baanapparatuur — fundamentele parameter 4.2.16	Documentcontrole (controleren hoe de certificaten van interoperabiliteitsonderdelen en mogelijke integratiemethodes zich verhouden tot de eigenschappen van de baanapparatuur)
Integratie met seinapparatuur langs het spoor	Controleren of alle door de toepassing vereiste functies zijn geïmplementeerd volgens de specificaties waarnaar in deze TSI wordt verwezen — fundamentele parameter 4.2.3	Documentcontrole (ontwerpspecificatie van de aanvrager en certificaten van interoperabiliteitsonderdelen)
	Controleren of de parameters correct zijn geconfigureerd (Eurobalise-telegrammen, RBC-berichten, positie van markeerborden enz.)	Documentcontrole (controleren hoe de parameters zich verhouden tot de eigenschappen van de baanapparatuur voor seingeving)
	Controleren of de interfaces correct zijn geïnstalleerd en correct werken	Keuring van het ontwerp en tests volgens de informatie van de aanvrager
	Controleren of het baansubsysteem besturing en seingeving correct werkt volgens de	Keuring van het ontwerp en tests volgens de

	informatie bij de interfaces met baanapparatuur voor seingeving (bv. Correcte aanmaak van Eurobalise-telegrammen door een LEU of van berichten door RBC)	informatie van de aanvrager
Integratie met trein-subsystemen besturing en seingeving en met rollend materieel	Controleren of de GSM-R een goede dekking biedt — fundamentele parameter 4.2.4	Metingen ter plaatse
	Controleren of de treindetectiesystemen voldoen aan de eisen van deze TSI — fundamentele parameter 4.2.10	Metingen ter plaatse
	Controleren of de treindetectiesystemen voldoen aan de eisen van deze TSI — fundamentele parameters 4.2.10 en 4.2.11	Bewijs van bestaande installaties controleren (voor systemen die al in gebruik zijn); tests uitvoeren volgens de standaarden voor nieuwe types
	Controleren of alle door de toepassing vereiste functies zijn geïmplementeerd volgens de specificaties waarnaar in deze TSI wordt verwezen — fundamentele parameters 4.2.3, 4.2.4 en 4.2.5	Rapporten van de operationele testscenario's als bepaald in punt 6.1.2 met verschillende gecertificeerde treinsubsystemen besturing en seingeving. Het rapport moet vermelden welke operationele scenario's zijn getest, welke treinapparatuur is gebruikt en of de tests zijn uitgevoerd in laboratoria, op testlijnen of in reële situaties.
Betrouwbaarheid, beschikbaarheid, onderhoudbaarheid, veiligheid (RAMS)	Controleren of er wordt voldaan aan de veiligheidseisen — fundamentele parameter 4.2.1	Toepassing van procedures als bepaald in de gemeenschappelijke veiligheidsmethode
	Controleren of kwantitatieve doelstellingen voor betrouwbaarheid worden behaald — fundamentele parameter 4.2.1	Berekeningen
	Controleren of aan de onderhoudseisen wordt voldaan — punt 4.5.2	Documentcontrole
Integratie met trein-subsystemen besturing en seingeving en met rollend materieel: tests	Het gedrag van het subsysteem testen onder zoveel verschillende operationele omstandigheden als redelijkerwijs haalbaar is (bv. Treinsnelheid, aantal treinen op de lijn,	Rapporten van testritten. Vermeld in het certificaat welke omstandigheden zijn getest en welke normen zijn toegepast.

onder operationele omstandigheden	weersomstandigheden). Met de test moet kunnen worden gecontroleerd: 1. of de treindetectiesystemen correct werken — fundamentele parameters 4.2.10 en 4.2.11 2. of het baansubstelsysteem besturing en seingeving compatibel is met de omgeving van de baanapparatuur — fundamentele parameter 4.2.16 Deze tests vergroten ook de zekerheid over het gebrek aan systematische storingen. Deze tests sluiten alle tests uit die in eerdere stadia werden uitgevoerd: tests op het niveau van de interoperabiliteitsonderdelen en tests op het subsysteem in een gesimuleerde omgeving moeten in aanmerking worden genomen.	De informatie in het certificaat en de begeleidende documentatie moet toereikend zijn om te kunnen bepalen welke controles nog moeten worden uitgevoerd alvorens een treinsubstelsysteem op een bepaalde route in gebruik te nemen. Wanneer in operationele omstandigheden aanvullende tests worden uitgevoerd met een subsysteem waarvoor reeds een EG-keuringsverklaring is afgegeven, kan de informatie betreffende die tests op verzoek van de aanvrager worden toegevoegd als aanvulling op de documentatie die het certificaat vergezelt.
---	---	---

8.3 TSI compliance dossier

Het project moet aantonen dat het ETCS systeem en het assentelsysteem voldoen aan de eisen van de TSI Besturing en Seingeving [4] (werkpakketten 3.5b en 9.1).

Het uitgangspunt hierbij is dat het cluster OVEB aantoont dat alle relevante TSI-eisen ofwel zijn geadresseerd op het GA niveau ofwel zijn verwerkt in de ontwerpvoorschriften, testvoorschriften et cetera. Op projectniveau moet alleen nog aangetoond worden dat aan deze voorschriften is voldaan.

Het opstellen van een TSI-verificatiematrix (WP 3.5b) en het opstellen van een TSI compliance dossier (WP 9.1) is dus niet aan de orde.

Compliance met de TSI-eisen wordt aangetoond als wordt aangetoond dat aan de ontwerpvoorschriften (met name OVS60040-2), productspecificaties, installatievoorschriften, testvoorschriften is voldaan. Het bewijs hiervoor wordt geleverd door middel van verificatie en validatie, zoals omschreven in § 4.2 en § 4.3.

Het te leveren bewijs van compliance overlapt dus grotendeels met het bewijs van veiligheid aangezien verificatie- en validatierapporten worden opgenomen in de SASC's. Te zijner tijd zal beoordeeld worden of deze SASC's al al het bewijs van compliance leveren of dat er nog een aanvullende informatie in een aanvullend dossier moet worden opgenomen.

8.4 Technisch Dossier

Punt 2.4 van de EG-keuringsprocedure voor subsystemen (bijlage IV bij de Interoperabiliteitsrichtlijn [1]) somt op wat het technisch dossier bij de EG-keuringsverklaring (van ProRail) dient te bevatten:

- a) de technische kenmerken van het ontwerp, met inbegrip van de voor het betrokken subsysteem relevante algemene en detailplannen zoals die worden uitgevoerd, elektrische en hydraulische schema's, schema's van de besturingscircuits, een voor de uitgevoerde conformiteitsbeoordeling voldoende gedetailleerde beschrijving van de geautomatiseerde systemen, handleidingen voor bediening en onderhoud enz.;
- b) een lijst van de in het subsysteem verwerkte interoperabiliteitsonderdelen als bedoeld in artikel 4, lid 3, onder d);
- c) de in artikel 15, lid 4, bedoelde dossiers, samengesteld door elke aangemelde instantie die betrokken is bij de keuring van het subsysteem, die het volgende bevatten:
 - kopieën van de EG-keuringsverklaringen en in voorkomend geval de voor de interoperabiliteitsonderdelen als bedoeld in artikel 4, lid 3, onder d), opgestelde EG-verklaringen van geschiktheid voor gebruik, waar nodig, vergezeld van de desbetreffende berekeningen en een kopie van de verslagen van de tests en onderzoeken die op grond van de gemeenschappelijke technische specificaties door de aangemelde instanties zijn uitgevoerd;
 - de beschikbare TKV die het keuringscertificaat vergezellen, met inbegrip van het resultaat van de door de aangemelde instantie uitgevoerde keuring met betrekking tot de geldigheid van de TKV;
 - het keuringscertificaat, vergezeld van de desbetreffende berekeningen en ondertekend door de met de keuring belaste aangemelde instantie, waarin wordt bevestigd dat het subsysteem in overeenstemming is met de vereisten van de toepasselijke TSI('s) en met vermelding van een eventueel tijdens de uitvoering van de werkzaamheden gemaakt voorbehoud dat niet is ingetrokken; het keuringscertificaat dient tevens vergezeld te gaan van de inspectie- en auditrapporten die de aangemelde instantie in het kader van haar opdracht heeft opgesteld overeenkomstig de punten 2.5.2 en 2.5.3;
- d) de overeenkomstig andere rechtshandelingen van de Unie afgegeven keuringscertificaten;
- e) wanneer op grond van artikel 18, lid 4, onder c), en artikel 21, lid 3, onder c), een beoordeling vereist is van de veilige integratie, moet het relevante technisch dossier het (de) beoordelingsverslag(en) bevatten betreffende de in artikel 6, lid 3, van Richtlijn 2004/49/EG van het Europees Parlement en de Raad (1) bedoelde gemeenschappelijke GVM's inzake risicobeoordeling.

Het technisch dossier bij de EG-keuringsverklaring wordt opgesteld door de aanvrager, dus door ProRail. Ten behoeve van dit technische dossier levert Sweco aan ProRail:

- Alle genoemde documenten onder a), voor zover ze betrekking hebben op de Specifieke Applicaties; de documenten die betrekking hebben op de Generieke Applicatie worden geleverd door het cluster OVEB;
- De NoBo technische dossiers als genoemd onder c), voor zover ze betrekking hebben op de Specifieke Applicaties; de NoBo technische

dossiers die betrekking hebben op de Generieke Applicatie worden geleverd door het cluster OVEB;

- Het Safety Assessment Report van de SA-AsBo, zoals genoemd onder e); het Safety Assessment Report van de GA-AsBo wordt geleverd door het cluster OVEB.

De onder b) en d) genoemde stukken worden geleverd door het cluster OVEB.

Referenties

Wetgeving

- [1] Richtlijn (EU) 2016/797 van het Europees parlement en de Raad van 11 mei 2016 betreffende de interoperabiliteit van het spoorwegsysteem in de Europese Unie
- [2] Richtlijn (EU) 2016/798 van het Europees parlement en de raad van 11 mei 2016 inzake veiligheid op het spoor
- [3] Uitvoeringsverordening (EU) Nr. 402/2013 van de Commissie van 30 april 2013 betreffende de gemeenschappelijke veiligheidsmethode voor risico-evaluatie en -beoordeling en tot intrekking van Verordening (EG) nr. 352/2009
- [4] Verordening (EU) 2016/919 van de Commissie van 27 mei 2016 betreffende de technische specificatie inzake interoperabiliteit van de subsystemen besturing en seingeving van het spoorwegsysteem in de Europese Unie
- [5] Uitvoeringsverordening (EU) 2019/773 van de Commissie van 16 mei 2019 betreffende de technische specificaties inzake interoperabiliteit van het subsysteem exploitatie en verkeersleiding van het spoorwegsysteem in de Europese Unie en tot intrekking van Besluit 2012/757/EU
- [6] Verordening (EU) Nr. 454/2011 van de Commissie van 5 mei 2011 betreffende de technische specificatie inzake interoperabiliteit van het subsysteem telematicatoepassingen ten dienste van passagiers van het trans-Europees spoorwegsysteem
- [7] Verordening (EU) Nr. 1305/2014 van de Commissie van 11 december 2014 betreffende de technische specificatie inzake interoperabiliteit van het subsysteem telematicatoepassingen voor goederenvervoer van het spoorwegsysteem in de Europese Unie en tot wijziging van Verordening (EG) nr. 62/2006
- [8] Wet van 23 april 2003, houdende nieuwe algemene regels over de aanleg, het beheer, de toegankelijkheid en het gebruik van spoorwegen alsmede over het verkeer over spoorwegen (Spoorwegwet)
- [9] De Blauwe Gids van 2022: richtlijnen voor de uitvoering van de productvoorschriften van de EU, Europese Commissie, ref. 2022/C 247/01

Normen

- [10] Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process, Comité Européen de Normalisation Electrotechnique (CENELEC), EN 50126-1, October 2017
- [11] Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety, Comité Européen de Normalisation Electrotechnique (CENELEC), EN 50126-2, October 2017
- [12] Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems, Comité Européen de Normalisation Electrotechnique (CENELEC), EN 50128, June 2011
- [13] Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling, Comité

Européen de Normalisation Electrotechnique (CENELEC), EN 50129,
December 2018

ProRail documenten

- [14] D-003122 ERTMS Noordelijke Lijnen – Veiligheidsmanagementplan, kenmerk K201897024-815065206-95, versie 1.2, 23 november 2022
- [15] Technische Referentie Architectuur Vervoersysteem – Systemen voor ERTMS Infrastructuur en Materieel, file name: ERTMS Technische Referentie Architectuur Vervoersysteem.vsd
- [16] VenV managementplan ERTMS Noordelijke Lijnen - Plan op hoofdlijnen voor project D-003122, kenmerk K201897024-815065206-100, versie 0.1, 31 januari 2022

Sweco documenten

- [17] Systeemdefinitie ERTMS Noordelijke Lijnen, 51006352-SWECO-SYS-ZZ-TS-SE-00001
- [18] Project Management Plan (PMP) – ERTMS Noordelijke Lijnen, 51006352-SWECO-MAN-ZZ-MS-ZM-00001
- [19] Organogram, 51006352-SWECO-MAN-ZZ-OR-SE-00001
- [20] V&G Management Plan
- [21] Verificatieplan
- [22] Validatieplan

Gezamenlijke documenten IB's

- [23] SE-Werkplan KA ENL, Nexus + Sweco + Arcadis

Bijlage 1 – Van toepassing zijnde TSI's

In deze bijlage wordt onderbouwd welke TSI's wel en niet van toepassing zijn.

TSI	Nr. ³	Van toepassing	Onderbouwing
Telematicatoepassingen Passagiers (TAP)	454/2011	Nee	Er is geen direct raakvlak tussen ERTMS en TAP. Er zijn wel raakvlakken met de verkeersleidingssystemen, maar die vallen buiten de scope van de IB's.
Wagons (WAG)	321/2013	Nee	Wijzigingen aan goederenwagons zijn niet in scope.
Infrastructuur (INF)	1299/2014	Nee	Wijzigingen aan de infrastructuur zijn niet in scope. Raakvlakken met INF worden gemanaged vanuit de TSI CCS.
Toegankelijkheid (PRM)	1300/2014	Nee	Wijzigingen aan de infrastructuur, treinen en locomotieven zijn niet in scope.
Energie (ENE)	1301/2014	Nee	Er worden geen wijzigingen aangebracht in de tractie-energievoorziening. De meeste baanvakken zijn sowieso niet voorzien van bovenleiding.
Rollend materieel (LOC&PAS)	1302/2014	Nee	Wijzigingen aan treinen en locomotieven zijn niet in scope.
Veiligheid in spoorwegtunnels (SRT)	1303/2014	Nee	Er zijn op deze percelen geen tunnels > 100 m.
Geluid (NOI)	1304/2014	Nee	Deze TSI is alleen van toepassing op rollend materieel.
Telematicatoepassingen Goederen (TAF)	1305/2014	Nee	Er is geen direct raakvlak tussen ERTMS en TAF. Er zijn wel raakvlakken met de verkeersleidingssystemen, maar die vallen buiten de scope van de IB's.
Besturing en Seingeving (CCS)	2016/919	Ja	ERTMS wordt toegepast in het project.

³ TSI's kunnen gewijzigd zijn door amendementen, maar het nummer blijft daarbij gehandhaafd

Exploitatie en Verkeersleiding (OPS)	2019/773	Nee	Deze TSI is van toepassing op de gebruikersprocessen, maar die vallen buiten de scope van de IB's.
--------------------------------------	----------	-----	--

Bijlage 2 – Uitgangspunten

In deze bijlage worden de uitgangspunten die eerder in dit document (expliciet of impliciet) zijn genoemd nog eens opgesomd.

De volgende uitgangspunten worden gehanteerd:

- Generieke Producten en de Generieke Applicatie voldoen aan de wettelijke eisen (§ 3);
- De conformiteitsverklaringen (voor Interoperability Constituents) van fabrikanten en de ondersteunende 'EG' certificaten van hun Notified Bodies zijn tijdig beschikbaar (§ 3);
- Het Type Examination Certificate (of eventueel het Intermediate Statement of Verification) voor de Generieke Applicatie, uitgegeven door cluster OVEB's Notified Body, is tijdig beschikbaar (§ 3);
- Het Independent Safety Assessment Report van de Generieke Applicatie, opgesteld door cluster OVEB's Assessment Body, is tijdig beschikbaar (§ 3);
- Alle veiligheidsrisico's m.b.t. de Generieke Producten en de Generieke Applicatie zijn voldoende gemitigeerd, hetzij in het ontwerp van de producten en systemen zelf, hetzij door verwerking van veiligheidseisen (Safety Related Application Conditions - SRACs) in ontwerpvoorschriften, installatievoorschriften, testvoorschriften en – specificaties, bedieningsvoorschriften en onderhoudsvoorschriften (§ 3, § 6.7.4);
- Hazards zijn te traceren naar veiligheidseisen (SRACs) en veiligheidseisen (SRACs) zijn terug te traceren naar hazards (§ 3, § 6.7.4);
- Deze ontwerpvoorschriften, installatievoorschriften, testvoorschriften en – specificaties, bedieningsvoorschriften en onderhoudsvoorschriften worden ondersteund door OVEB's Assessment Body (middels een brief of rapport) (§ 3, § 6.7.43);
- De processen voor uitgifte en inname van IMX data worden ontwikkeld onder het cluster IDE (§ 4.1);
- De processen voor uitgifte en inname van IMX data worden geaccepteerd door een Assessment Body (AsBo) (§ 4.1);
- Door ProRail aangeleverde IMX data is correct en voldoende nauwkeurig dan wel met behulp van andere (referentie) gegevens voldoende nauwkeurig en betrouwbaar te maken voor een veilig ontwerp (§ 4.1);
- Raakvlakken met het safety management van Thales, RIGD Loxia en eventueel de leverancier van de Object Controllers worden gemanaged door de Safety Manager ENL van ProRail (§ 5.2.2);
- Alle systemen en bijbehorende voorschriften worden vrijgegeven in parallel aan de goedkeuring van de Early Deployment Line. Daarom zijn Toestemmingen voor Gebruik (TvG's) van nog niet vrijgegeven ERTMS apparatuur (van ProRail) niet voorzien voor de latere percelen (§ 5.2.5);
- Ontwerpvoorschriften van de fabrikanten (zoals Thales) zijn verwerkt in de ontwerpvoorschriften van ProRail (§ 6.5);
- Tools voor het werken met IMX data (zowel ontwerpen als verifiëren) worden buiten het project ENL om ontwikkeld. Het aantonen dat de tools voldoen aan de eisen voor T2 of T3 tools valt dus buiten de scope het ENL project (§ 6.9);
- Het cluster OVEB aantoont dat alle relevante TSI-eisen ofwel zijn geïmplementeerd op het Generic Application (GA) niveau ofwel zijn verwerkt

in de ontwerpvoorschriften, installatievoorschriften, testvoorschriften et cetera (§ 3, § 8.1);

- TSI-eisen zijn te traceren naar eisen in de ontwerpvoorschriften, installatievoorschriften, testvoorschriften et cetera en deze eisen zijn terug te traceren naar TSI-eisen (§ 3, § 8.1);
- Deze ontwerpvoorschriften, installatievoorschriften, testvoorschriften et cetera worden ondersteund door OVEB's Notified Body (middels een brief of rapport) (§ 3, § 8.1);
- De verdeling van te leveren en te beoordelen bewijsvoering moet nog in detail worden afgestemd tussen OVEB en EUSI en moet nog worden geaccepteerd door beide NoBo's (§ 8.2).

Bijlage 3 – Risicomatrix

Deze bijlage geeft een voorbeeld van risicoclassificatie en een risicomatrix. In het project wordt niet deze matrix gebruikt maar de risicomatrix van ProRail.

De risicoklassen zijn als volgt:

Risk Classification		
	Very high	The risk is unacceptable
	High	The risk shall be reduced
	Average	The risk should be reduced further
	Low	The risk is acceptable

Dit is een voorbeeld van een risicomatrix.

				Likelihood					
				1	2	3	4	5	6
				Very unlikely	Unlikely	Occasionally	Probably	Regularly	Frequently
				Once in 100 years	Once in 10 years	Once a year	Once a month	Once a week	Dayly
				10 E-9	10 E-8	10 E-7	10 E-5	10 E-4	10 E-3
Severity	G	Catastrophic	Many casualties						
	F	Disastrous	A few casualties						
	E	Large	Single casualty						
	D	Considerable	A few heavily injured						
	C	Limited	Slightly injured						
	B	Minor	Minor injuries						
	A	No or very minor	No injuries						

Bijlage 4 – Audit programma

Onderstaande tabel geeft het voorlopige programma van safety audits weer:

Perceel	Fase	Onderwerpen
Groningen – Eemshaven/Delfzijl	Realisatie	Installatie Testen Validatie
Groningen – Bad Nieuweschans	Realisatie	Installatie Testen Validatie
Emplacement Groningen	Realisatie	Installatie Testen Validatie

Bijlage 5 – Checklist eisen safety plan

De norm EN 50126-2 specificeert in § 7.3.2.3 de eisen die aan een safety plan gesteld worden. Met onderstaande checklist wordt getoond in welke paragraaf (-fen) aan een eis wordt voldaan.

The Safety Plan shall define the following safety activities:

a) the policy and strategy for achieving safety;	3 Strategie
b) the scope of the plan;	1.2 Afbakening
c) planning of the safety activities;	6 Activiteiten en producten 7 Hazard management
d) the underlying system life cycle as well as the safety analysis, engineering processes and relationship with assessment to be applied during the life cycle, including processes for:	
– ensuring an appropriate degree of personnel independence in tasks, commensurate with the risk of the system;	5 Veiligheidsorganisatie
– hazard identification and analysis;	7 Hazard management
– risk assessment and on-going risk management;	7 Hazard management
– risk acceptance criteria and reviewing risk acceptance;	7.6 Risico evaluatie
– reviewing the effectiveness of risk reduction measures;	4.2 Verificatie 7.6 Risico evaluatie
– the establishment and on-going review of the adequacy of the safety requirements;	4.2 Verificatie 7.6 Risico evaluatie Fout! Verwijzingsbron niet gevonden.
– system design;	6.6 Systeemontwerp
– verification;	4.2 Verificatie
– validation to achieve compliance between system requirements and realisation;	4.3 Validatie
– achievement of compliance of the management process with the safety plan (e.g. confirmed via audits);	4.2 Verificatie 7.8 Safety audits

Together with our clients
and the collective
knowledge of our 18,500 ar-
chitects, engineers and
other specialists, we co-cre-
ate solutions that address
urbanisation, capture the
power of digitalisation, and
make our societies more
sustainable.

Sweco – Transforming soci-
ety together