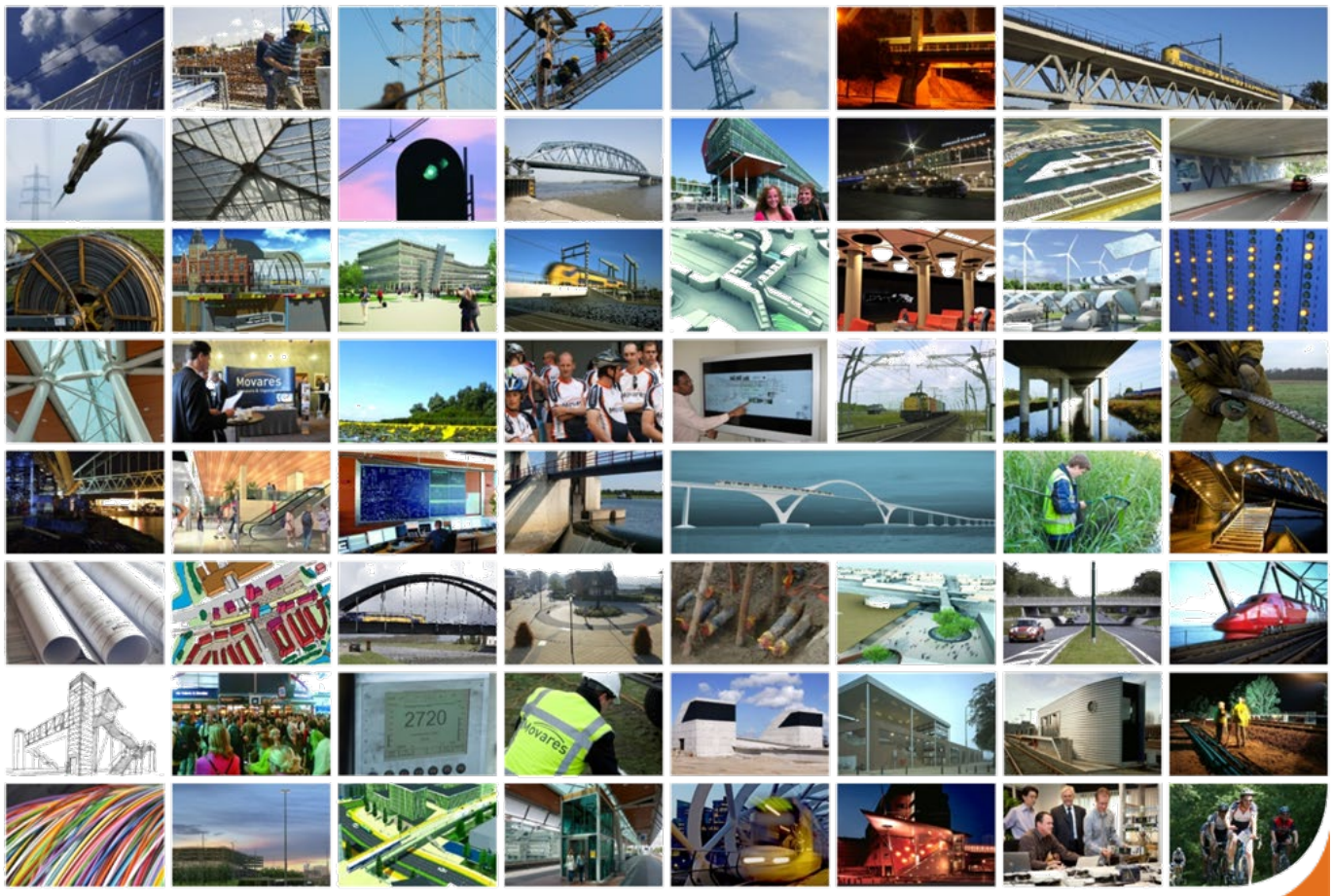
Borging integrale veiligheid HSL-Zuid

Auditrapport



16 september 2015 - Versie 1.0 Definitief

wij verbinden

Autorisatieblad

	Naam	Paraaf	Datum
Opgesteld door	ir. A. Eigenraam, ir. R. de Zutter		16-09-2015 17-09-2015
Controle door	ir. P.H.J. van de Ven ir. J. A. Koning		17-09-2015
Vrijgave door	ing. J. Jansen		Jansen J (Jeroen) 2015.09.17 18:44:03 +02'00'

Samenvatting

Begin 2014 heeft onderzoek[1] uitgewezen dat het integrale wijzigingsbeheer zoals dat voor de HSL-Zuid is georganiseerd geen invulling geeft aan het actief beheren van de integrale safety case voor de HSL-Zuid. Dit onderzoek wijst echter niet uit of de actuele veiligheidsborging voor de HSL-Zuid daarmee wel of niet afdoende is. Dit was aanleiding voor het Ministerie van I&M om met betrekking tot de veiligheidsborging voor de HSL-Zuid een aantal vragen te formuleren.

Formulering van de opdracht

Bij wijzigingen van het vervoersysteem HSL-Zuid wordt gewerkt op de wijze zoals is beschreven in de documenten *Memo Aanpak Integraal Safety Management* en *Borging Management of Change HSL-Zuid (MoC-proces).* Over deze documenten heeft het Ministerie de volgende vragen gesteld:

Hoofdvraag:
Is het wijzigingsbeheer, zoals beschreven in de documenten *Memo Aanpak Integraal Safety Management* en *Borging Management of Change HSL-Zuid* voldoende met het oog op het aantoonbaar borgen van de integrale veiligheid op de HSL-Zuid?

Subvragen:
- Is het proces goed ingericht?
- Wordt het proces goed uitgevoerd en voldoen de huidige afspraken tussen partijen gezien het toenemende vervoersaanbod op de HSL-Zuid?
- Welke aanbevelingen zijn er om de borging te verbeteren?

In opdracht van het Ministerie heeft Movares een audit uitgevoerd om deze vragen te kunnen beantwoorden.

Beantwoording van de vragen

Hoofdvraag:
Is het wijzigingsbeheer, zoals beschreven in de documenten *Memo Aanpak Integraal Safety Management* en *Borging Management of Change HSL-Zuid* voldoende met het oog op het aantoonbaar borgen van de integrale veiligheid op de HSL-Zuid?

Antwoord:
In de [Kadernota] is vastgelegd dat wordt gestreefd naar continue verbetering van veiligheid door toepassing van het ALARP principe. Mede in het licht van deze visie worden door de auditers op een aantal onderdelen van de veiligheidsborging van de HSL-Zuid verbeteringen voorgesteld. Deze verbeteringen hebben betrekking op de toewijzing van de verantwoordelijkheid voor veiligheidsvalidatie, een planmatiger aanpak van de veiligheidsborging en vastlegging van de integrale veiligheidsverant-woording.

Toelichting:
Het *Memo Aanpak Integraal Safety Management* geeft aan dat de veiligheidsborging voor de HSL-Zuid is ingericht conform de Europese Spoorwegveiligheidsrichtlijn, waarbij iedere partij verantwoordelijk is voor de veiligheid van zijn eigen systeemdelen. Deze richtlijn schrijft ook voor dat bij systeemgrensoverstijgende wijzigingen met de andere betrokken partijen moet worden afgestemd.

Het proces voor systeemgrensoverstijgende wijzigingen is vastgelegd in het document *Borging management of change*. De procesbeschrijving gaat alleen in op de

[1] Onderzoek vergunningverlening V250 (Horvat & Partners, Boer & Croon en Bosselaar-Strengers)

verantwoordelijkheden van de partijen, op de risico-inventarisatie en –evaluatie en op het proces om de daaruit volgende maatregelen door de betreffende partijen te laten implementeren. De overige activiteiten om de veiligheid op de HSL-Zuid aantoonbaar te borgen (integratie, verificatie en validatie) worden niet behandeld.

Subvragen:
Is het proces goed ingericht? Voldoen de huidige afspraken tussen partijen gezien het toenemende vervoersaanbod op de HSL-Zuid?

Antwoord:
Uit de afspraken tussen de partijen blijkt de intentie om zich gezamenlijk in te spannen om aan het vereiste hoge prestatieniveau van het HSL-Zuid vervoersysteem te kunnen voldoen.
De veiligheidsonderbouwing in de Integrale Safety Case HSL-Zuid is gebaseerd op het voorziene gebruik in 2022. Het groeiende verkeersaanbod stelt geen extra eisen aan de veiligheidsborging. Wel kan invulling worden gegeven aan de ambitie met betrekking tot het ALARP principe door het veiligheidsmanagementproces te verbeteren, met name op de volgende punten:

- Vastlegging van de veiligheidsdoelstellingen voor de HSL-Zuid, of een verwijzing daarnaar;
- Planmatige opzet van het veiligheidmanagement conform [EN50126];
- Vastlegging van de integrale veiligheidsonderbouwing conform [EN50126] en [EN50129];
- Eenduidige vastlegging van de verantwoordelijkheid voor systeemintegratie en (veiligheids)validatie

Wordt het proces goed uitgevoerd?
Antwoord:
De afspraken die de partijen in het MoC hebben vastgelegd worden nageleefd. Uit de interviews blijkt dat de betrokken partijen in de verschillende MoC-gremia met elkaar afstemmen, zowel inhoudelijk als procesmatig. Zoals in het antwoord op de hoofdvraag reeds is aangegeven ontbreekt in het MoC-proces een beschrijving van de integratie, verificatie en (veiligheids)validatie van wijzigingen. Uit de interviews is gebleken dat in voorkomende gevallen deze aspecten wel werden ingevuld.

Welke aanbevelingen zijn er om de borging te verbeteren?
Antwoord:
Op grond van het uitgevoerde onderzoek en de daaruit voortgekomen bevindingen worden de volgende aanbevelingen gedaan voor de verbetering van de veiligheidsborging en de vastlegging daarvan:

1. Zorg dat het MoC-proces wordt opgenomen in de VMS'en van ProRail en NS, en zorg ook dat de ontbrekende onderdelen integratie, verificatie en validatie in de beschrijving van het proces worden vastgelegd.
2. Formaliseer de actuele veiligheidsonderbouwing van de HSL-Zuid, zodat er een formele basis is voor (delta)risicoredeneringen.
3. Bedeel de rol van veiligheidsvalidator expliciet toe aan het Veiligheids Advies Overleg (VAO) zoals dat binnen het MoC-proces bestaat.

Uit de interviews bleek dat het aantal in behandeling zijnde veiligheidsrelevante issues sterk is afgenomen. Het vervoersaanbod op de HSL-Zuid groeit echter nog. Daarom

lijkt het zinvol en praktisch om de verbeteringsacties binnen afzienbare tijd te starten: verbeteren wanneer het kan en op sterkte zijn wanneer het moet.

Samenvattende conclusie

De structurele afstemming tussen de betrokken partijen in het MoC-proces is naar de mening van de auditors noodzakelijk vanwege de nog niet bewezen ´rijpheid´ [2], de complexiteit en het risicoprofiel van de HSL-Zuid.

Het MoC-proces beoogt mede invulling te geven aan de samenwerkingsverplichting op veiligheidsgebied zoals die door de Europese Spoorwegveiligheidsrichtlijn wordt opgelegd. Uit de auditresultaten blijkt dat op een aantal punten de veiligheidsborging verbeterd kan worden. Wanneer de hierboven genoemde aanbevelingen worden opgevolgd, dan zorgt naar onze mening het MoC-proces voor een adequate veiligheidsborging op de HSL-Zuid.

[2] Onder ´rijpheid´van een systeem wordt verstaan de mate waarin het systeem stabiel is en zich in de praktijk heeft bewezen. Als het systeem voldoende rijp is, kunnen algemene praktijkcodes worden opgesteld (voorschriften voor ontwerp en operatie) die bij uitbreidingen en wijzigingen kunnen worden gehanteerd.

Inhoudsopgave

1 Inleiding

1.1 Doel van dit rapport

Het doel van dit rapport is om het Ministerie van I&M inzicht te verschaffen in de veiligheidsborging binnen het wijzigingsbeheer van de HSL-Zuid, i.e. of de veiligheidsborging afdoende is.

1.2 Achtergrond

In de projectfase van de HSL-Zuid was de Staat de integrerende en validerende partij. In de beheerfase is er geen instantie meer die de expliciete verantwoordelijkheid draagt voor systeemintegratie en (veiligheids)validatie. De integratie- en validatieverantwoordelijkheid is vormgegeven als een afstemmings- en samenwerkingsverplichting van de bij de exploitatie van het vervoersysteem betrokken partijen. Deze partijen zijn:

- ProRail: infrabeheerder volgens de spoorwegwet (houder van de beheerconcessie van de hoofdspoorweginfrastructuur incl. HSL-Zuid). Onder dit beheer valt ook de HSL-Zuid. Daaruit voortvloeiend is ProRail ook verantwoordelijk voor het management van het contract met Infraspeed. Naast asset management (AM) is ProRail ook verantwoordelijk voor de verkeersleiding (VL) en het bewaken en schakelen van de tractievoeding (SMC) van de HSL-Zuid.
- NS Internationaal BV (verder in dit document aangeduid als NS): houder van de vervoersconcessie op de HSL-Zuid.
- Infraspeed: de infraprovider van de HSL-Zuid. Het contract met Infraspeed is afgesloten door de Staat.

Noot: Uitgangspunt voor deze audit is dat de veiligheidsborging als onderdeel van het wijzigingsproces geacht wordt een zaak te zijn van de concessiehouders NS en ProRail. Infraspeed opereert in deze visie als 'gewone' aannemer van ProRail.

Bij wijzigingen van het vervoersysteem HSL-Zuid wordt gewerkt op de wijze zoals is beschreven in de documenten *Memo Aanpak Integraal Safety Management* en *Borging Management of Change HSL-Zuid (MoC-proces).*

In het rapport *Onderzoek vergunningverlening V250* [Horvat] wordt geconstateerd dat het integrale wijzigingsbeheer zoals dat voor de HSL-Zuid is georganiseerd geen invulling geeft aan het actief beheren van de integrale safety case voor de HSL-Zuid. Dit onderzoek wijst echter niet uit of de actuele veiligheidsborging voor de HSL-Zuid daarmee wel of niet afdoende is. Dit was aanleiding voor het Ministerie van I&M om met betrekking tot de veiligheidsborging voor de HSL-Zuid een aantal vragen te formuleren.

1.3 Uw vraag

Hoofdvraag:

Is het wijzigingsbeheer, zoals beschreven in de 'Aanpak integraal safety management' en de 'Borging management of change' voldoende met het oog op het aantoonbaar borgen van de integrale veiligheid op de HSL-Zuid?

Subvragen:

- Is het proces goed ingericht?
- Wordt het proces goed uitgevoerd en voldoen de huidige afspraken tussen partijen gezien het toenemende vervoersaanbod op de HSL-Zuid?
- Welke aanbevelingen zijn er om de borging te verbeteren?

1.4 Leeswijzer

Dit rapport is als volgt opgebouwd:

Hoofdstuk 2 beschrijft de bij deze audit gevolgde aanpak.
In hoofdstuk 3 beschrijven wij onze visie op integrale veiligheidsborging.
In hoofdstuk 0 wordt de onderzoekshypothese getoetst.
Hoofdstuk 5 bevat de beantwoording van de onderzoeksvragen en onze aanbevelingen.

1.5 Referentiedocumenten

Ten behoeve van de audit zijn de volgende documenten geraadpleegd:

[Aanpak ISM]	Memo Aanpak Integraal Safety Management (ProRail, EDMS-#1784691-v2D d.d. 22 april 2014);
[MoC]	Borging Management of Change HSL-Zuid (ProRail, EDMS-#2939947-v7C d.d. 30 april 2014;
[Horvat]	Onderzoek vergunningverlening V250 (Horvat & Partners, Boer & Croon en Bosselaar-Strengers, Rapportnummer: 13025-R-006, definitieve versie d.d. 15 januari 2014);
[ISC HSL]	Integrale Safety Case HSL-Zuid - Revisie 4 (Rijkswaterstaat, DOCS\725911 d.d. 11 november 2008)
[EN50126]	NEN-EN 50126-1:1999, Spoorwegen en soortgelijke geleid vervoer - De specificatie en het bewijs van de bruikbaarheid, beschikbaarheid, onderhoudbaarheid en veiligheid - Deel 1: Basiseisen;
[EN50129]	NEN-EN 50129:2003, Railtoepassingen - Communicatie, signalering en processystemen - Elektronische signaleringssystemen met betrekking tot veiligheid;
[Richtlijn SV]	Richtlijn 2004/49/EG, Spoorwegveiligheidsrichtlijn;
[CSM-REA]	Verordening 352/2009, Common Safety Methods - Risk Evaluation and Assessment;
[Kadernota]	Veilig vervoeren, Veilig werken,Veilig leven met spoor - Derde kadernota railveiligheid (Ministerie van V&W, Juni 2010);
[Beheerconc.]	Concept-ontwerpbeheerconcessie 2015-2025 (Ministerie van I&M, april 2014);
[Vervoerconc.]	Vervoerconcessie voor het hogesnelheidsnet (Ministerie van V&W, juni 2009);
[PRC00278]	PRC00278 - Versie 001, Veiligheidsverantwoording bij wijzigingen (ProRail, EDMS-#2563173-v2 d.d. 13 oktober 2010).
[Vragen I&M]	Memo VS-AE-17G0AD4002, 19 juni 2015.

1.6 Afkortingen en begrippen

ALARA	As Low As Reasonably Achievable, zie ALARP.
ALARP	As Low As Reasonably Practicable, veiligheidsprincipe (maatregelen met een positief effect op de veiligheid mogen niet worden nagelaten als deze wenselijk, haalbaar en betaalbaar zijn).
AsBo	CSM-REA assessment body (AsBo) volgens de Europese verordeningen 352/2009 en 402/2013.
CMT	Contract management team, onderdeel van ProRail dat het contract met Infraspeed beheert.
EFFBD	Enhanced Functional Flow Block Diagram
NoBo	Notified body (NoBo) voor de subsystemen uit de interoperabiliteitsrichtlijn 2008/57/EC.

Rijpheid (van het systeem)	Mate waarin het systeem stabiel is en zich in de praktijk heeft bewezen. Als het systeem voldoende rijp is, kunnen algemene praktijkcodes worden opgesteld (voorschriften voor ontwerp en operatie) die bij uitbreidingen en wijzigingen kunnen worden gehanteerd.
Systeem integrator	Persoon of instantie die verantwoordelijk is voor systeemintegratie.
Systeemintegratie	Het samenvoegen van deelsystemen in een overkoepelend systeem, waarin door de samenhang tussen de deelsystemen de uiteindelijke eigenschappen van het overkoepelend systeem ontstaan.
Systeemvalidatie	Het door onderzoek en aanlevering van objectieve bewijzen aantonen dat een systeem in alle opzichten aan de gebruikseisen voldoet i.e. geschikt is voor gebruik.
Validator	Persoon of instantie die verantwoordelijk is voor validatie.
VAO	Veiligheid Advies Overleg binnen het MoC-proces
Veiligheidsborging	Planmatige (bij)sturing op veiligheidsdoelstellingen.
Veiligheids-managementplan	Beschrijving van de aanpak die wordt gevolgd om te borgen dat aan de veiligheidsdoelstellingen wordt voldaan.
Veiligheidsvalidatie	Het door onderzoek en aanlevering van objectieve bewijzen aantonen dat een systeem in alle opzichten aan de gestelde veiligheidsdoelstellingen voldoet i.e. voldoende veilig is. Tevens moet aangetoond worden dat de ongewijzigde delen niet onbedoeld zijn aangetast door de wijziging (non-regressie).
Verificatie	Het door onderzoek en aanlevering van objectieve bewijzen aantonen dat aan gespecificeerde eisen is voldaan.

1.7 Versiebeheer

Versie/datum	**Wijzigingen en opmerkingen**
08-12-2014	Versie ter interne (Movares) review
13-12-2014	Commentaar uit interne review verwerkt. Versie ter review door I&M.
1.0 concept/ 19-01-2015	Verwerking van het commentaar van I&M en de stuurgroep HSL-Zuid als vastgelegd in email *FW: commentaar IenM op concept rapport audit borging integrale veiligheid HSL-Zuid*, H.J. Heeres, 19 december 2014.
1.0 definitief/ 16-09-2015	Reviewcommentaar van I&M, NS en ProRail verwerkt. In antwoord op de vragen die I&M heeft gesteld als samenvatting van de vragen van NS en ProRail (email *FW: Audit integrale veiligheid* van H.J. Heeres, 10 april 2015) is door Movares Memo VS-AE-17G0AD4002 (19 juni 2015) opgesteld. Hierin is, als aanvulling op de audit, PRC 00278 van ProRail beoordeeld. De resultaten zijn overgenomen in Bijlage I.

2 Aanpak

Om de vraag te beantwoorden of het beschreven wijzigingsbeheer afdoende is om de integrale veiligheid op de HSL-Zuid te borgen, toetsen wij de volgende onderzoekshypothese.

De integrale veiligheid van de HSL-Zuid wordt geborgd doordat:

- *één instantie verantwoordelijk is voor systeemintegratie en (veiligheids)validatie;*
- *de veiligheid van wijzigingen in de verschillende deelsystemen, -processen en contracten integraal wordt verantwoord met een expliciete planmatige aanpak volgens de normen [EN50126] en [EN50129].*

Deze hypothese is gebaseerd op onze visie op integrale veiligheidsborging (zie hoofdstuk 3).

Voor deze audit is een bureaustudie uitgevoerd en is een aantal betrokkenen geïnterviewd.

De bureaustudie heeft tot doel om:

- een duidelijk beeld te krijgen over de wijze waarop het wijzigingsbeheer is ingericht en de mate waarin deze aansluit op regelgeving en beleid;
- te bepalen of het wijzigingsbeheer aanleiding geeft om de onderzoeks-hypothese te aanvaarden c.q. te verwerpen.

De interviews hebben tot doel om:

- te verifiëren of het wijzigingsbeheer functioneert op de wijze zoals wij dat uit de bureaustudie hebben opgemaakt;
- te bepalen of de uitvoering van het wijzigingsbeheer in de praktijk argumenten geeft om de onderzoekshypothese te aanvaarden c.q. te verwerpen.

In het kader van de bureaustudie zijn (relevante delen van) de volgende documenten bestudeerd[3]:

- Memo Aanpak Integraal Safety Management [Aanpak ISM];
- Borging Management of Change HSL-Zuid [MoC];
- Integrale Safety Case HSL-Zuid [ISC HSL];
- Europese spoorwegveiligheidsregelgeving;
  - Spoorwegveiligheidsrichtlijn [Richtlijn SV];
  - Verordening Common Safety Methods - Risk Evaluation and Assessment [CSM-REA];
- Derde kadernota railveiligheid [Kadernota].

Er hebben interviews plaatsgevonden met de leden van de Stuurgroep en de voorzitters van het Concessieteam en het Veiligheid Advies Overleg (VAO).
De Stuurgroep wordt gevormd door vertegenwoordigers van het Ministerie van I&M (voorzitter en secretaris), ProRail, NS, Infraspeed en ILT. Het Concessieteam bestaat uit vertegenwoordigers van de concessiehouders ProRail en NS. Het Veiligheid Advies Overleg bestaat uit de safety managers van Infraspeed, NS en ProRail.

[3] De overige in § 1.5 vermelde documenten zijn geraadpleegde normen en achtergronddocumentatie.
De safety cases van NS en Infraspeed zijn niet bestudeerd. Uitgangspunt bij deze audit is dat contractpartijen aan de contracteisen voldoen en evt. veiligheidsrelevante wijzigingen in hun eigen safety cases verwerken.

3 Integrale veiligheid

3.1 Onze visie op veiligheidsborging

Veiligheidsborging moet een vanzelfsprekend onderdeel zijn van het wijzigingsproces en mag niet afhankelijk zijn van de beoordeling door NoBo's, AsBo's en/of ILT.

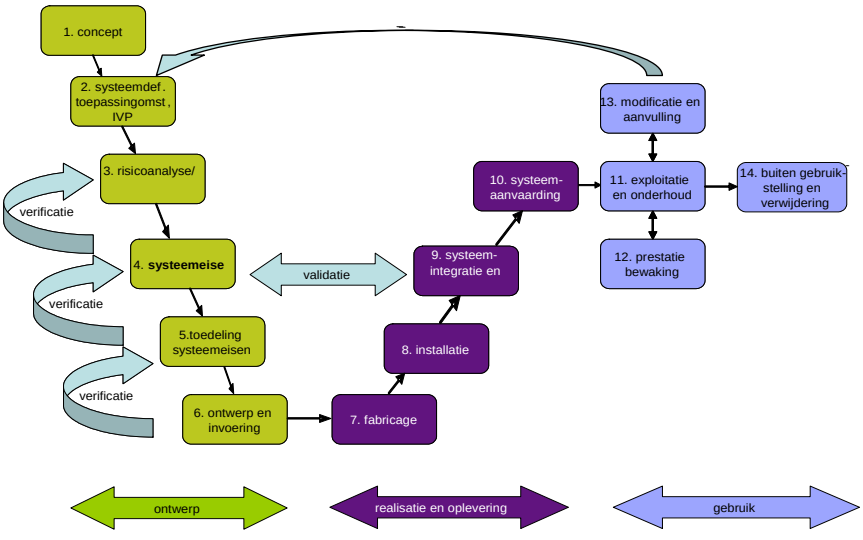
Om de veiligheid van een railvervoersysteem te borgen dient, zowel bij nieuwbouw als bij wijzigingen, een zorgvuldig proces van systems engineering te worden doorlopen.
Het bij spoorwegtoepassingen gangbare proces is beschreven in de norm [EN50126]. Belangrijke pijlers van dit proces zijn risico-inventarisatie en -evaluatie, verificatie en validatie en systeemintegratie en -validatie (zie kader).
Het proces is onderverdeeld in een aantal stappen (fases). Het systems engineering proces conform [EN 50126] wordt grafisch weergegeven in het zgn. V-model (zie Figuur 1).

Hierin wordt met verificatie bedoeld de controle of de output van een processtap voldoet aan de eisen en randvoorwaarden die als input zijn meegegeven. Met validatie wordt bedoeld de controle of de output van een processtap voldoet aan de gebruikerseisen die (vaak op een hoger abstractieniveau) zijn gesteld ('fitness for use').

Risicoinventarisatie en-evaluatie vindt plaats om maatregelen te bepalen waarmee de veiligheid op het gewenste niveau kan worden gebracht.

Verificatie en validatie zijn belangrijke controlemiddelen om te borgen dat het proces van systems engineering het gewenste resultaat oplevert. Verificatie houdt in dat wordt gecontroleerd of voldaan is aan alle eisen die voor die processtap gelden, dit is vooral een controle 'op papier' Bij validatie wordt beoordeeld of het (deel)systeem geschikt is voor gebruik. Deze beoordeling wordt veelal gebaseerd op praktijktests.

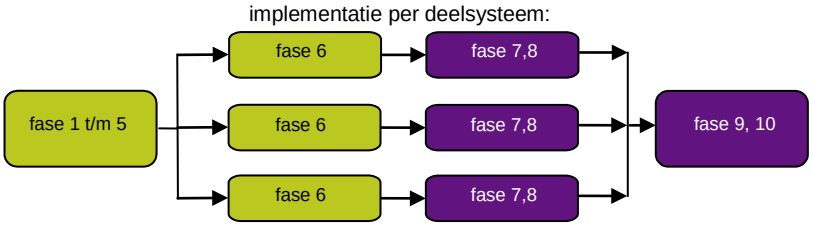
Systeemintegratie is de activiteit die ervoor moet zorgen dat alle deelsystemen samen een werkend geheel gaan vormen. Systeemintegratie begint met het formuleren van raakvlakeisen voor deelsystemen en eindigt met het samenvoegen van die deelsystemen en het testen van de correcte samenwerking tussen die systemen.



Figuur 1 Het V-model

3.2 Integrale veiligheid

Veelal zal het systems engineering proces betrekking hebben op meerdere deel-systemen, waarvoor verschillende partijen verantwoordelijk zijn. Iedere partij is dan zelf verantwoordelijk voor ontwerp en realisatie (fase 6 t/m 8) van het door die partij te realiseren deelsysteem. In fase 9 worden dan de afzonderlijke deelsystemen samengevoegd (geïntegreerd) en gevalideerd (zie Figuur 2).



Figuur 2 Integratie van deelsystemen

De norm [EN50129] beschrijft welke aspecten bij de veiligheidsonderbouwing dienen te worden beschouwd (zie kader) en wat daarover in het veiligheidsbewijs (de safety case) moet worden opgenomen.

Integrale veiligheidsborging heeft betrekking op het geheel van onderling samenhangende deelsystemen ('het geheel is meer dan de som der delen'). De deelsystemen betreffen zowel techniek (infra en materieel) als de operatie (verkeersleiding, vervoer, beheer en onderhoud).
Hierbij gaat het er vooral om of de veiligheid van het systeem als geheel robuust is:

- Hoe tolerant is de systeemveiligheid voor een fout in één deelsysteem?
- Is er in het ene deelsysteem voldoende rekening gehouden met de eigenschappen van het andere deelsysteem in bijzondere omstandigheden of situaties?[4]

De samenwerking tussen de voor deze deelsystemen verantwoordelijke partijen is een (afgeleide) randvoorwaarde voor integrale veiligheid.

In de veiligheidsonderbouwing wordt voor een systeem of proces aangetoond dat:

- het onder nominale omstandigheden goed functioneert;
- falen niet tot onveilige situaties kan leiden;
- verwachte invloeden van buitenaf geen onveilige situaties veroorzaken;
- alle functies die veiligheidsrelevant zijn beproefd zijn voordat het in gebruik is gesteld.

Tevens wordt aangegeven aan welke voorwaarden moet worden voldaan om het systeem of proces veilig te kunnen gebruiken.

Integraal safety management vereist een generiek (globaal) plan voor de algemene veiligheidsaanpak en een specifiek, gedetailleerd veiligheidsplan voor iedere door te voeren wijziging.

Integraal safety management is het planmatige proces (zie kader) met de stappen zoals in de vorige paragraaf beschreven, om de robuustheid te onderzoeken en waar nodig maatregelen te nemen wanneer het risico te groot wordt bevonden.

[4] Deelsystemen kunnen ook menselijke actoren zijn. Het niet optimaal afgestemd zijn van werkomstandigheden en voorzieningen maken systemen gevoelig voor menselijk falen.

Onze visie is als volgt samengevat in de onderzoekshypothese:

De integrale veiligheid van de HSL-Zuid wordt geborgd doordat:

- *één instantie verantwoordelijk is voor systeemintegratie en (veiligheids)validatie;*
- *de veiligheid van wijzigingen in de verschillende deelsystemen, -processen en contracten integraal wordt verantwoord met een expliciete planmatige aanpak volgens de normen [EN50126] en [EN50129].*

4 Toetsing onderzoekshypothese

Op basis van bevindingen uit de bureaustudie en de interviews[5] wordt nu de onderzoekshypothese getoetst:

De integrale veiligheid van de HSL-Zuid wordt geborgd doordat:

- *één instantie verantwoordelijk is voor Systeemintegratie en (veiligheids)validatie;*
- *de veiligheid van wijzigingen in de verschillende deelsystemen, -processen en contracten integraal wordt verantwoord met een expliciete planmatige aanpak volgens de normen [EN50126] en [EN50129].*

De audit heeft de volgende bevindingen opgeleverd die voor het toetsen van de hypothese relevant zijn:

> *Systeemintegratie en (veiligheids)validatie van het eindresultaat van de wijzigingen in hun samenhang zijn niet belegd. Geen van de bij de HSL-Zuid betrokken partijen is verantwoordelijk voor systeemintegratie en integrale veiligheidsverantwoording.*
>
> *Alle veiligheidsmanagement activiteiten binnen het MoC-proces worden door het VAO uitgevoerd. Dit beperkt zich volgens de MoC-procesbeschrijving [MoC] tot de risico-inventarisatie en -evaluatie en het vaststellen van de benodigde maatregelen en daarvoor benodigde wijzigingen. De taak omvat niet de bewaking en veiligheidsverantwoording van gerealiseerde wijzigingen in hun samenhang en het effect daarvan op het vervoersysteem. Het VAO is niet de systeemintegrator van de HSL-Zuid.*
>
> *De MoC-procesbeschrijving [MoC] beschrijft geen planmatige aanpak van het integrale veiligheidsmanagement en bevat geen integrale toetscriteria voor de aanvaardbaarheid van het restrisico zoals vastgelegd in de [ISC HSL] (par. 3.4) en in de [Kadernota].*
>
> *In het MoC-proces is er geen vastlegging van de onderbouwing van de veiligheid van het vervoersysteem als geheel. De [ISC HSL] wordt niet onderhouden maar dient als (vrijblijvend) naslagwerk. Voor elke wijziging wordt een separate risico-inventarisatie en -evaluatie gemaakt ('delta-analyse').*

Met betrekking tot de in de hypothese genoemde thema's concluderen wij het volgende:

- Er is geen eenduidige instantie verantwoordelijk voor systeemintegratie en veiligheidsvalidatie.
- De veiligheidsborging zoals nu vastgelegd in [MoC] is onvoldoende planmatig, geeft geen volledige invulling van het proces conform [EN50126] en levert geen verantwoording van de veiligheid van het vervoersysteem als geheel.

[5] De auditresultaten en bevindingen zijn opgenomen in Bijlage 1.

5 Beantwoording onderzoeksvragen en conclusie

Aan de hand van de bevindingen uit de bureaustudie en de interviews[6] en het resultaat van de toetsing van de onderzoekshypothes zijn de volgende antwoorden op de onderzoeksvragen geformuleerd:

Hoofdvraag:
Is het wijzigingsbeheer, zoals beschreven in de 'Aanpak integraal safety management' en de 'Borging management of change' voldoende met het oog op het aantoonbaar borgen van de integrale veiligheid op de HSL-Zuid?

Antwoord:
In de [Kadernota] is vastgelegd dat wordt gestreefd naar continue verbetering van veiligheid door toepassing van het ALARP principe. Mede in het licht van deze visie worden door de auditers op een aantal onderdelen van de veiligheidsborging van de HSL-Zuid verbeteringen voorgesteld. Deze verbeteringen hebben betrekking op de toewijzing van de verantwoordelijkheid voor veiligheidsvalidatie, een planmatiger aanpak van de veiligheidsborging en vastlegging van de integrale veiligheidsverantwoording.

Toelichting:
Het *Memo Aanpak Integraal Safety Management* [Aanpak ISM] is ingericht conform de Europese Spoorwegveiligheidsrichtlijn, waarbij iedere partij verantwoordelijk is voor de veiligheid van zijn eigen systeemdelen. Deze richtlijn schrijft ook voor dat bij systeemgrensoverstijgende wijzigingen met de andere betrokken partijen moet worden afgestemd.

Het proces voor systeemgrensoverstijgende wijzigingen is vastgelegd in het document *Borging management of change* [MoC]. De procesbeschrijving in [MoC] gaat alleen in op de verantwoordelijkheden van de partijen, op de risico-inventarisatie en –evaluatie en op het proces om de daaruit volgende maatregelen door de betreffende partijen te laten implementeren. De overige activiteiten om de veiligheid op de HSL-Zuid aantoonbaar te borgen (zie kader) worden niet behandeld.

Aantoonbare borging van integrale veiligheid vraagt om een planmatige aanpak voor het gehele proces van identificatie, inventarisatie en evaluatie van risico's, vaststellen van maatregelen ('veiligheidsvereisten') en implementatie, tot en met integratie, verificatie en (veiligheids)validatie van wijzigingen in hun onderlinge samenhang. Tevens moet daarin de wijze van veiligheidsverantwoording worden vastgelegd.

Subvragen:
Is het proces goed ingericht?

- Voldoen de huidige afspraken tussen partijen over de integrale veiligheid, waaronder het management- of- change-proces, gezien het toenemende vervoersaanbod op de HSL-Zuid qua vorm en effectiviteit aan de internationale normen/standaarden voor integrale veiligheid en de ambities ten aanzien van de spoorveiligheid, zoals die in Europese spoorveiligheidsregelgeving en in Nederland in de 3e kadernota railveiligheid zijn vastgelegd?

[6] De auditresultaten en bevindingen zijn opgenomen in Bijlage 1.

Antwoord:
Deze vraag bevat eigenlijk twee deelvragen, namelijk:

1) Voldoen de huidige afspraken tussen partijen over de integrale veiligheid, waaronder het management-of-change-proces, qua vorm en effectiviteit aan de internationale normen/standaarden voor integrale veiligheid en de ambities ten aanzien van de spoorveiligheid, zoals die in Europese spoorveiligheidsregelgeving en in Nederland in de Derde Kadernota Railveiligheid zijn vastgelegd?
2) Vereist het toenemende vervoersaanbod op de HSL-Zuid wijziging of uitbreiding van de afspraken tussen partijen over de integrale veiligheid?

Antwoord 1):
Uit de afspraken tussen de partijen blijkt de intentie om zich gezamenlijk in te spannen om aan het vereiste hoge prestatieniveau van het HSL-Zuid vervoersysteem te kunnen voldoen.

Statistisch is het niet mogelijk om in de korte tijd dat de HSL-Zuid in exploitatie is betrouwbare uitspraken te doen over de effectiviteit van het huidige MoC-proces en of daarmee de huidige veiligheidsdoelstellingen, zoals deze in de [Kadernota] zijn vastgelegd, worden gehaald.

Wel kan invulling worden gegeven aan de ambitie met betrekking tot het ALARP principe door het veiligheidsmanagementproces te verbeteren, met name op de volgende punten:

- Vastlegging van de veiligheidsdoelstellingen voor de HSL-Zuid, of een verwijzing daarnaar[7];
- Planmatige opzet van het veiligheidmanagement conform [EN50126];
- Vastlegging van de integrale veiligheidsonderbouwing conform [EN50126] en [EN50129];
- Eenduidige vastlegging van de verantwoordelijkheid voor systeemintegratie en (veiligheids)validatie .

Antwoord 2):
Het groeiend verkeersaanbod stelt geen extra eisen aan de veiligheidsborging zolang het daadwerkelijk gebruik de prognose voor 2022 zoals vastgelegd in de [ISC] niet overschrijdt.

Toelichting:
De veiligheidsonderbouwing in de [ISC HSL] is gebaseerd op het voorziene gebruik in 2022 Zolang het werkelijk gebruik de prognose voor 2022 niet overschrijdt, is het groeiend vervoersaanbod niet van invloed op de veiligheid van de HSL-Zuid.
Wel kan onbetrouwbaarheid bij toenemende gebruiksintensiteit tot veiligheidsissues leiden: verstoring van de dienstregeling en stilvallende treinen (bijv. door verbindingverlies GSM-R) kunnen, wanneer dit erg vaak voorkomt, tot onveiligheid leiden. Er wordt dan te vaak een beroep gedaan op bijzondere operationele maatregelen zoals aanwijzingen en evacuatie van reizigers.

[7] De doelstellingen voor railveiligheid uit de [Kadernota] worden via concessies aan ProRail en NS opgelegd.

Wordt het proces goed uitgevoerd?

- Worden de huidige afspraken over integrale veiligheid voldoende en binnen de kaders van Europese spoorveiligheidsregelgeving en Nederlandse 3e kadernota railveiligheid nageleefd?

  Antwoord:
  De afspraken die de partijen in het MoC hebben vastgelegd worden nageleefd. Uit de interviews blijkt dat de betrokken partijen in de verschillende MoC-gremia met elkaar afstemmen, zowel inhoudelijk als procesmatig. Zoals in het antwoord op de hoofdvraag reeds is aangegeven ontbreekt in het MoC-proces een beschrijving van de integratie, verificatie en (veiligheids)validatie van wijzigingen. Uit de interviews is gebleken dat in voorkomende gevallen deze aspecten wel werden ingevuld, bijv. door het uitvoeren van integratietesten bij de wijziging van 'national values' die werd doorgevoerd om de gevolgen van uitval van de verbinding tussen trein en RBC te beperken.

- Zo niet, voor welke afspraken geldt dat welke risico's zijn daaraan verbonden en hoe groot zijn deze hieraan gerelateerde risico's?

  Antwoord:
  Niet van toepassing.

Welke aanbevelingen zijn er om de borging te verbeteren?

- Welke maatregelen zijn gewenst om de integrale veiligheid te verbeteren en te komen tot een zodanig veiligheidsniveau zoals dat o.b.v. de 3e kadernota railveiligheid vereist is?
- Welke maatregelen daarvan zijn no-regret gelet op internationale normen/standaarden, ambities spoorveiligheid en het toenemende vervoersaanbod?
- Op welke wijze, door welke verantwoordelijke organisatie dienen en voor wanneer kunnen deze verbetermaatregelen worden geïmplementeerd?

Antwoord:
Onze aanbevelingen zijn opgenomen in § 5.1.

5.1 Aanbevelingen

Op grond van onze visie op safety management (zie § 3.1) en de in dit rapport opgenomen bevindingen bevelen wij het volgende aan:

1. Zorg dat het MoC-proces wordt opgenomen in de VMS'en van ProRail en NS, en zorg ook dat de ontbrekende onderdelen integratie, verificatie en validatie in de beschrijving van het proces worden vastgelegd. Denkbare opties voor de vastlegging zijn:

   - PRC00278 wordt zodanig aangepast dat alle integrale V&V activiteiten zijn vastgelegd. MoC verwijst dan naar deze aangepaste PRC00278. Het VMS van NS verwijst naar het MoC of naar de PRC00278 en verklaart deze van toepassing voor systeem(concessie)overstijgende issues waar NS de initiatiefnemer van is. (Het VMS van ProRail bevat al de verwijzing naar PRC00278).

   - Een gewijzigd MoC document verwijst naar de huidige PRC00278 en voegt de afspraken over integrale V&V voor systeem(concessie)overstijgende issues in het MoC document toe. De VMS-en van NS en van ProRail verwijzen naar het MoC document.

- Het MoC document vervalt en de afspraken over integrale V&V voor systeem(concessie)overstijgende issues worden in de VMS-en van NS en van ProRail vastgelegd.

2. Formaliseer de actuele veiligheidsonderbouwing van de HSL-Zuid. De stappen daartoe zijn:
   - Maak de ISC weer een formeel document om de (delta)risicoredeneringen logisch gezien geldig te laten zijn/worden.
   - Stel vervolgens een uitgangspuntendocument op waarin aangegeven wordt welke onderdelen van de ISC relevant zijn als basis voor de risicoredeneringen. Van onderdelen die afvallen moet de reden en de consequentie (of ontbreken daarvan) aangegeven worden.

   De actuele veiligheidsonderbouwing van de HSL-Zuid bestaat dan uit:
   - de ISC HSL-Zuid (als referentiedocument, maar wijzigt niet meer);
   - het document met de (verwijzingen naar) uitgangspunten voor risicoredeneringen;
   - de volledige gevaren-inventaris conform de Europese verordening *CSM-REA* – de (delta)risicoredeneringen - en de veiligheidsverantwoording voor alle wijzigingen.

   Noot: Mogelijk dat blijkt dat er al een zodanige basis aan praktijkcodes is ontwikkeld, dat (een aanzienlijk deel van) de ISC 'vervallen' verklaard kan worden.

3. Bedeel de rol van veiligheidsvalidator expliciet toe aan het Veiligheids Advies Overleg (VAO) zoals dat binnen het MoC-proces bestaat.
   Noot 1: De auditers zien het VAO als een groep vertegenwoordigers van de betrokken partijen en niet alleen als de naam van een overleg.

   Noot 2: Gezien het feit dat het VAO bestaat uit vertegenwoordigers van de betrokken organisaties, is er een risico dat de leden van het VAO elkaar onvoldoende uitdagen om tot het maximaal haalbare veiligheidsniveau te komen. Dit risico kan zo nodig worden gemitigeerd door het VAO voor te laten zitten door een externe partij.

Uit de interviews bleek dat het aantal in behandeling zijnde veiligheidsrelevante issues sterk is afgenomen. Het vervoersaanbod op de HSL-Zuid groeit echter nog. Daarom lijkt het zinvol en praktisch om de verbeteringsacties binnen afzienbare tijd te starten: verbeteren wanneer het kan en op sterkte zijn wanneer het moet.

5.2 Samenvattende conclusie

De structurele afstemming tussen de betrokken partijen in het MoC-proces is naar de mening van de auditors noodzakelijk vanwege de nog niet bewezen 'rijpheid' van het systeem (zie par. 1.6 Afkortingen en begrippen), de complexiteit en het risicoprofiel van de HSL-Zuid (kans op ongevallen met zeer ernstige gevolgen vanwege de hoge snelheid).

Het MoC-proces beoogt mede invulling te geven aan de samenwerkingsverplichting op veiligheidsgebied zoals die door de Europese Spoorwegveiligheidsrichtlijn wordt opgelegd. Uit de auditresultaten blijkt dat op een aantal punten de veiligheidsborging verbeterd kan worden. Wanneer de hierboven genoemde aanbevelingen worden

opgevolgd, dan zorgt naar onze mening het MoC-proces voor een adequate veiligheidsborging op de HSL-Zuid.

Colofon

Opdrachtgever Ministerie Infrastructuur & Milieu
H.J. Heeres

Uitgave Movares Nederland B.V.

Postbus 2855
3500 GW Utrecht

Telefoon 030-2654699

Ondertekenaar A. Eigenraam
Consultant

Projectnummer RA001884

Opgesteld door A. Eigenraam, R. de Zutter

Bijlage I Auditresultaten

De audit bestaat uit de volgende onderdelen:

- Bureaustudie
  - Bestudering van Europese spoorwegveiligheidsregelgeving (bevindingen genummerd als Bevinding Ri);
  - Bestudering van Nederlands spoorwegveiligheidsbeleid (bevindingen genummerd als Bevinding Bi);
  - Bestudering van relevante documentatie met betrekking tot de HSL-Zuid (bevindingen genummerd als Bevinding Di);
- Interviews (bevindingen genummerd als Bevinding Ii).

Europese spoorweg-veiligheidsregelgeving

Bij de exploitatie van spoorwegsystemen zijn twee soorten partijen betrokken: infrastructuurbeheerders en spoorwegondernemingen. De Europese Spoorwegveiligheidsrichtlijn [Richtlijn SV] stelt dat iedere partij verantwoordelijk is voor zijn eigen systeemdelen en dat partijen dienen samen te werken bij de uitvoering van risicobeheersingmaat-regelen (zie kader). Dit is vastgelegd in Artikel 14 lid 3 van de Richtlijn. De Richtlijn stelt geen nadere eisen aan en geeft geen nadere invulling van de samenwerkingsverplichting.

> Spoorwegveiligheidsrichtlijn, overweging (5): Allen die het spoorwegsysteem exploiteren, de infrastructuurbeheerders en spoorwegondernemingen, dragen de volle verantwoordelijkheid voor de veiligheid van het systeem, elk voor zijn eigen deel. Telkens wanneer dat nodig is, dienen zij samen te werken bij de uitvoering van de risico-beheersingsmaatregelen. De lidstaten moeten een duidelijk onderscheid maken tussen deze directe verantwoordelijkheid voor de veiligheid en de taak van de veiligheidsinstanties om een regelgevingskader te bieden en toezicht te houden op de prestaties van de exploitanten.

Op wijzigingen van het vervoersysteem is de Europese Verordening over een gemeen-schappelijke veiligheidsmethode voor risico-evaluatie en -beoordeling [CSM-REA] van toepassing. Deze stelt eisen aan het risico-beheerproces en de onafhankelijke beoordeling daarvan. In Bijlage 1, paragraaf 1.1 van deze verordening (Algemene verplichtingen en beginselen) wordt gesteld dat, met het oog op het beheer van de gevaren en de bijbehorende veiligheidsmaatregelen, de initiatiefnemer[8]:

- een document dient op te stellen met een beschrijving van de taken van de verschillende actoren en hun activiteiten inzake risicobeheer;
- de nauwe samenwerking tussen de verschillende betrokken partijen coördineert.

Ook [CSM-REA] stelt geen nadere eisen aan en geeft geen volledige invulling van de samenwerkingsverplichting uit de Spoorwegveiligheidsrichtlijn. [CSM-REA] heeft alleen betrekking op fase 1 t/m 5 van het V-model uit [EN50126] en gaat niet in op systeemintegratie en -validatie.

Bevinding R1

De Spoorwegveiligheidsrichtlijn bevat een samenwerkingsverplichting voor alle bij het spoorsysteem betrokken partijen.

[8] de persoon of instantie die verantwoordelijk is voor de tenuitvoerlegging van de wijziging.

Bevinding R2

De CSM-REA gaat in op deze samenwerking, maar heeft alleen betrekking op fase 1 t/m 5 van het V-model. Aan systeemintegratie- en -validatie worden in de Europese spoorwegveiligheidsregelgeving geen eisen gesteld, de verantwoordelijkheid hiervoor is niet belegd.

Bevinding R3

De CSM-REA stelt dat de initiatiefnemer voor een wijziging een gevareninventaris bijhoudt. Aangezien zowel een beheerder als een vervoerder initiatiefnemer kan zijn, bestaat er een reëel risico dat er geen integraal overzicht van gevaren is.

Railveiligheidsbeleid

Het Nederlandse railveiligheidsbeleid voor de middellange termijn (2010-2020) is vastgelegd in de Derde Kadernota Railveiligheid [Kadernota]. De Kadernota geeft de samenhang aan van de belangrijkste issues van de spoorwegveiligheid en beschrijft bestaand en nieuw beleid om de spoorwegveiligheid permanent te verbeteren (zie kader).

Veiligheidsvisie: permanent verbeteren

Bij het streven naar permanente verbetering gaat het om een proces van permanente reductie van de kans op doden, gewonden en schade. Ook als de doelstellingen daarvoor zijn gehaald, blijft het principe gelden dat maatregelen met een positief effect op de veiligheid zeker niet mogen worden nagelaten als deze wenselijk, haalbaar en betaalbaar zijn ('van goed naar beter'). Dit wordt ook wel verwoord met het principe 'As Low As Reasonably Practicable' (ALARP)

De formulering van veiligheidsdoelstellingen in de Kadernota sluit aan op de Europese indicatoren en definities. De doelstellingen zijn gericht op het permanent verbeteren van de veiligheid (ALARP, zie kader) voor alle risicodragers (reizigers, personeel, overweggebruikers etc.).

De Kadernota gaat ook in op de verantwoordelijkheidsverdeling. Er wordt onderscheid gemaakt tussen systeemverantwoordelijkheid en operationele verantwoordelijkheid voor de veiligheid van het spoorvervoer. De minister van I&M is systeemverantwoordelijk voor de veiligheid van het hoofdspoor. De minister is verantwoordelijk voor de inrichting en de werking van het stelsel. Daarbij gaat het om het bepalen en vastleggen van de regels, de toedeling van verantwoordelijkheden en de inrichting van het toezicht. De operationele verantwoordelijkheid is via wet- en regelgeving belegd bij infrastructuurbeheerders en vervoerders.

Bevinding B1 *De minister van I&M is systeemverantwoordelijk voor de veiligheid van het hoofdspoor.*

Bevinding B2

Het ALARP-principe is een belangrijke pijler om de spoorwegveiligheid permanent te verbeteren.

Integrale safety case

De Integrale safety case HSL-Zuid [ISC HSL] bevat o.a. de veiligheidsdoelstellingen (waaronder ALARP) uit het Integraal Veiligheidsplan. De veiligheidsanalyses waaraan in de [ISC HSL] wordt gerefereerd zijn gebaseerd op een exploitatiemodel van de HSL-Zuid tot 2022 .[9]

[9] [ISC HSL] p.93: Er is een "lichter" exploitatiemodel onder HS31a als nieuw uitgangspunt genomen voor de berekeningen ten aanzien van treinontsporing, omdat de concessie periode van de vervoerder "maar" tot 2022 loopt. Infraspeed hoeft niet nu al maatregelen te nemen, maar pas als dit voorzien noodzakelijk wordt.

Bevinding D1

De veiligheidsonderbouwing in de [ISC HSL] is gebaseerd op het voorziene gebruik in 2022.

Concessies

Voor de HSL-Zuid zijn twee concessies verleend:

- Een beheerconcessie, deze is verleend aan ProRail;
- Een vervoerconcessie, deze is verleend aan NS.

In de Concept-ontwerpbeheerconcessie 2015-2025 [Beheerconc.] wordt expliciet gerefereerd aan de Spoorwegveiligheidsrichtlijn [Richtlijn SV] en bijbehorende verordeningen (met rechtstreekse werking), en aan de permanente verbetering van de veiligheid.

Bevinding D2

De beheerconcessie bevat expliciete eisen met betrekking tot veiligheid.

De Vervoerconcessie voor het hogesnelheidsnet[10] [Vervoerconc.] bevat geen verwijzingen naar wet- en regelgeving en/of beleid m.b.t. spoorwegveiligheid. Er zou wel een bijlage zijn waarin eisen met betrekking tot veiligheid zijn opgenomen, maar hierover beschikken de auditors niet. De opdrachtgever heeft aangegeven dat in de nieuwe concessie de nieuwe (Europese en nationale) wet- en regelgeving wordt opgenomen.

Bevinding D3

Tijdens de audit was er geen schriftelijk bewijs beschikbaar dat de huidige vervoerconcessie eisen met betrekking tot veiligheid bevat.

Veiligheidsmanagement HSL-Zuid

Het memo ‘Aanpak integraal safety management’[Aanpak ISM] geeft een onderbouwing vanuit de wet- en regelgeving voor het niet noodzakelijk zijn van het onderhouden van de Integrale Safety Case HSL-Zuid [ISC HSL]. De conclusie in dit memo luidt: “Er is dus geen separaat organisatieonderdeel in de gebruiksfase van de HSL-Zuid dat expliciet de verantwoordelijkheid draagt voor systeemintegratie of het aantonen van de integrale veiligheid. Deze verantwoordelijkheid ligt bij de sector als geheel.”

Bevinding D4

Geen van de bij de HSL-Zuid betrokken partijen is verantwoordelijk voor systeemintegratie en integrale veiligheidsverantwoording.

Wijzigingsproces HSL-Zuid

Proces

De veiligheidsgerelateerde activiteiten in het MoC-proces zijn vermeld in de uitgangspunten van [MoC]:

- *Het CMT als voorzitter VAO borgt de werkwijze en methodieken ten behoeve van het opstellen, bijhouden en beschikbaar stellen van de veiligheidsbewijsvoering. Let wel: de betrokken partijen blijven zelf verantwoordelijk voor de borging van de veiligheid, d.w.z. het juist vaststellen van de risico's en mitigerende maatregelen alsmede invoering van de maatregelen en het opstellen van de daarmee samenhangende bewijsvoering.*
- *Door deelname aan analyse, hazard identificatie en het overeenkomen van mitigerende maatregelenmaatregelen bij het oplossen van veiligheidsissues, geven de betrokken partijen invulling aan een deel van hun veiligheidsverantwoordelijkheid.*

[10] Looptijd 2009-2024

Bevinding D5

De beschrijving van het veiligheidsmanagement proces in [MoC] blijft beperkt tot de risico-inventarisatie en -evaluatie en de inhoudelijke vaststelling van de te nemen maatregelen.

Bevinding D6

Implementatie van de wijzigingen in de eigen systemen en processen is een verantwoordelijkheid van de partijen zelf.

Bevinding D7

Systeemintegratie en (veiligheids)validatie van het eindresultaat van de wijzigingen in hun samenhang zijn niet belegd.

Bevinding D8

[MoC] beschrijft geen planmatige aanpak van het integrale veiligheids-management.

Veiligheidsverantwoording

Over de status van [ISC HSL] staat in [MoC] het volgende:

- *De [ISC HSL] is in 2008 opgeleverd en bevroren en dient als naslagwerk. Een deel van de oorspronkelijke ISC, de zogenaamde EFFBD's (beschrijvingen interface interacties) en bijbehorende risicoanalyses is nog tot 2010 onderhouden en vervolgens ook bevroren . Het Beheerteam ISC is eind 2010 opgeheven. Het veiligheidsbewijs in de vorm van een separate risicoanalyse voor elke systeemoverstijgende wijziging wordt sindsdien onderhouden door het VAO.*
- *De [ISC HSL] is in oktober 2008 opgeleverd door het HSL-Zuid project. De ISC wordt sinds die tijd niet meer onderhouden maar functioneert nog wel als naslagwerk bij het uitvoeren van de veiligheidsanalyses (zogenaamde risicoredeneringen).*

Bevinding D9

De [ISC HSL] wordt niet onderhouden maar dient als (vrijblijvend) naslagwerk.

Bevinding D10

Voor elke wijziging wordt een separate risico-inventarisatie en -evaluatie gemaakt ('delta-analyse').

Bevinding D11

[MoC] bevat geen integrale toetscriteria voor de aanvaardbaarheid van het restrisico zoals vastgelegd in de [ISC HSL] (par. 3.4) en in de [Kadernota]

PRC00278

Het belangrijkste aanknopingspunt v.w.b. het gevolgde V&V proces binnen MoC is procedure PRC00278. MoC heeft als uitgangspunt dat bij wijzigingen deze procedure wordt gevolgd.
Daarom is deze procedure nader bekeken (zie [Vragen I&M]).

Bevinding D12

Nadruk ligt op het aantonen van de juistheid van en het voldoen aan de vereisten per eigenaar. Er wordt niet duidelijk gemaakt of er ook aangetoond wordt dat de wijzingen in hun samenhang (veilig) werken en of er onderzoek gedaan is naar mogelijke regressie van het (niet-gewijzigde deel van het) systeem.

Bevinding D13

Wanneer de PRC00278 ook voor systeemgrensoverstijgende (concessieoverstijgende) issues gevolgd wordt, dan dient het proces en de organisatie daarvan duidelijk beschreven te worden in het VMS van zowel ProRail als NS.

Bevinding D14

De processen en de terminologie in de CSM REA wijken af van verwante System Engineering (SE) processen en begrippen in de EN50126. Er is echter geen equivalent begrip gevonden voor validatie van het geheel.

Interviews

Bijlage II bevat citaten uit de interviews. De daaruit voortkomende bevindingen zijn hieronder overgenomen. Slechts een deel van de hier vermelde bevindingen wordt gebruikt bij het toetsen van de onderzoekshypothese en/of het beantwoorden van de onderzoeksvragen. De niet gebruikte bevindingen zijn wel van belang voor de beeldvorming over het functioneren van het MoC-proces.

Bevinding I1

De Stuurgroep HSL-Zuid speelt geen rol in het veiligheidsmanagement en/of MoC-proces.

Bevinding I2

Het Concessieteam is de beheerder van het MoC-proces..

Bevinding I3

Het MoC-proces is niet vastgelegd in de VMS-en van de betrokken partijen.

Bevinding I4

Alle veiligheidsmanagement activiteiten binnen het MoC-proces worden door het VAO uitgevoerd. Dit beperkt zich volgens de MoC-procesbeschrijving (zie [MoC]) tot de risico-inventarisatie en -evaluatie en het vaststellen van de benodigde maatregelen en daarvoor benodigde wijzigingen.

Bevinding I5

Het systeemintegratieproces en de (veiligheids)validatie van wijzigingen van het vervoersysteem als geheel zijn niet vastgelegd / niet belegd. Uit de interviews blijkt dat er integratietesten hebben plaatsgevonden.

Bevinding I6

Het MoC-proces is alleen nodig voor issues en wijzigingen waarvoor de concessiehouders moeten samenwerken.

Bevinding I7

Het standpunt van ILT (voorheen IVW) dat wijzigingen niet per se in [ISC HSL] behoeven te worden verwerkt, heeft geresulteerd in risicoredeneringen per issue. Hierbij wordt ervan uitgegaan dat de veiligheid reeds bewezen is in [ISC HSL].

Bevinding I8

NS en Infraspeed moeten contractueel hun eigen (deel) safety case onderhouden.

Bevinding I9

In het MoC-proces is er geen vastlegging van de onderbouwing van de veiligheid van het vervoersysteem als geheel, bijvoorbeeld conform [EN 50129] (top level safety case met zgn. related safety cases).

Bevinding I10

Het VAO is niet de systeemintegrator van de HSL-Zuid, maar is een instantie waar een aantal safetymanagementactiviteiten is belegd. De taak omvat niet de bewaking en veiligheidsverantwoording van gerealiseerde wijzigingen in hun samenhang en het effect daarvan op het vervoersysteem.

Bevinding I11

Het is praktisch om de de rol van systeemintegrator bij ProRail te beleggen. De

systeemintegrator verricht die safety management activiteiten die nodig zijn om tot een integrale veiligheidsverantwoording te kunnen komen.

Bevinding I12

Het huidige MoC-proces als geheel is vooral een consensusproces. Goede veiligheidsbeoordeling vraagt een "challenging"/prikkelende houding van partijen. Deze prikkeling is in een consensusproces niet te verwachten.

Bevinding I13

Een beheerst wijzigingsproces en een integrale veiligheidsverantwoording zijn op de HSL-Zuid noodzakelijk vanwege nog niet bewezen rijpheid van het systeem en complexiteit van zowel het vervoersysteem als de organisatie, en vanwege het risicoprofiel (kans op ongevallen met zeer ernstige gevolgen vanwege de hoge snelheid).

Bevinding I14

Omdat er bij de veiligheidsanalyses ten behoeve van [ISC HSL] is uitgegaan van de maximale capaciteit en deze maximale capaciteit nog niet is bereikt, is er geen zorg over de veiligheid van de HSL-Zuid bij groeiend verkeersaanbod.[11]

Bevinding I15

Bij groeiend verkeersaanbod is de gevoeligheid van het vervoersproces voor storingen voor ILT een punt van zorg. De afhandeling van veelvuldig stilvallende treinen heeft impact op de veiligheid.

[11] De veiligheidsanalyses waaraan in de [ISC HSL] wordt gerefereerd zijn gebaseerd op een exploitatiemodel van de HSL-Zuid tot 2022. Zolang het vervoersaanbod niet verder groeit dan de prognose 2022 is de conclusie uit de [ISC HSL] geldig.

Bijlage II Interviews

Als onderdeel van de audit zijn interviews afgenomen met de diverse vertegenwoordigers van de bij het MoC-proces betrokken partijen. Op basis van de beschrijving van de MoC-overlegstructuur zijn voor de interviews de volgende personen geselecteerd:

- Lieske Streefkerk-Arts (Ministerie van I&M), voorzitter Stuurgroep;
- Joost Kolkman (Ministerie van I&M), secretaris Stuurgroep;
- Jan Tiecken (ProRail-AM, contractmanager HSL-Zuid), lid Stuurgroep en Concessieteam;
- Ron Heeren (NS-International, hoofd operations, lid Stuurgroep en Concessieteam (plaatsvervangend voorzitter);
- Vincent Verbeet (NS-International, programmadirecteur HSL-aanbod), lid Stuurgroep;
- Bas Oosthoek (ProRail-AM), lid Stuurgroep, voorzitter Operationeel Issue Overleg en Issue Management Overleg;
- Henny Koppens, ILT (agenda)lid Stuurgroep;
- Mariet Brinkman (ProRail-V&D, accountmanager NS, voorzitter Concessieteam;
- Thijs van Reenen (ProRail-AM, tot 6-10-2014 lid Contract Management Team), tot 6-10-2014 lid voorzitter Veiligheids Advies Overleg.
- Bas Roordink (ProRail-AM, sinds 6-10-2014 lid Contract Management Team), sinds 6-10-2014 lid voorzitter Veiligheids Advies Overleg.
- Jasper Egmond, voorzitter Technisch Issue Overleg en Beheerteam ERTMS;
- Remco de Looff, Infraspeed, lid Stuurgroep[12];
- Arnold Hornung, Infraspeed, lid Stuurgroep[12].

De gesprekken zijn in een open atmosfeer gevoerd, de antwoorden zijn consistent. Verschillen worden vooral veroorzaakt door het perspectief van waaruit het MoC-proces door de geïnterviewde wordt beschouwd, en door de aard van zijn of haar betrokkenheid bij het proces.

De bevindingen naar aanleiding van de interviews zijn vermeld in Bijlage 1.

[12] De vertegenwoordigers van Infraspeed zijn niet geïnterviewd, maar hebben de auditvragen schriftelijk beantwoord.

De in deze bijlage opgenomen citaten (*cursief*) uit de gesprekken zijn gegroepeerd naar de volgende onderwerpen:

- Stuurgroep
- Concessieteam (CT)
- Proces
- Integratierol
- Vastlegging
- HSL-Zuid versus conventioneel spoor

Stuurgroep:

- *De voorzitter van de Stuurgroep HSL-Zuid vertegenwoordigt de systeemverantwoordelijkheid van de minister.*
- *De Stuurgroep houdt zich (op tactisch/strategisch niveau) bezig met partij overstijgende zaken, voornamelijk m.b.t. gebruik (nieuwe vervoerproducten) en functionaliteit van de HSL.*
- *Beslissingen worden genomen bij consensus.*
- *Belangrijk verschil met het Concessieteam is dat ook Infraspeed aan tafel zit.*
- *Het project is nog steeds een groot project voor 2de kamer, mede daarom is de Stuurgroep gehandhaafd.*
- *De Stuurgroep speelt geen rol in het MoC-proces.*

Concessieteam (CT):

- *In het CT zijn de concessiehouders van de HSL-Zuid vertegenwoordigd.*
- *Doel van het CT is verbetering van de samenwerking tussen partijen t.b.v. verbetering van de performance: doelstellingen m.b.t. punctualiteit / uitval en evt. benodigde maatregelen met elkaar afspreken.*
- *Het CT bepaalt de prioriteiten en planning. De Stuurgroep is dan een escalatieniveau met 'verbreding' door de aanwezigheid van o.a. Infraspeed.*
- *Na de opheffing van het Opstartteam (reden: het is nu een stabiel vervoersysteem) is het wijzigingsbeheer cf. het MoC-proces overgedragen aan het Concessieteam.*
- *Het mandaat voor de uitvoering van wijzigingen ligt bij de lijnorganisaties van de betrokken partijen. Vanwege de overlegstructuur is het risico klein dat na een CT akkoord blijkt dat Infraspeed niet meegaat in de wijziging.*

Proces:

- *Na het afsluiten van de bouwfase werd de ISC niet meer onderhouden. Het MoC-proces is toen ontstaan om te bewaken en te borgen dat het systeem (veilig) blijft werken. In het document Borging MoC werd het proces vastgelegd zoals dat gegroeid was.*
- *Het MoC-proces is primair bedoeld voor veiligheidsrelevante wijzigingen.*
- *MoC is een invulling en operationalisering van het VMS (issues op raakvlak vervoer en HSL-infrastructuur).*
- *Het MoC-proces is niet expliciet in het VMS opgenomen.*
- *Het VMS borgt het V&V proces, maar dat wordt niet behandeld in MoC.*

- *Ondanks dat integrale V&V dus niet is vastgelegd zijn voor de wijziging van de national values wel degelijk testplannen gemaakt. Dit wordt ook vereist vanuit het VMS. ProRail voerde hierbij de regie.*
- *MoC is ontstaan bij de oplevering van de ISC. Toets Luxcontrol: ProRail moet iets doen aan veiligheidsmanagement in de opstartfase.*
- *VAO zorgt voor veiligheidsonderbouwing t.b.v. besluitvorming. Validatie van het eindresultaat is niet belegd.*
- *In het VAO worden de veiligheidsaspecten beoordeeld en vastgelegd in een veiligheidsverantwoording (veiligheidsredenering). Op basis hiervan gaat een advies naar het OIO. Vervolgens gaat dit advies naar CT/Stuurgroep. Goedkeuring in CT/Stuurgroep is eigenlijk slechts een formele vaststelling.*
- *Het proces is wat reactief, echte validatieactiviteiten lijken er niet te zijn. Niet alles staat echter in het MoC-proces beschreven, er zijn wel degelijk terugkoppelingen (binnen partijen) over het eindresultaat.*
- *Wijzigingen die niet systeem overstijgend zijn hoeven niet het MoC-proces te doorlopen.*
- *…De wijziging is concessieoverstijgend maar qua veiligheid niet systeemgrensoverstijgend.*
- *Als een issue binnen de eigen organisatie oplosbaar is, dan is MoC niet nodig.*

Vastlegging:

- *Na het afsluiten van de bouwfase werd de ISC niet meer onderhouden.*
- *IVW heeft daar een punt van gemaakt: wijzigingen hoeven niet per se in de ISC verwerkt te worden, maar er moet wel 'iets' worden gedaan om veiligheid bij wijzigingen te onderbouwen, dat is het MoC-proces geworden.*
- *Tevens is het zo dat er bij de HSL een noodzaak is om veiligheidsissues expliciet te documenteren in de respectievelijke safety cases (NS, Infraspeed). Hierdoor is er meer opdruk een MoC-proces in te richten.*
- *De veiligheidsbewijsvoering bestaat uit risicoredeneringen, evt. onderliggende analyses/rapporten, verwijzingen naar bestaande veiligheidsdocumentatie.*
- *Daarnaast zijn er de deel-safety cases van de betrokken partijen.*
- *Naleving van veiligheidsprincipes en –concepten is door het loslaten van de ISC niet echt meer geborgd.*
- *Infraspeed is van mening dat ook de integrale systeemgrensoverstijgende safety case moet worden 'onderhouden' en in geval van wijzigingen geactualiseerd.*

Integratierol:

- *Voorzitterschap VAO was een bewuste keuze. De ISC is destijds bij ProRail neergelegd. ProRail heeft toen besloten om de ISC niet te onderhouden, maar dan moest de veiligheid wel op een andere wijze geborgd blijven. Daartoe is het VAO ingesteld met ProRail als voorzitter.*
  Het voorzitterschap kan evt. bij een andere partij liggen, maar heeft vanuit pragmatisme niet de voorkeur.

- *ISC had eigenlijk bij de Staat, als systeemintegrator, moeten liggen. Als 'uitvoeringsorganisatie' van de Staat is het logisch dat deze dan bij ProRail komt te liggen en niet bij één vervoerder.*
  Als RWS was blijven bestaan als beheerder van de hogesnelheidsinfra, dan was de ISC waarschijnlijk daar gebleven.
- *… systeemintegrator nodig is om het geheel af te hechten, incl. validatie van het eindresultaat.*
  "We hebben hem nodig maar niemand wil dat". Een logische plek om de rol van systeemintegrator te beleggen is het ministerie, een praktische plek is ProRail.
- *MoC is een consensus proces (poldermodel) waardoor men mogelijk al gauw tevreden is (risico van gezapigheid). Een systeemintegrator van buitenaf zal waarschijnlijk meer challenging zijn.*
- *Voor het ERTMS programma heeft I&M hiervoor een systeemintegrator aangesteld (procesmatige rol tussen de partijen).*
- *Ook voor conventioneel spoor ontbreekt een systeemintegrator. Bij systeemoverstijgende issues wordt er vaak eerst naar elkaar gewezen, voordat er een gezamenlijke actie ontstaat. De aanpak van STS passages kwam hierdoor ook moeizaam tot stand. Hier is uiteindelijk wel een Stuurgroep STS onder leiding van ProRail opgezet.*

HSL-Zuid versus conventioneel spoor:

- *De baan-trein interactie op de HSL is anders dan op conventioneel spoor. Daarnaast is de safety case en de daarop volgende MoC-procesgang een verplichting vanuit de HSL concessie.*
- *Iets extra's (MoC dus) is op HSL-Zuid nodig vanwege nieuw beveiligingssysteem (ERTMS) en hoge snelheid.*
- *MoC-proces is voor het hogesnelheidsvervoerssysteem nodig om de risico's die kleven aan het met hoge snelheid rijden beheerst gemitigeerd moeten worden en zeker gesteld moet worden dat het vervoersysteem integraal integer blijft.*
- *De reden om dit bij HSL te doen is hiervoor al aangegeven: de speciale setting met IFS en Staat.*
- *Belangrijk issue "Verbindingsverlies": Je zou zeggen dat dit gewoon opgelost kon worden binnen de concessie, maar dat lukte niet door de houding van Infraspeed t.a.v. het contract.*
  ILT ziet Infraspeed als "gewone" aannemer.
- *Er is bij ILT geen zorg over de veiligheid van de HSL-Zuid, ook niet bij groeiend vervoersaanbod: de ISC gaat uit van maximale capaciteit. Wel is er zorg of de HSL-Zuid robuust genoeg is als er veel meer treinen gaan rijden dan nu.*