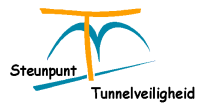




Veiligheidskritische functies in tunnels

Bepaling van de vereiste betrouwbaarheid van de
(geautomatiseerde) veiligheidssystemen

Datum 27 december 2011
Status Versie 1.1, Definitief



Veiligheidskritische functies in tunnels

Bepaling van de vereiste betrouwbaarheid van de
(geautomatiseerde) veiligheidssystemen

Datum 27 december 2011
Status Versie 1.1, Definitief

Colofon

Uitgegeven door Steunpunt Tunnelveiligheid
 Informatie
 Telefoon
 Fax
 Uitgevoerd door Ronald Mante
 Gecontroleerd door Versie 1:
 Tineke Wiersma, Jelle Hoeksma, Wim Janssen,
 Ronald Gram, Josephine L'Ortye, Jan van Wijgerden,
 Sipke van Manen

 Versie 1.1:
 Tineke Wiersma, Jelle Hoeksma en Ben Pronk
 Geautoriseerd door Ronald Mante
 Vrijgegeven door
 Datum 27 december 2011
 Documentnummer 4818-2011-0034
 Status Versie 1.1
 Versienummer Definitief

Documentgeschiedenis		
Versie	Datum	Toelichting
Concept 1	13 april 2011	Eerste werkversie.
Concept 2	18 april 2011	Nadere invulling prestatie-eisen.
Concept 3	6 juni 2011	Nadere inbedding gebruik TOPAAS, nadere formulering betrouwbaarheidseisen en conclusies en aanbevelingen. Tevens aanvullende berekeningen toegevoegd.
Versie 1, Definitief	20 juni 2011	Intern door werkgroep goedgekeurde versie.
Versie 1.1, Concept 1	28 november 2011	Resultaten externe toetsing verwerkt, o.a. commentaar van Advisory Board Landelijk Tunnelregisseur (Helsloot, Vrijling en Leegwater).
Versie 1.1, Eindconcept	20 december 2011	Opmerkingen toetsing concept 1 verwerkt.
Versie 1.1, Definitief	27 december 2011	Definitief gemaakt na instemming Change Advisory Board Landelijk Tunnelregisseur.

Inhoud

1	Inleiding 7
1.1	Aanleiding 7
1.2	Doel 8
1.3	Opbouw rapport 9
2	Nadere beschrijving IEC-61508 en TOPAAS 10
2.1	IEC-61508 10
2.2	TOPAAS 12
3	Aanpak 14
3.1	Inleiding 14
3.2	Layers of Protection 15
3.3	Berekening Risk Reduction Factoren met RWSQRA versie 2.0 17
4	Resultaten 20
4.1	Geautomatiseerde veiligheidssystemen conform de VRC 20
4.2	Aanvullingen op basis van gevarenanalyse 22
4.3	Risk Reduction Factoren van veiligheidsmaatregelen 24
5	Specificatie veiligheidskritische functies 27
5.1	Inleiding 27
5.2	Tunnelventilatie 28
5.3	Veilige vluchtweg 30
5.4	Beheerst afsluiten 35
5.5	Filevermijding 36
5.6	Calamiteitenknop 37
6	Conclusies en aanbevelingen 40
6.1	Conclusies 40
6.2	Aanbevelingen 41
	Lijst van aangehaalde literatuur 42
	Bijlage A Gevarenanalyse 43
	Bijlage B Berekening Risk Reduction Factoren 49

1 Inleiding

1.1 Aanleiding

In Rijkstunnels worden diverse veiligheidsmaatregelen getroffen om aan de wettelijke eisen en de veiligheidsrichtlijnen van Rijkswaterstaat te voldoen. Dit betreffen zowel technische als organisatorische maatregelen.

Binnen de verzameling technische maatregelen vragen de geautomatiseerde veiligheidssystemen nadere aandacht in het kader van functionele veiligheid. Functionele veiligheid betreft het deel van de tunnelveiligheidsmaatregelen, dat afhankelijk is van het correct functioneren van een of meer technische, software intensieve systemen, die automatisch bepaalde preventieve of mitigerende maatregelen nemen, op basis van een (potentieel) gevaarlijke situatie die wordt gedetecteerd.

Bij deze systemen is het van belang dat er sprake is van "veilige software". Dit is software die:

- Doet wat gedaan moet worden om het veiligheidssysteem correct te laten functioneren (zodat de gewenste prestaties worden geleverd);
- Dat doet met de vereiste betrouwbaarheid;
- Fail safe gedrag vertoont indien de energievoorziening of de besturing uitvalt.

Probleem daarbij is onder andere, dat het borgen en kwantificeren van de betrouwbaarheid van software lastig is. Het is daardoor eveneens lastig om vast te stellen of de functionele veiligheid voldoende is geborgd.

De internationale norm om de functionele veiligheid (waaronder de betrouwbaarheid) van geautomatiseerde systemen te borgen is de IEC 61508: "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems".

Rijkswaterstaat heeft daarnaast het instrument TOPAAS¹ laten ontwikkelen en valideren, waarmee de betrouwbaarheid van software kan worden gekwantificeerd. Dit instrument wordt onder andere gebruikt om de betrouwbaarheid van de besturingssystemen van de beweegbare waterkeringen vast te stellen, te kunnen aantonen dat de keringen voldoen aan de wettelijke vastgestelde faalkanseisen.

Beide methoden (IEC-61508 en TOPAAS) hebben een andere scope en invalshoek, maar vertonen ook raakvlakken. De IEC-norm stelt eisen en randvoorwaarden aan de totstandkoming en de instandhouding van de software-intensieve systemen, om op die wijze de functionele veiligheid (waaronder de betrouwbaarheid) te borgen. Indien aantoonbaar aan bepaalde eisen en randvoorwaarden is voldaan, dan kan het bijbehorende niveau van functionele veiligheid ("Safety Integrity Level, SIL-niveau) worden "geclaimd". De betrouwbaarheid wordt hierbij dus niet rechtstreeks aangetoond, maar aannemelijk gemaakt door het gevolgde proces en de genomen ontwerpmaatregelen.

¹ TOPAAS = Task Oriented Probability of Abnormalities Analysis for Software.

Bij TOPAAS ligt echter de nadruk op het kwantificeren van de betrouwbaarheid van het resultaat, dus de software zelf, zodat door middel van een foutenboomanalyse kan worden aangetoond dat aan de betrouwbaarheidseisen wordt voldaan. Het kwantificeren van de softwarebetrouwbaarheid gebeurt met TOPAAS op basis van kenmerken van zowel het product als het gevolgde proces. Overeenkomst is dus dat zowel de IEC-norm als TOPAAS belang hechten aan een gestructureerd totstandkomingsproces. Dit betekent dat het totstandkomingsproces van de software "aan de voorkant" zodanig kan worden ingericht, dat dit leidt tot een resultaat dat qua betrouwbaarheid hoog scoort in TOPAAS. Zo leidt bijvoorbeeld ook de toepassing van de IEC-61508 tot hoge scores. Beide methoden kunnen dus los van elkaar, maar ook complementair aan elkaar worden toegepast.

Bij veel van de momenteel lopende tunnelprojecten bij Rijkswaterstaat loopt men tegen de vraag aan hoe moet worden omgegaan met functionele veiligheid, hoe de norm IEC-61508 en/of TOPAAS moeten worden toegepast in samenhang met de wettelijke eisen, en, meer specifiek, aan welke geautomatiseerde veiligheidssystemen hoge betrouwbaarheidseisen moeten worden gesteld omdat ze een grote rol spelen in het reduceren van de risico's voor de weggebruikers: de "veiligheidskritische functies".

Omdat het in het kader van uniformiteit en efficiency ongewenst is dat er per tunnelproject een eigen invulling wordt gegeven aan deze problematiek, is er in opdracht van de Landelijk Tunnelregisseur van Rijkswaterstaat een werkgroep gevormd, die de veiligheidskritische functies nader heeft gedefinieerd.

In deze werkgroep hadden vertegenwoordigers zitting van het Steunpunt Tunnelveiligheid (STV), Bureau Veiligheidsbeambte (BVB) en de Landelijk Tunnelregisseur (LTR):

- Ronald Gram (LTR, voorzitter);
- Jan van Wijgerden (LTR);
- Jelle Hoeksma (BVB);
- Wim Janssen (BVB);
- Tineke Wiersma (STV);
- Josephine L'Ortye (STV);
- Ronald Mante (STV).

Dit rapport is een weergave van de aanpak, bevindingen, conclusies en aanbevelingen van de werkgroep.

1.2

Doel

Dit rapport heeft tot doel om te definiëren wat de veiligheidskritische functies in een Rijkstunnel zijn, en welke prestatie- en betrouwbaarheidseisen bij deze functies horen.

Deze informatie kan worden gebruikt als basis voor het ontwerp en de instandhouding van nieuwbouwtunnels en aanpassingen van bestaande tunnels, op basis de tunnelstandaard van de LTR, in combinatie met de norm IEC-61508 en/of TOPAAS.

1.3 **Opbouw rapport**

Na deze inleiding is het rapport als volgt opgebouwd. **Hoofdstuk 2** geeft allereerst een nadere beschrijving van zowel de IEC-61508 als TOPAAS. Vervolgens beschrijft **hoofdstuk 3** de gevolgde aanpak van de werkgroep om te komen tot een vaststelling van de veiligheidskritische functies met de bijbehorende betrouwbaarheidseisen. De resultaten van deze aanpak komen in **hoofdstuk 4** aan bod. In **hoofdstuk 5** worden vervolgens de veiligheidskritische functies nader beschreven. In **hoofdstuk 6** worden tenslotte nog enkele conclusies en aanbevelingen gegeven.

2 Nadere beschrijving IEC-61508 en TOPAAS

2.1 IEC-61508

De norm IEC-61508 [1] gaat uit van een lifecycle benadering, waarbij eisen worden gesteld aan de (beheers)maatregelen die moeten worden genomen bij het ontwerp, de realisatie en de instandhouding (beheer en onderhoud) van de geautomatiseerde veiligheidssystemen. De omvang, aard en diepgang van deze maatregelen is afhankelijk van de prestatie-eisen die aan het veiligheidssysteem worden gesteld. Deze prestatie-eisen zijn op hun beurt afhankelijk van de aard en omvang van de veiligheidsrisico's die met het systeem moeten worden beheerst. Anders geformuleerd: hoe groter de bijdrage van het systeem aan de reductie van de veiligheidsrisico's van (in dit geval) de weggebruikers in de tunnel, hoe hoger de prestatie-eisen die aan het systeem worden gesteld. De maat die de IEC-norm definieert voor het vereiste prestatieniveau is het zogenaamde SIL-niveau: Safety Integrity Level. De norm onderscheidt 4 SIL-niveaus, waarbij SIL 1 de laagste en SIL 4 de hoogste eisen stelt. Het SIL-niveau van een veiligheidssysteem moet worden vastgesteld op basis van een risicoanalyse. Als het SIL-niveau is vastgesteld, dan is op basis van de IEC-norm duidelijk welke (beheers)maatregelen gedurende de levenscyclus van het systeem moeten worden genomen om de vereiste prestaties (blijvend) te borgen.

Het stappenplan (lifecycle phases) voor functionele veiligheid volgens de IEC-61508 is afgebeeld in de figuur op de volgende pagina.

De stappen zijn onder te verdelen in 3 hoofdfasen:

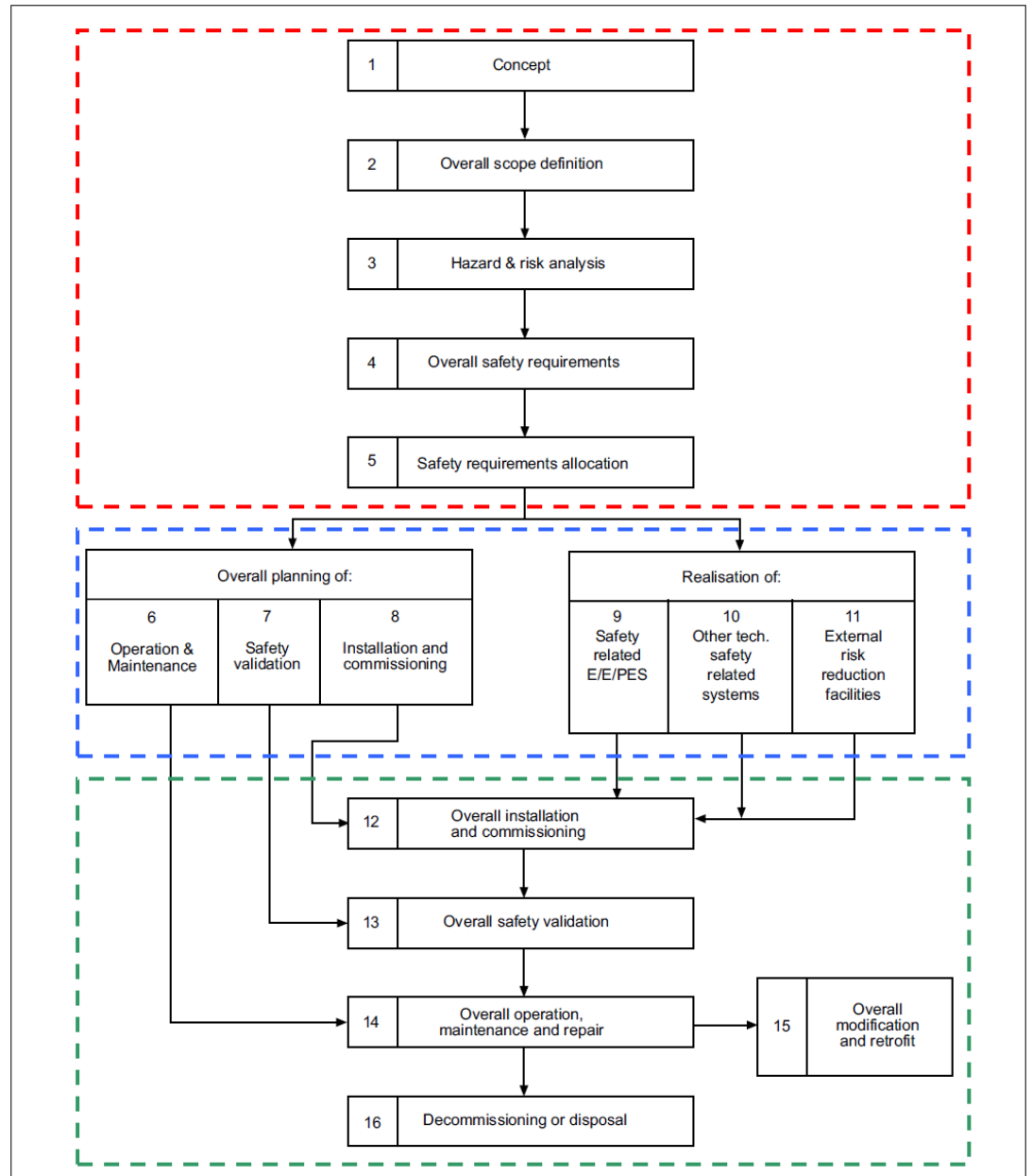
- Analyse (stap 1 t/m 5)
- Realisatie (stap 6 t/m 11)
- Gebruik (stap 12 t/m 16)

Dit rapport heeft in feite betrekking op de fase Analyse (stap 1 t/m 5).

Stap 1 en 2 hebben betrekking op het definiëren en afbakenen van het systeem en het proces waarvan de veiligheid moet worden geborgd. Het systeem is in dit geval een tunnel. Het proces is een veilige doorstroming van het verkeer door de tunnel: het voorkomen van ongevallen en (indien er onverhoopt toch ongevallen optreden) het beperken van letselschade.

Stap 3 t/m 5 hebben betrekking op het analyseren van de veiligheidsrisico's die moeten worden beheerst en het bepalen en vastleggen van de eisen waaraan moet worden voldaan om dit te bereiken:

- Identificeren en inschatten potentiële gevaren en risico's;
- Toetsen of de risico's voldoen aan de geldende normen;
- Nagaan of voldoende veiligheidsmaatregelen zijn genomen op de verschillende beschermingsniveaus (Layers of Protection);
- Bepalen welke geautomatiseerde veiligheidssystemen nodig zijn om te borgen dat er aan de veiligheidsnormen wordt voldaan;
- Bepalen SIL-niveau van de geautomatiseerde veiligheidssystemen en de verdere eisen die aan de systemen worden gesteld;
- Documenteren van de resultaten.



Bron: IEC-61508

N.B.:

De overige stappen (6 t/m 16) maken zoals gezegd geen deel uit van deze rapportage, maar zouden moeten worden doorlopen bij het verdere ontwerp, de realisatie en het beheer en onderhoud van de geautomatiseerde veiligheidssystemen, op basis van de (beheers)maatregelen die volgens de IEC-61508 moeten worden toegepast bij het gekozen SIL-niveau.

2.2 TOPAAS

TOPAAS [2] is in opdracht van Rijkswaterstaat ontwikkeld en gevalideerd door een consortium van Det Norske Veritas, Movares, Technische Universiteit Eindhoven, Logica, Refis en Intermedion. Het betreft een methode die zowel richtlijnen geeft voor het modelleren van software-falen in foutenbomen als het schatten van de faalkans van een taakuitvoering door een softwaremodule. Op basis van TOPAAS is het derhalve mogelijk om de faalkans van software te kwantificeren, zodat de betrouwbaarheid van een systeem als geheel (hardware + software) kan worden aangetoond door middel van een foutenboomanalyse. Wereldwijd is momenteel geen beter instrument beschikbaar om de betrouwbaarheid van software te kwantificeren. De methode is beschreven in [3].

Kern van TOPAAS is dat software in modules kan worden opgedeeld en dat het (mogelijk) falen van deze modules in een foutenboom als basisgebeurtenissen kunnen worden opgenomen². Falen van een software-module kan vervolgens opgedeeld worden in falen ten gevolge van de onverwachtheid van invoer en het falen van de beslislogica van de software-module zelf.

Falen ten gevolge van de onverwachtheid van invoer heeft te maken met het gebruik van de softwaremodule buiten de ontwerptoleranties, wat per definitie ongedefinieerde taakuitvoering van de softwaremodule tot gevolg heeft. Er is hierbij dus sprake van een mismatch tussen de invoer waar de softwaremodule voor is ontworpen en de werkelijke invoer die de omgeving genereert. Dit speelt in de regel alleen bij softwaremodules met een externe interface. Bij systemen met louter interfaces binnen het systeem zou onvoorziene invoer alleen het gevolg kunnen zijn van falen van een voorliggende component in de keten, waardoor deze component ongespecificeerde output/gedrag gaat vertonen, waardoor dus eigenlijk het falen op het conto van de voorliggende component moet worden gerekend.

De bepaling van een faalkans van de beslislogica van een softwaremodule gebeurt in TOPAAS op basis van expert opinion, waarbij het Bayesiaanse gedachtegoed wordt gevolgd. Deze expert opinion is vervat in een parametermodel, waarbij de factoren die in ogenschouw worden genomen voortkomen uit een expertgroep en internationaal onderzoek. De invloed van de factoren is ingeschat door experts en vervolgens gekalibreerd met een twintigtal referentieprojecten. Daarbij is vastgesteld dat de uitkomsten van het parametermodel een zeer sterke correlatie vertonen met de inschatting van de experts.

De parameters, op basis waarvan de faalkans van de softwaremodule wordt bepaald, zijn:

- Totstandkomingsproces
- Producteigenschappen
- Requirements traceability/verifieerbaarheid
- Testen
- Executieomgeving/gebruik

² Naast softwarematig falen dient in een foutenboomanalyse uiteraard ook rekening te worden gehouden met menselijk falen en hardwarematig falen.

De faalkans van de (beslislogica van de) softwaremodule bedraagt 10^x , waarbij de waarde van "x" afhankelijk is van de scores op bovengenoemde parameters.

Normaal gesproken is de resulterende waarde van "x" een negatief (rationeel) getal. De maximale faalkans van een module bedraagt uiteraard 1.

De bepaling van de faalkans van de softwaremodule gebeurt bij voorkeur door een onafhankelijk ICT-deskundige, in overleg met de softwarebouwer, in de vorm van een audit, waarbij de scores zoveel mogelijk worden onderbouwd met feitenmateriaal.

Om TOPAAS te kunnen toepassen, moeten er uiteraard eerst faalkanseisen worden vastgesteld voor de software, of beter gezegd, voor het systeem c.q. de veiligheidsfunctie waar de software deel van uit maakt. Deze eisen moeten worden uitgedrukt in concrete getallen, en niet zoals bij de IEC-61508 in een SIL-niveau. Omdat TOPAAS echter geen methode geeft voor het afleiden van deze faalkanseisen, zal in dit rapport gebruik worden gemaakt van een stappenplan in de geest van de IEC-61508, waarbij voor de afgeleide SIL-niveaus ook een corresponderende faalkans zal worden vastgesteld, zodat TOPAAS desgewenst kan worden toegepast bij de vervolgstappen.

3 Aanpak

3.1 Inleiding

De aanpak voor het vaststellen van de veiligheidskritische functies en de bijbehorende eisen (vergelijkbaar met de analysefase conform IEC-61508) is op een pragmatische wijze ingevuld, vanwege het feit dat er in het verleden op basis van een ruime ervaring reeds is vastgesteld welke gevaren in een tunnel kunnen optreden, welke risico's daaraan gekoppeld zijn, welke veiligheidsmaatregelen moeten worden genomen om deze risico's te beheersen en op welke punten geautomatiseerde veiligheidssystemen nodig zijn of toegevoegde waarde hebben om aan de veiligheidsnormen te voldoen. De voor dit doel relevante kennis en ervaring is met name vastgelegd in:

- De Veiligheidsrichtlijnen deel C (VRC) [3], waarin de veiligheidsvoorzieningen zijn vastgelegd die in nieuw te bouwen Rijkstunnels moeten worden aangebracht. Bestaande tunnels moeten zoveel mogelijk aan de VRC worden aangepast, voor zover dit technisch mogelijk en zinvol (kosteneffectief) is.
- Het rekenprogramma RWSQRA [4], [5], waarmee door middel van een kwantitatieve risicoanalyse kan worden getoetst of aan de geldende veiligheidsnormen voor het persoonlijk risico en het groepsrisico wordt voldaan, met de geplande veiligheidsvoorzieningen. RWSQRA rekent op basis van een zeer uitgebreide gebeurtenissenboom, waarin de diverse ongevalsscenario's die in een tunnel kunnen optreden zijn verwerkt. Deze gebeurtenissenboom is mede gebaseerd op diverse gevarenanalyses die in het verleden zijn uitgevoerd. De recent gevalideerde versie 2.0 van RWSQRA biedt tevens de mogelijkheid om de vereiste betrouwbaarheid van de diverse veiligheidsmaatregelen af te leiden vanuit de veiligheidsnormen waaraan moet worden voldaan. Deze mogelijkheid is benut om het benodigde SIL-niveau van de geautomatiseerde veiligheidssystemen vast te stellen (zie hierna).

Concreet is de Analysefase als volgt ingevuld.

Als eerste stap is nagegaan welke geautomatiseerde veiligheidssystemen (in de zin van IEC 61508) volgens de VRC in een tunnel moeten worden aangebracht. Hierbij is als hulpmiddel gebruik gemaakt van het "Layers of Protection" model (zie paragraaf 3.2).

Daarna is ter controle een globale gevarenanalyse uitgevoerd, om na te gaan of er sprake is van nadere aandachtspunten die niet (expliciet) in de VRC of RWSQRA zijn meegenomen. Ook hierbij is gebruik gemaakt van het Layers of Protection model³.

Vervolgens is het belang van de verschillende veiligheidsmaatregelen, waaronder de geautomatiseerde veiligheidssystemen, gekwantificeerd door vaststelling van de Risk Reduction Factor (RRF) van de betreffende maatregel. De RRF is een factor die wordt gedefinieerd in de IEC-61511 [6], een aan de IEC-61508 gerelateerde norm.

³ Een globale aanvullende analyse volstond hier, omdat er zoals gezegd al uitgebreide gevarenanalyses hebben plaatsgevonden in het kader van de ontwikkeling van RWSQRA. De globale aanvullende analyse diende daarom vooral om inzicht te krijgen in hoe de verschillende veiligheidsmaatregelen in Rijkstunnels verdeeld zijn over de verschillende beschermingslagen c.q. protection layers. Dit om na te gaan in welke mate de verschillende beschermingslagen bijdragen aan het beheersen van de gevaren.

Kort gezegd drukt de RRF uit in welke mate een bepaalde maatregel bijdraagt aan de reductie van het veiligheidsrisico. Aangezien er een relatie bestaat tussen de RRF en het SIL-niveau, kan het vereiste SIL-niveau worden vastgesteld op basis van een berekening van de RRF. Voor de berekening van de RRF's van de verschillende veiligheidsmaatregelen is gebruik gemaakt van RWSQRA versie 2.0 (zie paragraaf 3.3).

Op basis van de berekening van de RRF's is bepaald of een geautomatiseerd veiligheidssysteem "veiligheidskritisch" is (SIL 1 of hoger) of dat de vereiste betrouwbaarheid laag is, zodat de in de IEC-61508 voorgeschreven beheersmaatregelen niet hoeven te worden toegepast ("SIL 0"). In het laatste geval zijn uiteraard nog wel de eisen van "good engineering practice" van toepassing.

Tenslotte zijn de nadere eisen aan de veiligheidskritische functies gedefinieerd en vastgelegd in deze rapportage (zie hoofdstuk 5).

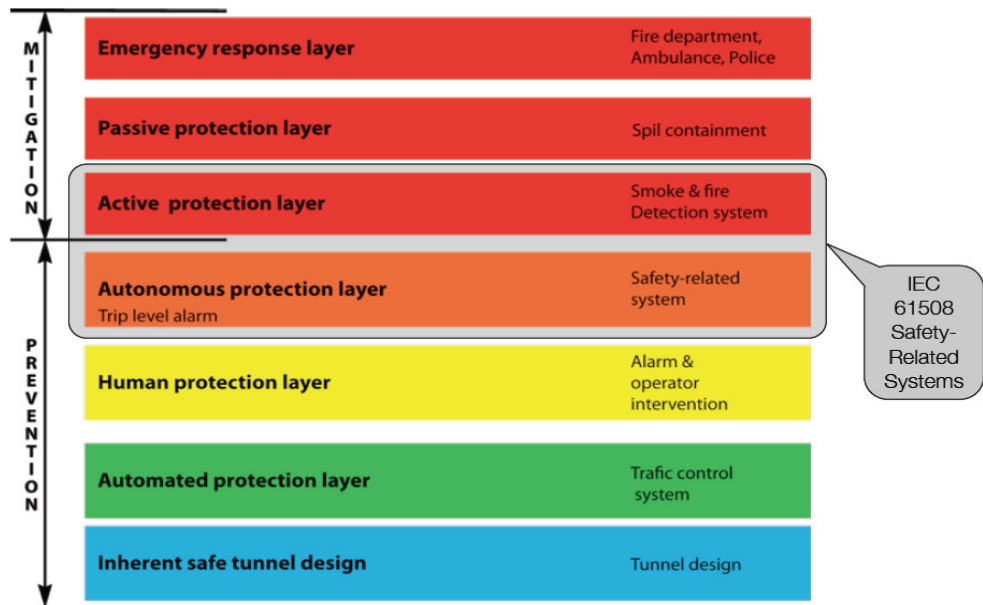
Deze aanpak is niet volledig conform het stappenplan van de IEC-61508, maar sluit daarentegen wel aan bij de wettelijk voorgeschreven QRA en de gebruikelijke veiligheidseisen voor tunnels. Dit heeft als groot voordeel dat een brug wordt geslagen tussen de wet- en regelgeving en de (internationale) normen en richtlijnen op het gebied van functionele veiligheid.

3.2 Layers of Protection

De veiligheidsmaatregelen in een tunnel (of een ander systeem) kunnen worden ingedeeld naar de "beschermingslaag" waarin ze functioneren. De beschermingslagen bieden bescherming tegen de gevolgen van een eventueel ongeval. Het zijn in feite achter elkaar geplaatste "vangnetten", waarbij iedere laag een deel van de optredende risico's beheerst c.q. reduceert. In het ideale geval zouden de beschermingslagen een volledige bescherming moeten bieden tegen alle risico's. Dit is in de praktijk uiteraard onmogelijk. De van toepassing zijnde beschermingslagen zijn, in volgorde van "ingrijpen" (zie ook figuur op volgende pagina):

1. Inherent veilig ontwerp: bijvoorbeeld veilig wegontwerp, 1 rijrichting per tunnelbuis, verbod gevaarlijke stoffen, enz.;
2. Automatische beschermingslaag: bijvoorbeeld het MTM-systeem, waarmee snelheidsverschillen worden genivelleerd, waardoor de kans op kop-staartbotsingen afneemt;
3. Menselijke beschermingslaag: dit is de wegverkeersleider, die door allerlei acties het verkeersmanagement en het incidentmanagement ondersteunt, bijvoorbeeld door het indrukken van de calamiteitenknop;
4. Autonome beschermingslaag: dit zijn de systemen die automatisch ingrijpen om een ongeval of gevaar te voorkomen; als voorbeeld zou kunnen worden gedacht aan het automatisch afkruisen van een rijstrook als een stilstaand voertuig wordt gedetecteerd;
5. Actieve beschermingslaag: dit zijn de systemen die automatisch ingrijpen om de gevolgen van een ongeval of gevaar te beperken, bijvoorbeeld het automatisch afsluiten van de tunnel, het automatisch opstarten van de ventilatie, enz.;
6. Passieve beschermingslaag: dit is bijvoorbeeld het rioleringsstelsel, waarmee gevaarlijke vloeistoffen, die bij een ongeval vrijkomen, worden afgevoerd;
7. Hulpverleningslaag: dit is de repressie door de hulpverleningsdiensten (brandweer, GHOR, politie e.d.).

Layers of protection philosophy

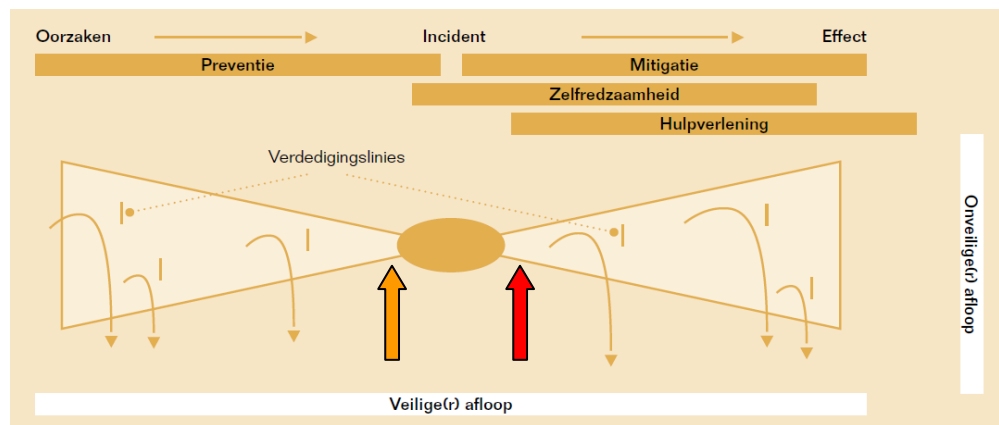


Bron: Risknowlogy

De eerste beschermingslaag (inherent veilig ontwerp) vormt dus het eerste "vangnet" tegen de gevolgen van een ongeval (bijvoorbeeld door de kans op een ongeval te verlagen). De zevende beschermingslaag (hulpverlening) is de laag die als laatste optreedt, meestal geruime tijd na het optreden van het ongeval. De effectiviteit van deze laag is dus beperkt, aangezien de eerste minuten na het ongeval cruciaal zijn bij het voorkomen van slachtoffers. Dit illustreert het belang van de effectiviteit van de onderliggende (eerdere) beschermingslagen.

Zoals uit het voorgaande blijkt, bevinden de geautomatiseerde veiligheidssystemen (functionele veiligheidssystemen) zoals bedoeld door IEC-61508 zich dus in de autonome beschermingslaag en de actieve beschermingslaag.

In termen van het vlinderdasmodel bevinden deze systemen zich dus net links van de knoop (het incident) en net rechts van de knoop, zie figuur.



Het geschetste Protection Layer model is gebruikt als hulpmiddel om vast te stellen welke veiligheidsmaatregelen uit de VRC behoren tot de geautomatiseerde veiligheidssystemen en dus een bijdrage leveren aan de functionele veiligheid.

Het model is eveneens gebruikt bij de in paragraaf 3.1 genoemde aanvullende gevarenanalyse, om na te gaan in welke mate de verschillende beschermingslagen bijdragen aan het beheersen van de gevaren.

3.3 Berekening Risk Reduction Factoren met RWSQRA versie 2.0

Het rekenprogramma RWSQRA 2.0 biedt de mogelijkheid om te selecteren welke veiligheidsmaatregelen aanwezig zijn in een tunnel, en dus om de risico's voor de weggebruikers te berekenen met of zonder een bepaalde maatregel.

De Risk Reduction Factor (RRF) van een bepaalde maatregel kan dus worden bepaald door eerst de risico's te berekenen voor de situatie dat alle veiligheidsmaatregelen in de tunnel aanwezig zijn, en vervolgens te bekijken in welke mate deze risico's toenemen indien de beschouwde maatregel niet aanwezig is.

In formule:

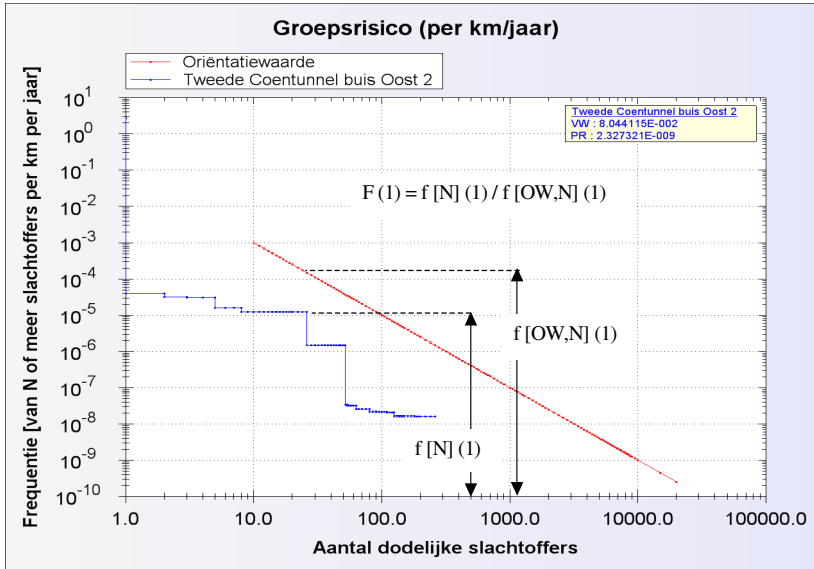
$$\text{RRF maatregel "x"} = \frac{\text{Risico zonder maatregel "x" (maar met overige maatregelen)}}{\text{Risico alle maatregelen aanwezig (incl. maatregel "x")}}$$

De RRF zou in principe kunnen worden berekend op basis van het persoonlijk risico of op basis van het groepsrisico. Het groepsrisico is hiervoor echter veel geschikter, omdat de specifieke tunnelrisico's (de extra risico's van een tunnel ten opzichte van de open weg) beter tot uitdrukking komen in het groepsrisico, terwijl de waarde van het persoonlijk risico vooral wordt gedomineerd door de "normale" verkeersongevallen, die ook op de open weg plaatsvinden. Dit betekent dat het effect van een veiligheidsmaatregel, die bedoeld is om de specifieke tunnelrisico's te beheersen, ook beter zichtbaar is in het groepsrisico dan in het persoonlijk risico. Er is derhalve gekozen voor het groepsrisico als basis voor de berekening van de RRF's.

Om de groepsrisico's met en zonder maatregel onderling te kunnen vergelijken, is er voor gekozen de verhouding van de fN-curve ten opzichte van de norm ($0,1/N^2$ per kilometer per jaar) te beschouwen. Deze methode wordt ook vaak gehanteerd in het domein van de externe veiligheid, bijvoorbeeld bij het karakteriseren of vergelijken van de groepsrisico's van transportroutes.

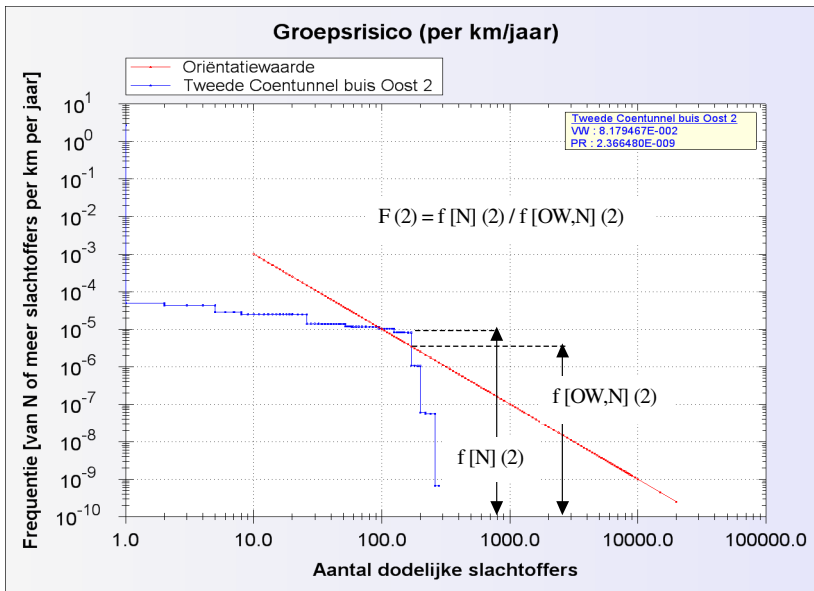
Het groepsrisico is beschouwd per tunnelbuis. Voor de verhouding tussen de fN-curve en de norm is altijd het punt van de fN-curve genomen dat de normwaarde het dichtste benadert of het meeste overstijgt. In de figuur op de volgende pagina is dit geïllustreerd, met als voorbeeld de fN-curve van de buis Oost 2 van de Tweede Coentunnel.

Grafiek alle maatregelen



RRF vluchtdeuren = $F(2) / F(1)$

Grafiek zonder vluchtdeuren



De bovenste fN-curve geldt voor de situatie dat alle veiligheidsmaatregelen aanwezig zijn, conform de VRC. De onderste fN-curve geldt voor de situatie dat de tunnelbuis geen vluchtdeuren heeft, maar dat verder alle overige veiligheidsmaatregelen wel aanwezig zijn.

Merk op dat een toename van het groepsrisico ten opzichte van de norm, zoals hierboven beschreven, in de regel niet overeenkomt met een zelfde toename van het groepsrisico over de hele lijn. De vergelijking van de maatgevende punten ten opzichte van de normlijn leidt rekenkundig eerder tot een hoge RRF dan een vergelijking van de groepsrisico's als geheel. Aangezien een hogere RRF leidt tot hogere betrouwbaarheidseisen, is de gekozen benadering derhalve conservatief.

Op basis van de aldus met RWSQRA berekende RRF's zijn vervolgens de SIL-niveaus van de veiligheidsmaatregelen vastgesteld via de volgende door de IEC-61511 gedefinieerde relatie [6]:

SIL	PFD (faalkans per aanvraag)	RRF
1	0,1 - 0,01	10 - 100
2	0,01 - 0,001	100 - 1.000
3	0,001 - 0,0001	1.000 - 10.000
4	0,0001 - 0,00001	10.000 - 100.000

4 Resultaten

4.1 Geautomatiseerde veiligheidssystemen conform de VRC

Volgens de VRC moeten de volgende geautomatiseerde veiligheidssystemen in Rijkstunnels worden aangebracht:

1. Automatische regeling verlichting ingangszone, op basis van de hoeveelheid daglicht (zie bijlage hoofdstuk 5 VRC).
2. Automatisch afsluiten tunnel bij uitval netvoeding + falen noodstroomvoorziening (zie bijlage hoofdstuk 9 VRC).
3. Automatisch afsluiten tunnel bij uitval besturing (zie bijlage hoofdstuk 9 VRC).
4. Automatisch afkruisen rijstrook + instellen snelheidsverlaging op naastliggende rijstroken op basis van (zie bijlage hoofdstuk 9 VRC):
 - Detectie gebruik noodtelefoon in hulppostkast⁴, of:
 - Detectie openen hulppostkast in combinatie met detectie gebruik noodtelefoon, of:
 - SOS-detectie in combinatie met detectie openen hulppostkast, of:
 - SOS-detectie in combinatie met detectie openen hulppostkast en detectie gebruik noodtelefoon, of:
 - SOS-detectie in combinatie met zichtmeting, of:
 - SOS-detectie in combinatie met branddetectie (temperatuurmeting).

N.B.: het automatisch afkruisen van rijstroken op basis van SOS-detectie vergt aanpassing van het gecertificeerde MTM-systeem. Deze aanpassing is momenteel nog niet gecertificeerd. Mede hierom voorziet de RWS-tunnelstandaard van de Landelijk Tunnelregisseur vooralsnog niet in deze functie. Bij de nadere eisen aan de veiligheidskritische functies (zie hoofdstuk 5) wordt derhalve geen rekening gehouden met deze voorziening.

5. Automatisch inschakelen op calamiteitenstand van de tunnelventilatie in de incidentbuis (stand-by fase na detectie) + alarmsignaal naar tunneloperator (conform hoofdstuk 14 VRC), op basis van (zie bijlage hoofdstuk 9 VRC):
 - Zichtmeting, of:
 - Branddetectie/temperatuurmeting (indien aanwezig), of:
 - Detectie openen hulppost + detectie uitnemen slanghaspel (uit dezelfde hulppost), of:
 - Detectie openen hulppost + detectie uitnemen draagbaar brandblusapparaat (uit dezelfde hulppost).

N.B.: in de RWS-tunnelstandaard wordt (in afwijking van de VRC) uitgegaan van ventilatie op 50% van de calamiteitenstand in de stand-by fase na detectie (calamiteitenstand = 100% van het vermogen) om het energieverbruik bij "valse meldingen" te beperken. De ventilatie wordt pas op volledige calamiteitenstand geschakeld bij de overgang van stand-by fase na detectie naar calamiteitenbedrijf. Bij de nadere eisen aan de veiligheidskritische functies (zie hoofdstuk 5) wordt hier derhalve ook van uit gegaan.

⁴ De rijstrook aangrenzend aan de hulppostkast wordt in dat geval afgekruid.

Omdat de calamiteitenstand is uitgelegd op het beheersen van grote branden, en deze branden enige tijd nodig hebben om zich tot hun maximale vermogen te ontwikkelen, is deze gefaseerde schakeling van de ventilatie geen bezwaar. Uitzondering wordt gevormd door de plasbranden. Deze zullen zich wel zeer snel ontwikkelen. Er mag echter worden aangenomen dat deze branden relatief snel worden opgemerkt door de operator, door het alarmsignaal dat wordt afgegeven als de incidentbuis naar stand-by fase na detectie gaat.

6. Automatisch in gereedheid brengen van de veilige vluchtweg:
 - a. Zonodig vergrendelde vluchtdeuren ontgrendelen;
 - b. Zonodig deuren in de vluchtroute die toegang geven tot ruimten anders dan de vluchtroute vergrendelen;
 - c. Mechanische overdrukventilatie in veilige ruimte (midentunnelkanaal) starten;
 - d. Vluchtwegverlichting op het juiste niveau zetten.

N.B.: volgens de RWS-tunnelstandaard worden (in aanvulling op de VRC) bij tunnels met een midentunnelkanaal (MTK) ook nog de bordjes met de dynamische aanduiding van de vluchtrichting in het MTK ingeschakeld (waarbij de juiste vluchtrichting wordt aangegeven). Bij de nadere eisen aan de veiligheidskritische functies (zie hoofdstuk 5) wordt hier derhalve ook van uit gegaan.

Het automatisch in gereedheid brengen van de veilige vluchtweg gebeurt als de incidentbuis in stand-by fase na detectie gaat, dus op basis van de volgende detecties (zie bijlage hoofdstuk 9 VRC):

- o Zichtmeting, of:
 - o Branddetectie/temperatuurmeting (indien aanwezig), of:
 - o Detectie openen hulppost + detectie uitnemen slanghaspel (uit dezelfde hulppost), of:
 - o Detectie openen hulppost + detectie uitnemen draagbaar brandblusapparaat (uit dezelfde hulppost).
7. Automatisch inschakelen van de verlichting in de incidentbuis op optimaal niveau. Dit gebeurt indien de incidentbuis in stand-by fase na detectie gaat (zie bijlage hoofdstuk 9 VRC), dus op basis van dezelfde detecties als genoemd bij 6 (automatisch in gereedheid brengen van de veilige vluchtweg). "Optimaal niveau" wil zeggen dat het 100% lichtniveau van de centrale zone over de hele lengte van het gesloten deel van de tunnel wordt ingeschakeld. Eventueel al ingeschakelde extra verlichting in de ingangzone wordt daarbij niet uitgeschakeld.
 8. Automatisch afsluiten van de tunnelbuizen die nodig zijn voor de afhandeling van een calamiteit. Dit gebeurt als de tunnel in calamiteitenbedrijf gaat, dus op basis van de volgende detecties (zie bijlage hoofdstuk 9 VRC):
 - o SOS-detectie in combinatie met zichtmeting en combinatie van 2 of meer van de volgende detecties: openen hulppost, branddetectie/temperatuurmeting (indien aanwezig), slanghaspel uitnemen (uit de geopende hulppost), draagbaar brandblusapparaat uitnemen (uit de geopende hulppost).

9. Automatisch in calamiteitenstand schakelen van de ventilatie van de tunnelbuizen naast de incidentbuis. Dit gebeurt indien de tunnel in calamiteitenbedrijf gaat (zie bijlage hoofdstuk 9 VRC), dus op basis van dezelfde detecties als genoemd bij 8 (automatisch afsluiten tunnelbuizen die nodig zijn voor afhandelen calamiteit).
10. Automatisch inschakelen van de pompen van de brandblusinstallatie en het onder druk brengen van het brandblussysteem. Dit gebeurt indien de tunnel in calamiteitenbedrijf gaat (zie bijlage hoofdstuk 9 VRC), dus op basis van dezelfde detecties als genoemd bij 8 (automatisch afsluiten tunnelbuizen die nodig zijn voor afhandelen calamiteit).
11. Automatisch stoppen van alle vuilwaterpompen en het in calamiteitenstand zetten van het inschakelregime. Dit gebeurt indien de tunnel in calamiteitenbedrijf gaat (zie bijlage hoofdstuk 9 VRC), dus op basis van dezelfde detecties als genoemd bij 8 (automatisch afsluiten tunnelbuizen die nodig zijn voor afhandelen calamiteit).
12. Automatisch activeren van de voorzieningen voor de hulpverleningsdiensten. Dit gebeurt indien de tunnel in calamiteitenbedrijf gaat (zie bijlage hoofdstuk 9 VRC), dus op basis van dezelfde detecties als genoemd bij 8 (automatisch afsluiten tunnelbuizen die nodig zijn voor afhandelen calamiteit).

N.B. (bij 5 t/m 12): de RWS-tunnelstandaard voorziet niet in een branddetectie door middel van temperatuurmeting, omdat een dergelijke voorziening te weinig toegevoegde waarde heeft ten opzichte van de overige detectiemiddelen, zoals SOS-detectie met camerabeelden en zichtmeting. Bij de nadere eisen aan de veiligheidskritische functies (zie hoofdstuk 5) wordt derhalve ook niet uitgegaan van de aanwezigheid van een temperatuurmeting.

4.2 **Aanvullingen op basis van gevarenanalyse**

De resultaten van de gevarenanalyse zijn opgenomen in bijlage A. Het blijkt dat verreweg de meeste risico's (voor zover er in een tunnel sprake is van een verhoogd risico ten opzichte van de open weg) worden beheerst door een of meer beschermingslagen van het Protection Layer model (zie paragraaf 3.2). Het zwaartepunt van de bescherming ligt in een combinatie van een inherent veilig ontwerp en beheersmaatregelen die door de operator (wegverkeersleider) worden genomen. De geautomatiseerde veiligheidssystemen ondersteunen de operator in feite bij de belangrijke functies, door acties te nemen indien de operator om wat voor reden dan ook niet reageert. Met de berekening van de RRF's (zie paragraaf 4.3) wordt het belang van de verschillende functies nader onderbouwd.

Ten aanzien van de in te VRC genoemde geautomatiseerde veiligheidssystemen is uit de gevarenanalyse nog een aandachtspunt naar voren gekomen ten aanzien van het automatisch afsluiten van de tunnel, voor de afhandeling van een calamiteit. Dit moet op een beheerste wijze gebeuren, waarbij eerst een snelheidsverlaging moet worden ingesteld met het MTM-systeem. Vervolgens moet de VRI voor de tunnelbuizen op "rood" schakelen. Pas daarna mag de afsluitboom naar beneden gaan. Uiteraard is het van belang dat de tunnelbuizen bij een (sterk vermoeden van) brand worden afgesloten, om de toestroom van verkeer de incidentbuis in te stoppen, en de naastgelegen buis vrij te maken voor de hulpverlening.

Indien dit echter onbeheerst gebeurt, kunnen er (aanvullende) ongevallen plaatsvinden, doordat voertuigen tegen de afsluitboom rijden, en/of omdat achterop komende voertuigen botsen tegen een voertuig dat wel tijdig remt. Bij het automatisch afsluiten van de tunnelbuizen hoort dus nog een tweede functie, namelijk:

- Het voorkomen dat de tunnelbuizen onbeheerst worden afgesloten bij een automatische afsluiting. De functie valt uiteen in 2 subfuncties:
 - o Het voorkomen dat de afsluitboom naar beneden gaat, zonder dat eerst een snelheidsverlaging is ingesteld met het MTM-systeem en de VRI op "rood" is gegaan;
 - o Het voorkomen van de VRI op "rood" gaat, zonder dat eerst een snelheidsverlaging is ingesteld met het MTM-systeem.

Een functie die verder aanvullend op de VRC zou kunnen worden aangebracht om kop-staart botsingen, alsmede blootstelling aan rook en gassen en dampen bij brand e.d. te voorkomen, is:

- Het voorkomen dat de staart van een file (nagenoeg stilstaand verkeer) die benedenstrooms van de tunnel ontstaat de tunnel ingroeit (filevermijding).

Het risico van blootstelling aan rook, gassen en dampen bij een file in de tunnel heeft er mee te maken dat in geval van brand de (langs)ventilatie wordt ingeschakeld, waardoor de hitte en rook richting de voertuigen benedenstrooms van de brand wordt geblazen. De omstandigheden voor de aanwezigen aldaar om de vluchtdeuren veilig te bereiken kunnen daardoor snel slechter worden, hetgeen leidt tot een toename van het risico om te overlijden.

Een filevermijdingssysteem bestaat in de meest simpele vorm uit een filedetectie benedenstrooms van de tunnelbuis, gevolgd door een ingreep van de tunneloperator (wegverkeersleider) waardoor de toestroom van verkeer de tunnelbuis in wordt vermindert, bijvoorbeeld door snelheidsverlaging, het afkruisen rijstroken of het afsluiten van de tunnelbuis. De RWS-tunnelstandaard voorziet in een dergelijk systeem, dat wil zeggen, de hiertoe benodigde voorzieningen in combinatie met de procedure om deze voorzieningen in onderlinge samenhang in te zetten:

- Filedetectie: SOS tot 600m voorbij de tunnelbuizen [7];
- Beperken toestroom verkeer: MTM, VRI en afsluitboom voor de tunnelbuizen [7];
- Procedure (procesbeschrijving) voor operator: N01 Sturen & geleiden van files bij tunnels [9].

Verder is, los van de geautomatiseerde veiligheidssystemen, nog een ander aanvullend aandachtspunt naar voren gekomen uit de gevarenanalyse:

- Het aanbrengen van een of meer veiligheidskabels aan de tunneltechnische installaties die aan het plafond van de tunnelbuis hangen, om te voorkomen dat deze op het wegdek vallen na bijvoorbeeld een aanrijding door een te hoog voertuig, of, in geval van de ventilatoren, lostrillen door dynamisch gebruik.

4.3 Risk Reduction Factoren van veiligheidsmaatregelen

De RRF van de verschillende veiligheidsmaatregelen is conform paragraaf 3.3 berekend voor een groot aantal tunnelsituaties, waarbij er is gevarieerd met de invoerparameters tunnellingte, filekans, aantal rijstroken per tunnelbuis, verkeersintensiteit en transportaantallen gevaarlijke stoffen. In bijlage B is een aantal voorbeelden opgenomen van deze berekeningen. Het blijkt dat de orde van grootte van RRF van een aantal veiligheidsmaatregelen (zoals bijvoorbeeld de tunnelventilatie) redelijk onafhankelijk is van de specifieke tunnelsituatie. Bij andere veiligheidsmaatregelen (zoals bijvoorbeeld de vluchtdeuren) is de orde van grootte van de RRF met name afhankelijk van de tunnellingte in combinatie met de kans op een file benedenstrooms van de tunnel. Andere variabelen, zoals bijvoorbeeld het aantal rijstroken per tunnelbuis, of het al dan niet toelaten van LPG-transporten, blijken veel minder van invloed te zijn op de RRF van de veiligheidsmaatregelen. Er is daarom voor gekozen om de toekomstige verkeerssituatie van de Tweede Coentunnel (buis Oost 2) als uitgangspunt te nemen voor de berekeningen, omdat deze situatie zich kenmerkt door een hoge verkeersintensiteit in combinatie met een relatief hoog aantal transporten van brandbare vloeistoffen. Vervolgens is bij deze verkeerssituatie gevarieerd met tunnellingte, aantal rijstroken per tunnelbuis en kans op een file benedenstrooms van de tunnel. Tenslotte zijn de aldus afgeleide RRF's voor de veiligheidsmaatregelen nog getoetst aan de situatie van een aantal andere maatgevende tunnels, zoals de A2 Leidsche Rijn tunnel en de Keizer Karel tunnel (A9). Daarbij is gebleken dat de uitkomsten in lijn waren met elkaar.

De berekening van het vereiste betrouwbaarheidsniveau van het "voorkomen dat de tunnelbuizen onbeheerst worden afgesloten" (zie paragraaf 4.2) is overigens niet berekend met behulp van RWSQRA, omdat een ongeval met de afsluitboom buiten de tunnel plaatsvindt, op de open weg. RWSQRA is niet geschikt om de hiermee samenhangende risico's te bepalen.

Er is bij de berekening van het vereiste betrouwbaarheidsniveau echter wel aansluiting gezocht bij de verwachtingswaarde voor het aantal doden per jaar, die met RWSQRA wordt berekend.

Er is daarbij gesteld dat het aantal doden dat per jaar mag vallen ten gevolge van het onbeheerst afsluiten van een tunnelbuis ten hoogste 1% mag bedragen van de verwachtingswaarde van het aantal doden per jaar in die tunnelbuis. Zie bijlage B voor de verdere berekening.

Uit de berekeningen volgt, dat de volgende geautomatiseerde veiligheidsfuncties in algemene zin "veiligheidskritisch" zijn in tunnels, omdat ze (met een RRF van 5 of hoger) in aanmerking komen voor een SIL-niveau 1 of hoger⁵:

1. Automatisch inschakelen van de tunnelventilatie in de incidentbuis op 50% van het maximale vermogen;
2. Automatisch in gereedheid brengen van de veilige vluchtweg;
3. Voorkomen dat automatische afsluiting van de tunnelbuizen onbeheerst gebeurt.

Bij tunnels van categorie A blijkt aanvullend ook "veiligheidskritisch":

4. Aanwezigheid van een (bekwame) tunneloperator.

⁵ Een RRF van 5 of hoger is hierbij conservatief naar boven afgerond, c.q. afgerond naar 10

De tunneloperator is bij deze tunnels veiligheidskritisch, omdat bij het scenario "warme BLEVE" het geven van een tijdige vluchtinstructie belangrijk is om het aantal slachtoffers te beperken. Bij dit scenario is het middentunnelkanaal immers geen veilige ruimte, alle mensen die zich nog in de tunnel bevinden zullen bij de explosie overlijden. Het geven van vluchtinstructies is niet geautomatiseerd, dus de tunneloperator is op dit punt de enige "protection layer". Het geven van een vluchtinstructie is bij dit scenario extra van belang voor de aanwezigen bovenstrooms van de brand (die de oorzaak vormt van een warme BLEVE) omdat deze vanwege de ingeschakelde tunnelventilatie niet worden geprikkeld om te vluchten. Bij een "normale" brand (zonder explosiegevaar) is dit niet direct een risico, omdat men in principe veilig is, maar als de tunnel moet worden ontruimd voordat de BLEVE plaatsvindt, ligt dit kritischer.

De tunneloperator is uiteraard geen geautomatiseerd systeem, dus er is geen sprake van een vereist SIL-niveau zoals bij technische voorzieningen. Echter, de operator dient wel voldoende te zijn opgeleid, getraind en geoefend om de vereiste betrouwbaarheid en effectiviteit van de vluchtinstructies te garanderen. Conform de VRC dient bij voorkeur gebruik te worden gemaakt van vooraf ingesproken standaardomroepberichten, die door de operator worden geactiveerd via het groepscommando "evacuatie".

Bij lange tunnels, met een hoge kans op files, kan aanvullend de volgende functie "veiligheidskritisch" zijn:

5. Het voorkomen dat de staart van een file (nagenoeg stilstaand verkeer) die benedenstrooms van de tunnel ontstaat de tunnel ingroeit (filevermijding, zie ook paragraaf 4.2).

Verder blijkt uit de berekeningen, dat de overige veiligheidsmaatregelen veelal een RRF van net iets meer dan 1 hebben. Dit betekent dat deze maatregelen ieder afzonderlijk weinig effect hebben op het (verlagen van het) groepsrisico. Dit komt omdat veel veiligheidsmaatregelen in de tunnel in feite "functioneel redundant" zijn. Voorbeeld: het niet ingrijpen door de operator kan worden opgevangen door het automatisch inschakelen van de ventilatie op basis van zichtmeting. Een RRF van iets meer dan 1 betekent echter niet dat de betreffende maatregel overbodig is. Het is wel een bevestiging dat redundantie een gunstige invloed heeft op de betrouwbaarheidseisen van de afzonderlijke maatregelen.

Binnen de groep van "niet-veiligheidskritische" functies is er een aantal veiligheidsmaatregelen die (onder sommige omstandigheden) een RRF hebben die groter is dan 1 maar kleiner dan 5. Dit zijn:

- Automatische regeling verlichting ingangszone, op basis van de hoeveelheid daglicht;
- Riolering.

Indien de regeling van de ingangsverlichting faalt, heeft dit een verhogend effect op de ongevalkans in de ingangszone van de tunnel ("zwart gat effect"). De effecten van een ongeval in de ingangszone kunnen zich vervolgens manifesteren in de hele tunnel, in geval van brand en het vrijkomen van gevaarlijke stoffen. Van een verhoogde kans op een ongeval is echter alleen overdag sprake, op heldere zonnige dagen. Bovendien is er bij een ongeval in de ingangszone met name sprake van risico's voor de weggebruikers in de tunnel indien er sprake is van een

benedenstroomse file. Door deze 2 factoren wordt het effect van de regeling van de ingangsverlichting op het groepsrisico zodanig beperkt, dat de RRF onder de "veiligheidskritische" drempel blijft. Echter, omdat bij falen de ongevalskans in bepaalde situaties significant kan worden verhoogd, vereist de functie wel nadere aandacht. Zo moet het falen van de functie (zie VRC voor faaldefinities) automatisch aan de operator worden gemeld, zodat deze zonodig kan ingrijpen (snelheidsverlaging instellen, handmatig bijregelen, enz.).

De riolering speelt een belangrijke rol bij het afvoeren van brandbare of toxische vloeistoffen, die bij een ongeval vrij kunnen komen. Als zodanig heeft de riolering een relatief groot veiligheidseffect in tunnels met veel bulktransporten van bijvoorbeeld benzine. Het is in feite de enige "protection layer" die kan voorkomen dat er een grote plas van een brandbare of toxische vloeistof op het wegdek ontstaat bij een ongeval waarbij gevaarlijke stoffen vrijkomen. Aangezien riolering geen geautomatiseerd systeem is, heeft het relatief grote veiligheidseffect geen consequenties voor de eisen aan bijvoorbeeld detectie of besturing. Het betekent wel dat het beheer en onderhoud van de riolering nadere aandacht vraagt.

5 Specificatie veiligheidskritische functies

5.1 Inleiding

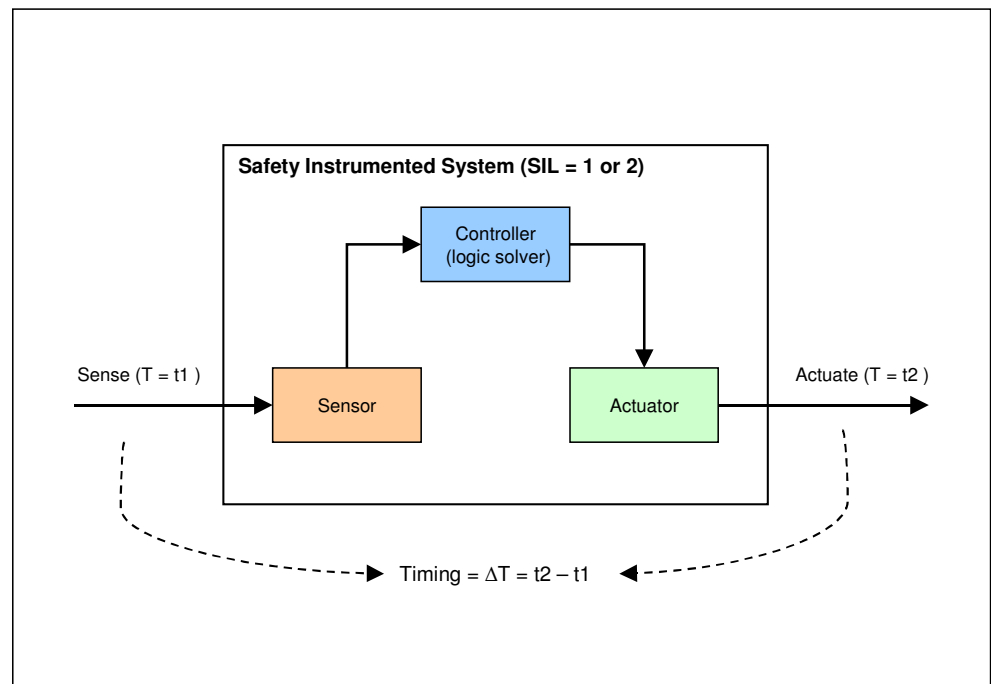
Zoals vermeld in paragraaf 4.3 zijn de volgende geautomatiseerde veiligheidsfuncties in algemene zin "veiligheidskritisch" in tunnels:

1. Automatisch inschakelen op calamiteitenstand van de tunnelventilatie in de incidentbuis;
2. Automatisch in gereedheid brengen van de veilige vluchtweg;
3. Voorkomen dat automatische afsluiting van de tunnelbuizen onbeheerst gebeurt.

Bij lange tunnels, met een hoge kans op files, kan aanvullend de volgende functie veiligheidskritisch zijn:

4. Het voorkomen dat de staart van een file (nagenoeg stilstaand verkeer) die benedenstrooms van de tunnel ontstaat de tunnel ingroeit (filevermijding).

In de navolgende paragrafen worden de veiligheidskritische functies nader gespecificeerd op basis van het SLATS-model (zie figuur):



- Sense: wat wordt gemeten?
- Logic: bij welke meetwaarden moet worden ingegrepen?
- Actuate: welke acties worden genomen bij ingreep?
- Time: hoe snel moeten de acties worden genomen na detectie?
- Safety integrity: welk SIL-niveau moet de functie hebben (bij toepassing IEC-61508)?
- Faalkans: welke faalkans is toegestaan (bij toepassing TOPAAS)?

Het SIL-niveau en de toegestane faalkans worden beiden gespecificeerd, omdat zowel de IEC-61508 als TOPAAS kunnen worden toegepast om te borgen dat het ontwerp van de veiligheidskritische functies aan de eisen voldoet (zie paragraaf 1.1 en paragraaf 6.2).

Er is sprake van falen van de veiligheidskritische functie als:

- Het systeem niet reageert (voorbeeld: ventilatie gaat bij aanspraak niet aan);
- Het systeem de verkeerde dingen doet (voorbeeld: ventilatie blaast tegen de rijrichting in, in plaats van met de rijrichting mee);
- Het systeem te laat reageert (voorbeeld: ventilatiecapaciteit is te laat op vol vermogen).

De toegestane faalkans per aanvraag geeft derhalve het totale faalbudget weer voor al deze faalwijzen.

Vanwege de samenhang met de geautomatiseerde veiligheidsfuncties wordt in paragraaf 5.6 tevens ingegaan op de vereiste betrouwbaarheid van de calamiteitenknop.

Voor de volledige specificaties van installaties die zorg dragen voor de vervulling van de veiligheidskritische functies wordt verwezen naar de Basisspecificatie TTI van de RWS-tunnelstandaard [7].

5.2 Tunnelventilatie

Sense	- Zichtmeting ($k > 0,012/m$), of:
Logic	- Detectie openen hulppost + detectie uitnemen slanghaspel, of: - Detectie openen hulppost + detectie uitnemen draagbaar brandblusapparaat.
Actuate	- Inschakelen op 50% van de calamiteitenstand van de tunnelventilatie in de incidentbuis, en: - Alarmsignaal naar de operator.
Time	Maximaal 60 seconden (vanaf detectie tot ventilatie op 50% totale vermogen)
SIL	1
Faalkans	< 0,02 per aanvraag

Opmerkingen:

- De vereiste reactietijd van het systeem (Time) kan als volgt worden onderbouwd, uitgaande van de detectie met de zichtmeter:
 - Reactietijd zichtmeter bij optreden $k > 0,012/m$: 2 tot 5 seconden;
 - Reactietijd besturing (PLC's): 5 tot 10 seconden;
 - Benodigde tijd voor ventilatie om na inschakelen op 50% van het totale vermogen te komen: 45 seconden.

Uiteraard is er ook nog sprake van de benodigde tijd voor de rook om vanaf de locatie van de brand de zichtmeter te bereiken. Deze tijd is buiten de vereiste reactietijd van de veiligheidskritische functie gehouden, maar wordt beperkt doordat de RWS-tunnelstandaard vereist dat de zichtmeters met een onderlinge afstand van maximaal 250m in de tunnelbuis worden aangebracht.

Uitgaande van een conservatieve situatie met fileverkeer en een luchtsnelheid van 2m/s in de tunnelbuis, zou dit betekenen dat het maximaal 125 seconden duurt eer de rook de zichtmeter bereikt. Bij normaal rijdend verkeer (snelheid 100-120 km/u) treedt een luchtstroming van 4-6 m/s op en zal de rook veel sneller worden gedetecteerd, namelijk binnen 42-63 seconden.

Voor wat betreft de besturing: een reactietijd van 5 tot 10 seconden is technisch ruim haalbaar. Sneller zou dus kunnen. Er is echter gekozen voor deze timing, zodat het systeem de "duurzaamheid" van de detecties nog kan verifiëren, om de kans op valse meldingen te verkleinen.

Het opstarten van de ventilatie tot 50% van het totale vermogen kost enige tijd, omdat dit veel energie vergt en er dus trapsgewijs groepen moeten worden bijgeschakeld om overbelasting van de energievoorziening te voorkomen. Het kost daarom ongeveer 90 seconden om na inschakelen op vol vermogen te komen. Het zal dus ongeveer 45 seconden kosten om 50% van het vermogen te bereiken.

- Bij een detectie door het openen van een hulppost in combinatie met het uitnemen van een slanghaspel of een draagbaar brandblusapparaat moeten deze signaleringen plaatsvinden binnen een bepaalde tijdspanne om als combinatie te worden gedetecteerd. Te denken valt aan een tijdspanne van 10 tot 15 seconden (in de RWS-tunnelstandaard is deze tijdspanne parametreerbaar).
- De RRF van de ventilatie is redelijk onafhankelijk van lengte van de tunnel en de kans op een benedenstroomse file, en heeft veelal een waarde tussen 5 en 8. Er is echter conservatief uitgegaan van een RRF van 10, op basis waarvan is gekozen voor SIL 1. Bij een verhoogde kans op een benedenstroomse file (nagenoeg stilstaand verkeer) neemt het veiligheidseffect van de ventilatie in feite af. Dit is logisch, omdat in een situatie met bijvoorbeeld brand in combinatie met een file alle weggebruikers benedenstrooms van de brand door de langventilatie in de rook worden gezet, zodat de kans op slachtoffers toeneemt. Dit leidt in de praktijk echter niet tot lagere betrouwbaarheidseisen voor de ventilatie, omdat een probleem met verhoogde filekansen in principe zou moeten worden opgelost met aanvullende maatregelen.
- De gekozen faalkans ($< 0,02$ per aanvraag) komt overeen met de faalkanseis met betrekking tot technisch falen van de ventilatie conform de VRC. Er is hier voor gekozen deze eis betrekking te laten hebben op de hele keten sensor --> controller --> actuator (zie paragraaf 5.1). De eis sluit aan bij het betrouwbaarheidsniveau dat bij SIL 1 zou moeten worden bereikt (faalkans per aanvraag 0,1 – 0,01, zie paragraaf 3.3) en is bovendien technisch haalbaar.
- In lijn met de vorige opmerking heeft de vermelde faalkans ($< 0,02$ per aanvraag) alleen betrekking op het technisch falen van de veiligheidskritische functie. De kans op systeemfalen (het optreden van backlayering van de rook, ondanks dat de ventilatie en de overige techniek correct werkt, zie hoofdstuk 12 van de VRC) moet dus niet worden meegenomen in de foutenboomanalyse met betrekking tot het technisch falen van de veiligheidskritische functie, maar separaat worden getoetst, bijvoorbeeld met het softwarepakket ProTuVem 2.0, op basis van de eisen in de VRC (c.q. de RWS-tunnelstandaard).

- Ook ten behoeve van de beheersing van de luchtkwaliteit in de tunnelbuis wordt de tunnelventilatie automatisch ingeschakeld (en uitgeschakeld) op basis van zichtmeting (zie hoofdstuk 14 van de VRC). Deze functie maakt echter geen deel uit van de hier beschreven veiligheidskritische functie.
- Er is een relatie tussen de tunnelventilatie en het in gereedheid brengen van de veilige vluchtweg, zie paragraaf 5.3. De ventilatie moet dus in samenhang met de vluchtdeuren en de overdrukventilatie in de veilige ruimte worden beschouwd.
- Voor de eisen met betrekking tot het veilig faalgedrag van de zichtmeting en de ventilatie (bij uitval van de energievoorziening of de besturing) wordt verwezen naar de Basisspecificatie TTI van de RWS-tunnelstandaard [7].
- Voor de te nemen maatregelen bij het falen van de zichtmeting, de ventilatie, de besturing of de energievoorziening wordt verwezen naar de faaldefinities van de TTI, opgenomen in het Systemontwerp van de RWS-tunnelstandaard [8].

5.3 Veilige vluchtweg

Sense	<ul style="list-style-type: none"> - Zichtmeting ($k > 0,012/m$) of: - Detectie openen hulppost + detectie uitnemen slanghaspel, of: - Detectie openen hulppost + detectie uitnemen draagbaar brandblusapparaat.
Logic	
Actuate	<ul style="list-style-type: none"> a. Zonodig vergrendelde vluchtdeuren ontgrendelen; b. Zonodig deuren in de vluchtroute die toegang geven tot ruimten anders dan de vluchtroute vergrendelen; c. Mechanische overdrukventilatie in veilige ruimte (midentunnelkanaal) starten; d. Vluchtwegverlichting op het juiste niveau zetten; e. Bordjes met dynamische vluchtrouteaanduiding in MTK inschakelen (waarbij de juiste vluchtrichting wordt aangegeven).
Time	75 seconden
SIL	a t/m c: zie tabel op volgende pagina d en e: n.v.t. ("SIL 0")
Faalkans	a t/m c: zie tabel op volgende pagina d en e: overeenkomstig faalkans gebruikelijke COTS-componenten (Commercial Off The Shelf)

SIL-niveau (en tussen haakjes de faalkans per aanvraag) m.b.t. ont-/vergrendelen (vlucht)deuren en starten overdrukventilatie				
Filekans Tunnellengte	Hoog (5x / week)	Normaal (1x / week)	Laag (1x / 2 weken)	Systeem filevermijding
< 500m	1 (< 0,01)	1 (< 0,01)	1 (< 0,01)	1 (< 0,01)
500m -1.000m	2 (< 0,01)	1 (< 0,01)	1 (< 0,01)	1 (< 0,01)
1.000m - 1.250m	2 (< 0,01)	2 (< 0,01)	1 (< 0,01)	1 (< 0,01)
1.250m - 2.500m	2 (< 0,01)	2 (< 0,01)	2 (< 0,01)	1 (< 0,01)
2.500m - 5.000m	2 (< 0,005)	2 (< 0,005)	2 (< 0,01)	2 (< 0,01)
> 5.000m	2 (< 0,005)	2 (< 0,005)	2 (< 0,005)	2 (< 0,01)

Legenda

	RRF < 100
	100 < RRF < 500
	RRF > 500

Opmerkingen:

- De vereiste reactietijd van het systeem (Time) kan als volgt worden onderbouwd, uitgaande van de detectie met de zichtmeter (zie ook opmerkingen bij tunnelventilatie, paragraaf 5.2):
 - Reactietijd zichtmeter bij optreden $k > 0,012/m$: 2 tot 5 seconden;
 - Reactietijd besturing (PLC's): 5 tot 10 seconden;
 - Benodigde tijd voor overdrukventilatie om na inschakelen vereiste overdruk in MTK te realiseren: 60 seconden.
- Bij een detectie door het openen van een hulppost in combinatie met het uitnemen van een slanghaspel of een draagbaar brandblusapparaat moeten deze signaleringen plaatsvinden binnen een bepaalde tijdspanne om als combinatie te worden gedetecteerd. Te denken valt aan een tijdspanne van 10 tot 15 seconden (in de RWS-tunnelstandaard is deze tijdspanne parametreerbaar).
- Het SIL-niveau van het ontgrendelen/vergrendelen van (vlucht)deuren en het inschakelen van de overdrukventilatie wordt vooral bepaald door de lengte van de tunnel, in combinatie met de kans op een benedenstroomse file. Dit komt omdat het belang van het correct functioneren van de vluchtvoorzieningen uiteraard toeneemt naarmate het risico dat zich veel mensen benedenstrooms van de brand bevinden toeneemt.
- De SIL-niveaus en de faalkansen in de tabel zijn gebaseerd op de RRF van de vluchtdeuren, die voor een groot aantal verschillende situaties zijn berekend met RWSQRA.
- De toegestane faalkans bij SIL 1 ($< 0,01$ per aanvraag) is strenger gekozen dan bij de ventilatie (zie paragraaf 5.2) omdat de RRF van de vluchtdeuren hoger is dan die van de ventilatie. Bij SIL 2 is eveneens gekozen voor een toegestane faalkans $< 0,01$ per aanvraag, indien de RRF < 500 . Bij een RRF > 500 is de toegestane faalkans gesteld op $< 0,005$ per aanvraag. Met deze keuzes wordt een balans beoogd tussen gewenste betrouwbaarheid en technische haalbaarheid.
- Het berekende SIL-niveau is noodzakelijk voor de ontgrendeling van de vluchtdeuren, omdat dat de meest essentiële schakel in de toegang naar een veilige ruimte is. Het op het juiste niveau zetten van de vluchtwegverlichting is veel minder kritisch dan het ontgrendelen van de deuren of het starten van de overdrukventilatie, en kan dus als "SIL 0" worden geclassificeerd. Niet meteen duidelijk is echter of het berekende SIL-niveau ook adequaat is voor de overdrukventilatie. Hiervoor is derhalve een aanvullende risicobeschuwing uitgevoerd (zie tabel hierna).

Uiteindelijk is er voor gekozen het berekende SIL-niveau ook van toepassing te verklaren op het starten van de overdrukventilatie, omdat de vluchtgang zonder overdruk geen veilige ruimte is, c.q. de vluchtende mensen niet veilig zijn als er rook in de vluchtgang komt. De kans dat er rook in de vluchtgang komt neemt bovendien toe met de lengte van de tunnel.

Gevolgen indien overdrukventilatie in MTK faalt		
Scenario	Gevolg	Risico
Alleen vluchtdeuren geopend bovenstrooms van de brand	Vluchtgang MTK blijft rookvrij	[-]
Een of meer vluchtdeuren geopend bovenstrooms van de brand, in combinatie een vluchtdeur benedenstrooms van de brand	Afhankelijk van de drukverschillen bovenstrooms en benedenstrooms. De kans dat de druk bovenstrooms hoger is dan benedenstrooms is vrij groot, vanwege de druk van de brand, tegen de ventilatierichting in. In dat geval blijft de vluchtgang rookvrij. Alleen als de benedenstroomse vluchtdeur zich in de buurt van een aanjaagventilator bevindt, kan de druk benedenstrooms hoger zijn dan bovenstrooms, waardoor er rook in de vluchtgang kan stromen.	Laag. Risico wordt hoger naarmate zich meer aanjaagventilatoren in de tunnel bevinden, dus bij lange tunnels.
Een of meer vluchtdeuren geopend benedenstrooms van de brand	Rook kan in de vluchtgang stromen, door drukverschil.	Laag bij "korte" tunnels, bijvoorbeeld onderwatertunnels; Hoog bij "lange" tunnels, bijvoorbeeld landtunnels.
Meerdere vluchtdeuren geopend, zowel bovenstrooms als benedenstrooms van de brand	Afhankelijk van drukverschillen kan rook in de vluchtgang stromen.	Laag bij "korte" tunnels, bijvoorbeeld onderwatertunnels; Hoog bij "lange" tunnels, bijvoorbeeld landtunnels.
Hulpverleningsdiensten openen een vluchtdeur vanuit de nevenbuis	Hulpdiensten arriveren veelal 12-15 minuten na de melding van de calamiteit bij de tunnel. De kans dat er dan nog mensen vanuit de incidentbuis moeten vluchten naar het MTK (en een vluchtdeur openen benedenstrooms van de brand) is laag. Aangezien de vluchtdeuren zelfsluitend zijn is de kans dat er rook in de vluchtgang komt via een vluchtdeur die nog open staat is derhalve laag	Laag.

- De benodigde kracht om een vluchtdeur te openen mag maximaal 100N bedragen, conform de VRC. Deze kracht is door 99% van de Nederlandse weggebruikers met weinig moeite op te brengen. Het blijkt dat de vluchtdeuren in veel tunnels in de praktijk niet aan deze eis voldoen, omdat bij een ingeschakelde tunnelventilatie en overdrukventilatie het drukverschil tussen de incidentbuis en het MTK zodanig groot wordt dat de vluchtdeuren in hun sponning worden gedrukt en daarom moeilijk zijn te openen. Dit ondanks het feit dat het schuifdeuren betreft. Als de benodigde openingskracht oploopt tot 400N, dan is de deur voor veel mensen met enige moeite nog net te openen. Als de benodigde kracht hoger wordt dan 400N, dan moet de deur in de praktijk als "vergrendeld" worden beschouwd, ook als er geen sprake is van een "echte" deurvergrendeling. De vluchtdeuren, tunnelventilatie en overdrukventilatie moeten daarom in onderlinge samenhang worden ontworpen, gerealiseerd en onderhouden, om aan de vereiste maximale openingskracht van 100N te voldoen. Dit houdt onder meer in, dat de overdrukventilatie automatisch moet worden geregeld op basis van het drukverschil tussen het MTK en de incidentbuis. Idealiter is dit drukverschil ongeveer 50 Pa, maar in de praktijk zijn in tunnels drukverschillen tot 800 Pa gemeten (in een situatie waarbij de tunnelventilatie niet is ingeschakeld of faalt, en de overdrukventilatie wel is ingeschakeld). De betrouwbaarheid van de tunnelventilatie en het in gereedheid brengen van de veilige vluchtweg hebben dus invloed op elkaar. Dit ontwerp-probleem overstijgt de scope van de IEC-61508, en kan dus niet geheel worden beheerst door geautomatiseerde veiligheidssystemen. Er moeten buiten de maatregelen volgens IEC-61508 dus nog meer ontwerp- en beheersmaatregelen worden genomen om aan de eis voor de openingskracht te voldoen.
- Voor de eisen met betrekking tot het veilig faalgedrag van de zichtmeting, de vluchtdeurvergrendeling, de overdrukventilatie e.d. (bij uitval van de energievoorziening of de besturing) wordt verwezen naar de Basisspecificatie TTI van de RWS-tunnelstandaard [7].
- Voor de te nemen maatregelen bij het falen van de zichtmeting, de vluchtdeurvergrendeling, de overdrukventilatie, de besturing of de energievoorziening e.d. wordt verwezen naar de faaldefinities van de TTI, opgenomen in het Systeemontwerp van de RWS-tunnelstandaard [8].

5.4 Voorkomen onbeheerst afsluiten tunnelbuis

Sense	<ul style="list-style-type: none"> - Afsluitboom: bij commando "neer" nagaan: <ul style="list-style-type: none"> o Status VRI ("rood" of "uit") - VRI: bij commando "rood" nagaan: <ul style="list-style-type: none"> o Status MTM (snelheidsverlaging "70" / "50" ingesteld of niet).
Logic	
Actuate	<ul style="list-style-type: none"> - Afsluitboom: <ul style="list-style-type: none"> o Indien VRI niet "rood", dan commando "rood" naar VRI; o Indien VRI na commando nog steeds niet "rood", dan afsluitboom <u>niet</u> neer. o Indien VRI na commando wel "rood", dan afsluitboom neer. - VRI: <ul style="list-style-type: none"> o Indien MTM geen snelheidsverlaging, dan commando snelheidsverlaging naar MTM; o Indien MTM na commando nog steeds geen snelheidsverlaging, dan VRI niet op "rood"; o Indien MTM na commando wel snelheidsverlaging, dan VRI op "rood"
Time	5 seconden (beslistijd afsluitboom wel/niet neer)
SIL	Afsluitboom: 2 VRI: 1
Faalkans	Afsluitboom: < 0,00385 per aanvraag VRI: < 0,0154 per aanvraag

Opmerkingen

- De veiligheidskritische functie heeft betrekking op de bewaken van het onbeheerst automatisch afsluiten van de tunnel. De "omgekeerde" functie, het zorgen dat de tunnel automatisch wordt afgesloten bij vermoeden van brand, blijkt volgens de berekening van de RRF niet veiligheidskritisch te zijn. Dit komt door de werking van de tunnelventilatie, die er voor zorgt dat de tunnelbuis bovenstrooms van de brand rookvrij blijft. Hierdoor lopen de mensen die toch de tunnel inrijden geen direct gevaar. Pas als de ventilatie ook zou falen, dan levert het niet afsluiten van de tunnelbuis gevaarlijke situaties op.
- De SIL-niveaus zijn in dit geval niet afgeleid op basis van de RRF's, omdat dit niet mogelijk is met RWSQRA. Een ongeval als gevolg van het onbeheerst sluiten van de afsluitboom vindt immers buiten de tunnel plaats, terwijl RWSQRA alleen de risico's als gevolg van een ongeval in de tunnel kan berekenen. Er is derhalve gebruik gemaakt van een alternatieve rekenmethode, namelijk door uit te gaan van een maximaal aantal doden dat door het onbeheerst afsluiten van de tunnelbuis mag vallen. Dit aantal is conservatief gesteld op 1% van de (met RWSQRA te bepalen) verwachtingswaarde voor het aantal doden per jaar in de tunnelbuis. Hieruit zijn de faalkansen per aanvraag afgeleid en vervolgens zijn de corresponderende SIL-niveaus bepaald. Zie bijlage B voor de uitwerking van deze berekening.
- Voor de eisen met betrekking tot het veilig faalgedrag van de afsluitboom, VRI en MTM (bij uitval van de energievoorziening of de besturing) wordt verwezen naar de Basisspecificatie TTI van de RWS-tunnelstandaard [7].

- Voor de te nemen maatregelen bij het falen van de afsluitboom, VRI, MTM, de besturing of de energievoorziening wordt verwezen naar de faaldefinities van de TTI, opgenomen in het Systeemontwerp van de RWS-tunnelstandaard [8].

5.5 Filevermijding

In de meest simpele vorm bestaat een filevermijdingssysteem uit een procedurele maatregel (zie paragraaf 4.2). In verreweg de meeste gevallen zal dit volstaan om aan de wettelijke veiligheidseisen en om aan de betrouwbaarheidseisen voor de veilige vluchtweg te voldoen (zie paragraaf 5.3). Indien dit niet het geval blijkt te zijn, dan kan een geautomatiseerd systeem worden overwogen. De RWS-tunnelstandaard voorziet hier echter niet in, wat betekent dat dit aanpassingen zou vergen aan het standaard-besturingssysteem. Indien er ondanks dit nadeel moet worden gekozen voor een geautomatiseerd systeem, dan gelden de navolgende eisen.

Sense	- SOS-detectie ($v < 25$ km/u) op het weggedeelte benedenstrooms van de tunnelbuis
Logic	
Actuate	- Verminderen toestroom van verkeer de tunnel in, door middel van bijvoorbeeld: <ul style="list-style-type: none"> o Snelheidsverlaging (MTM) op de toeleidende weg naar de tunnelbuis, of: o Afkruisen rijstroken (MTM) op de toeleidende weg naar de tunnelbuis, of: o Doseren verkeer dat de tunnel inrijdt, met een tunneldoseerinstallatie (variant op toeritdosering), of: - Stimuleren doorstroming benedenstrooms van de tunnel, door middel van bijvoorbeeld openstellen spitsstrook o.i.d.
Time	Nader te bepalen per tunnel. Is afhankelijk van de beschikbare tijdsduur tussen het moment van de eerst mogelijke detectie en het moment dat de staart van de file de tunnelbuis bereikt. Deze tijdsduur is op zijn beurt afhankelijk van de verkeersintensiteit en de lengte waarover detectielussen zijn aangebracht voorbij de uitgang van de tunnelbuis. Aanbevolen wordt de vereiste reactietijd (timing) veiligheidshalve te stellen op 50% van de betreffende tijdsduur.
SIL	Zie tabel op volgende pagina. Deze waarden gelden voor de situatie dat het filevermijdingssysteem als enige aanvullende maatregel wordt toegepast (bovenop de standaardvoorzieningen). Bij meerdere aanvullende maatregelen wordt het systeem waarschijnlijk minder kritisch en gelden er wellicht lagere waarden.
Faalkans	Nader te bepalen per tunnel (zie bij opmerkingen voor toelichting).

SIL-niveau filevermijding			
Filekans Tunnellengte	Hoog (5x / week)	Normaal (1x / week)	Laag (1x / 2 weken)
< 500m	0	0	0
500m - 1.000m	0	0	0
1.000m - 2.000m	0	0	0
2.000m - 3.000m	1	0	0
3.000m - 5.000m	1	1	1
5.000m - 7.000m	2	1	1
7.000m - 10.000m	2	2	1
> 10.000m	2	2	2

Opmerkingen

- De aangegeven SIL-waardes zijn (uiteraard) niet van toepassing als er sprake is van een niet-geautomatiseerd systeem, maar van een procedurele maatregel. De SIL-waardes geven echter wel een indicatie van de vereiste betrouwbaarheid. Dit betekent dat het bij een SIL-waarde van 2 voor de hand ligt om te kiezen voor een geautomatiseerd systeem. Bij SIL 0 ligt het voor de hand te kiezen voor de bediening door de tunneloperator. Bij SIL 1 zou een nadere afweging kunnen plaatsvinden tussen bediening of automatische ingreep.
- Er dient te worden opgemerkt dat de uiteindelijke effectiviteit van het systeem niet alleen afhangt van de techniek, maar ook van het effect op het verkeer. Dit effect is niet geheel voorspelbaar, omdat dit in sterke mate afhangt van de plaatselijke situatie in combinatie met het menselijk gedrag in het verkeer. Het is derhalve denkbaar dat het gespecificeerde betrouwbaarheidsniveau in de praktijk niet kan worden bereikt. Per tunnel zal nader moeten worden ingeschat wat haalbaar is.
- Een tunnel > 2.500m, een verkeersaanbod conform de Coentunnel en een hoge kans op file (> 1x per etmaal) voldoet niet meer aan de norm voor het groepsrisico zonder een systeem om stilstaand verkeer in de tunnel te voorkomen, of een andere aanvullende maatregel om het groepsrisico te verlagen. Bij een lagere kans op file geldt een hogere tunnellengte waarboven aanvullende maatregelen moeten worden toegepast om aan de norm voor het groepsrisico te voldoen.

5.6 Calamiteitenknop

Naast de in de voorgaande hoofdstukken en paragrafen gespecificeerde geautomatiseerde systemen beschikt de tunneloperator (wegverkeersleider) conform de VRC in de bedieningcentrale op zijn desk over gemakkelijk bedienbare fysieke calamiteitenknoppen (ten minste 1 per rijrichting), die hij kan indrukken in geval van een calamiteit. Door het indrukken van deze knop (= menselijke beschermingslaag) worden de tunnelinstallaties van de geselecteerde tunnelbuis (en de ondersteunende nevenbuis) via één handeling in calamiteitenbedrijf geschakeld (zie hoofdstuk 9 VRC):

- Vluchtweg in gereedheid brengen;
- Verlichting in incidentbuis op optimaal niveau schakelen;
- Tunnelventilatie in incidentbuis in calamiteitenstand schakelen;
- De voor de afhandeling van de calamiteit benodigde tunnelbuizen afsluiten voor verkeer;
- Tunnelventilatie naastgelegen tunnelbuizen in calamiteitenstand schakelen;
- Pompen van de brandblusinstallatie inschakelen en het brandblussysteem onder druk brengen (indien van toepassing);
- Alle vuilwaterpompen stoppen en het inschakelregime in calamiteitenstand zetten;
- Voorzieningen hulpdiensten activeren.

Tussen het moment van indrukken en het schakelen naar Calamiteitenbedrijf dient een instelbare tijdvertraging van enige seconden aanwezig te zijn. De tunneloperator heeft daarmee de tijd om te controleren of de juiste tunnelbuis is geselecteerd en om een eventuele vergissing direct te herstellen. Als de tunneloperator niet reageert, start het calamiteitenbedrijf voor de geselecteerde tunnelbuis na enkele seconden automatisch. De reactietijd van de calamiteitenknop wordt overigens niet alleen bepaald door de instelbare bedenkt- of hersteltijd, maar ook door de tijd die het commando nodig heeft om van de verkeerscentrale via het VIC-net de tunnel te bereiken. Deze tijd bedraagt (rekening houdend met zeer ongunstige situaties waarbij een deel van het VIC-net in storing ligt en het signaal via een andere weg in de ring zijn weg moet zoeken) niet meer dan 2 seconden⁶.

Naast de fysieke calamiteitenknoppen beschikt de tunneloperator conform de VRC op zijn beeldscherm ook nog over een gemakkelijk bedienbaar (touch screen) groepscommando "calamiteit" en een groepscommando "evacuatie".

Met het groepscommando "calamiteit" kan de operator bij het optreden van één of meer detectiesignalen via één handeling de tunnelinstallaties van de geselecteerde tunnelbuis (en de ondersteunende nevenbuis) in calamiteitenbedrijf schakelen. De functionaliteit van dit groepscommando "calamiteit" is gelijk aan die van de fysieke calamiteitenknop. Bij het groepscommando "evacuatie" worden alle maatregelen ter ondersteuning van het vluchtproces geactiveerd: vluchtinstructies via luidsprekersysteem en HF ("inbraak" via autoradio's), contourverlichting rondom vluchtdeuren en geluidsbakens boven vluchtdeuren.

Gegeven het feit dat het in calamiteitenbedrijf schakelen van de installaties ook wordt ondersteund door geautomatiseerde veiligheidssystemen (zie paragraaf 4.1 en paragraaf 5.2 en 5.3) kan de betrouwbaarheid van de fysieke calamiteitenknop en de touch screen groepscommando's "calamiteit" en "evacuatie" liggen in de orde van grootte van de door de VRC vereiste technische betrouwbaarheid van de ventilatie: 98% per aanspraak. Het ligt daarbij voor de hand om deze betrouwbaarheidseis te hanteren voor elke maatregel onder de knop afzonderlijk, dus bijvoorbeeld:

⁶ Bij de geautomatiseerde veiligheidssystemen speelt een dergelijk tijdverlies niet, aangezien de automatische ingreep via de PLC's en de besturing loopt, die zich bij de tunnel bevinden. De automatische ingreep gaat dus buiten de verkeerscentrale om.

- Vluchtweg in gereedheid brengen met een betrouwbaarheid van 98% per aanspraak;
- Verlichting in incidentbuis op optimaal niveau schakelen met een betrouwbaarheid van 98% per aanspraak;
- Tunnelventilatie in incidentbuis in calamiteitenstand schakelen met een betrouwbaarheid van 98% per aanspraak;
- Enz.

Een dergelijke betrouwbaarheid sluit ook aan bij het feit dat we bij de tunneloperator ook nog te maken hebben met het aspect menselijk falen. Het heeft immers geen zin bovenmatig strenge betrouwbaarheidseisen te stellen aan de techniek als deze niet door de operator wordt gebruikt.

Veel belangrijker is het om aan de operator zichtbaar te maken of het indrukken van de calamiteitenknop, groepscommando calamiteit of groepscommando evacuatie het gewenste effect heeft, c.q. of alle maatregelen succesvol zijn geactiveerd. De operator moet derhalve na het indrukken van de calamiteitenknop of een groepscommando op zijn beeldscherm direct een overzicht krijgen van de status van de installaties "onder de knop":

- Geactiveerd, of:
- bezig met activeren, of:
- Niet geactiveerd (binnen de daarvoor gestelde tijd).

De operator moet vervolgens de mogelijkheid hebben om via een touch screen knop in hetzelfde scherm (knop in de statuslijst) de maatregel c.q. installatie alsnog te activeren⁷. Op deze wijze heeft de tunneloperator overzicht over de gang van zaken, bevindt de betrokkenheid van de operator zich op een adequaat niveau en is de betrouwbaarheid van het schakelen naar calamiteitenbedrijf (met of zonder evacuatie) eveneens op een adequaat niveau geborgd.

Consequentie van deze filosofie is wel dat er zeer strenge eisen worden gesteld aan de betrouwbaarheid van de informatievoorziening aan de operator, over de status van de maatregelen/installaties. Omdat het hier alleen gaat om signalering en melding wordt een betrouwbaarheid van 99,5% per aanvraagde maatregel haalbaar geacht (het VIC-net, een belangrijke schakel in de signalering en melding, heeft een betrouwbaarheid van 99,9%).

Samenvattend gelden de volgende eisen voor de calamiteitenknop en de groepscommando's "calamiteit" en "evacuatie" op het beeldscherm:

- Faalkans per maatregel: < 0,02 per aanspraak (ook bij het separaat activeren van de maatregel indien activering via knop/groepscommando niet tot het gewenste resultaat heeft geleid);
- Reactietijd knop/groepscommando:
 - o Bedenk-/hersteltijd voor operator: instelbaar, bijvoorbeeld 5 tot 10 seconden;
 - o Reactie maatregelen na bedenk-/hersteltijd: 2 seconden;
- Betrouwbaarheid informatie aan operator over status maatregelen na indrukken knop/groepscommando: 99,5% per aanvraag per maatregel.

⁷ In de MMI van de RWS-tunnelstandaard van de Landelijk Tunnelregisseur is hier in voorzien.

6 Conclusies en aanbevelingen

6.1 Conclusies

Op basis van een analyse van de VRC, een gevarenanalyse en een kwantificering van de veiligheidseffecten met RWSQRA versie 2.0 (berekening RRF's), zijn de volgende geautomatiseerde veiligheidsfuncties in tunnels in algemene zin te beschouwen als "veiligheidskritisch", omdat ze een SIL-niveau van 1 of hoger moeten hebben:

1. Automatisch inschakelen op calamiteitenstand van de tunnelventilatie in de incidentbuis;
2. Automatisch in gereedheid brengen van de veilige vluchtweg;
3. Voorkomen dat automatische afsluiting van de tunnelbuizen onbeheerst gebeurt.

Bij lange tunnels, met een hoge kans op files, kan aanvullend de volgende functie "veiligheidskritisch" zijn⁸:

4. Het voorkomen dat de staart van een file (nagenoeg stilstaand verkeer) die benedenstrooms van de tunnel ontstaat de tunnel ingroeit (filevermijding).

Verder kan, los van de vraag of een veiligheidsmaatregel een geautomatiseerd systeem is dat onder de scope van de IEC-61508 valt, worden geconcludeerd dat de volgende veiligheidsmaatregelen een significante invloed hebben op de reductie van het groepsrisico in de tunnel, omdat de RRF (onder sommige omstandigheden) duidelijk hoger is dan de RRF van de overige veiligheidsmaatregelen:

- Vluchtdeuren
- Overdrukventilatie vluchtgang
- Tunnelventilatie
- Tunneloperator (bij categorie A tunnels)
- Filevermijding (bij lange tunnels)
- Riolering
- (Regeling) ingangsverlichting

De overige veiligheidsmaatregelen hebben een lagere RRF, c.q. deze maatregelen hebben ieder afzonderlijk weinig effect op het (verlagen van het) groepsrisico. Dit komt omdat er bij veel veiligheidsmaatregelen in de tunnel in feite sprake is van een zekere "functionele redundantie": bij falen van een bepaalde maatregel is er vaak nog een andere maatregel die ook voorziet in de functie van de falende maatregel. Zo is er bijvoorbeeld sprake van verschillende detectiemiddelen die brand kunnen detecteren en zijn er verschillende "protection layers" die in kunnen grijpen indien een brand wordt gedetecteerd. Deze functionele redundantie betekent niet noodzakelijkerwijs dat bepaalde veiligheidsmaatregelen overbodig zijn (de onderhavige analyse is er niet op gericht om na te gaan welke veiligheidsvoorzieningen kunnen vervallen). Wel is aangetoond dat de functionele redundantie leidt tot minder strenge betrouwbaarheidseisen voor elke maatregel afzonderlijk.

⁸ De RWS-tunnelstandaard voorziet niet in een geautomatiseerd filevermijdingssysteem, maar in een procedurele maatregel. In verreweg de meeste gevallen zal dit voldoende zijn (zie paragraaf 5.5). Indien een geautomatiseerd systeem is een aanvullende maatregel, die alleen moet worden overwogen indien dit noodzakelijk is om aan de wettelijke veiligheidseisen te voldoen of de betrouwbaarheidseisen voor de veilige vluchtweg (zie paragraaf 5.3).

6.2 Aanbevelingen

Pas de in hoofdstuk 5 genoemde SIL-niveaus of betrouwbaarheidseisen toe bij de geautomatiseerde veiligheidsfuncties (veiligheidskritische functies).

Zorg dat de vereiste betrouwbaarheid wordt bereikt c.q. aangetoond door toepassing van een gevalideerde methode, dus de IEC-61508 of een foutenboom-analyse waarbij de betrouwbaarheid van de softwarecomponenten in de foutenboom worden gekwantificeerd met TOPAAS (en waarbij het totstandkomingsproces van de software "aan de voorkant" zodanig wordt ingericht, dat dit leidt tot een resultaat dat qua betrouwbaarheid hoog scoort in TOPAAS).

De score-parameters in TOPAAS dekken niet de volledige IEC-61508 af, maar wel de belangrijkste aspecten die in de IEC-61508 een rol spelen. Er kan dus over worden gediscussieerd of een "full-blown" toepassing van de IEC-61508 een beter resultaat zou kunnen worden behaald dan met TOPAAS. Dit is echter geenszins zeker. Ook de IEC-61508 kent zijn beperkingen. Bovendien is er tot nu toe in Nederland nog geen ervaring opgedaan met de toepassing van de norm bij tunnels, waardoor de vraag gerechtvaardigd is of RWS en de markt al de vereiste taakvolwassenheid hebben om de norm volledig toe te passen. Aangezien de norm eisen stelt aan de organisaties die er mee werken is dit probleem ook niet eenvoudig op te lossen door middel van bijvoorbeeld het "inhuren" van de juiste specialisten. Al met al bestaat er een voorkeur voor de toepassing van TOPAAS in plaats van de IEC-61508.

Besteedt naast de geautomatiseerde veiligheidssystemen nog nadere aandacht aan de betrouwbaarheid van de calamiteitenknop en de groepscommando's "calamiteit" en "evacuatie" (zie paragraaf 5.6) Toon ook de betrouwbaarheid van deze voorzieningen aan met een foutenboomanalyse.

Pas bij de overige veiligheidsvoorzieningen een betrouwbaarheid toe die in de praktijk eenvoudig haalbaar is met COTS, en/of stem de betrouwbaarheid af op de beschikbaarheidseisen aan de tunnel. Deze betrouwbaarheid hoeft in principe niet te worden aangetoond met een foutenboomanalyse, maar moet in de ontwerpdocumentatie wel aannemelijk worden gemaakt.

Tenslotte:

- Zorg dat het falen van de installaties / maatregelen die deel uit maken van de keten van de veiligheidskritische functies of de calamiteitenknop en de groepscommando's "calamiteit" en "evacuatie" automatisch worden gemeld aan de tunneloperator (en de technisch beheerder), zodat compenserende maatregelen (en herstelmaatregelen) kunnen worden genomen.
- Zorg dat ook het falen van de regeling van de ingangsverlichting automatisch aan de operator wordt gemeld (en de technisch beheerder).
- Zorg voor een goede opleiding, training en oefening voor de tunneloperator;
- Pas een onderhoudsregime op de riolering van de tunnel toe die aansluit bij het (relatief hoge) veiligheidseffect van deze maatregel.

Lijst van aangehaalde literatuur

1. NEN-EN-IEC-61508 (2010), Functionele veiligheid van elektrische/ elektronische/ programmeerbare elektronische systemen verband houdend met veiligheid:
 - Deel 1: Algemene eisen;
 - Deel 2: Richtlijnen voor elektrische/ elektronische/ programmeerbare elektronische systemen verband houdend met veiligheid;
 - Deel 3: Eisen voor programmatuur
 - Deel 4: Definities en afkortingen
 - Deel 5: Voorbeelden van methoden voor het vaststellen van veiligheidsniveaus
 - Deel 6: Richtlijnen voor de toepassing van IEC-61508-2 en IEC-61508-3.
 - Deel 7: Overzicht van technieken en voorzieningen.
2. TOPAAS, Een structurele aanpak voor faalkansanalyse van software intensieve systemen, Rijkswaterstaat Dienst Infrastructuur, versie Definitief, 1 april 2011
3. Veiligheidsrichtlijnen deel C (VRC), inclusief bijlagen, Steunpunt Tunnelveiligheid, 15 juni 2009.
4. Gebruikershandleiding RWSQRA 2.0, Steunpunt Tunnelveiligheid, doc.nr. 4818-2011-0008, versie Definitief, januari 2011.
5. Het RWSQRA-model voor wegtunnels, versie 2.0, Achtergronddocument, Steunpunt Tunnelveiligheid, doc.nr. 4818-2011-0009, versie Definitief, januari 2011.
6. NEN-EN-IEC-61511 (2005), Functionele veiligheid, Veiligheidssystemen voor de procesindustrie:
 - Deel 1: Raamwerk, definities, systeem, hardware- en software-eisen;
 - Deel 2: Richtlijnen voor de toepassing van IEC-61508-1;
 - Deel 3: Richtlijnen voor de bepaling van de vereiste veiligheidsintegriteitsniveaus.
7. Basisspecificatie TTI RWS Tunnelsysteem, versie Definitief 1.1, 1 september 2011, doc.nr. HB 1264869.
8. Systeemontwerp RWS Tunnelsysteem, versie Definitief 1.1, 1 september 2011, doc.nr. HB 1266157.
9. Bedrijfsprocessen (UPP) RWS Tunnelsysteem, versie Definitief 1.1, 1 september 2011, doc.nr. HB 1462429.

Bijlage A Gevarenanalyse

In het kader van de vaststelling van de functionele veiligheidssystemen (geautomatiseerde veiligheidssystemen) is een gevarenanalyse uitgevoerd, om na te gaan in welke mate de verschillende beschermingslagen uit het Protection Layer model (zie paragraaf 2.3) bijdragen aan het beheersen van de gevaren. De resultaten van deze analyse zijn weergegeven in de onderstaande tabel.

Nr.	Gevaren (hazards)	Protection Layers + toelichting 1 = Inherent veilig ontwerp 2 = Automatische beschermingslaag 3 = Menselijke beschermingslaag 4 = Autonome beschermingslaag 5 = Actieve beschermingslaag 6 = Passieve beschermingslaag 7 = Hulpverleningslaag	Functionele veiligheidssystemen (in betekenis IEC-61508)
A.	Verkeer		
A.1	Frontale botsing (spookrijder)	1, 3, 7 Het risico wordt met name beheerst door een inherent veilig ontwerp (1 rijrichting per tunnelbuis) in combinatie met het ingrijpen door de operator (afkruisen rijstroken, afsluiten tunnel e.d.) indien er een spookrijder wordt gesignaleerd. Noch de VRC, noch de tunnelstandaard van de LTR voorziet in een aanvullend geautomatiseerd veiligheidssysteem ter bescherming tegen spookrijders (bijvoorbeeld afkruisen rijstrook spookrijder op basis van detectie tegengestelde rijrichting). De vraag is ook of een dergelijk systeem wenselijk is gegeven het feit dat het middel bij disfunctioneren erger kan zijn dan de kwaal.	N.v.t.
A.2	Frontale botsing (tegenverkeer bij onderhoud)	1, 2, 3, 7 Preventieve maatregelen door snelheidsverlaging, evt. scheiding tussen rijrichtingen, enz. Er is geen aanvullende automatische functie om bij een desondanks dreigende botsing in te grijpen.	N.v.t.
A.3	Kop-staart botsing	1, 2, 3, (4), 7 Risico wordt met name beheerst door combinatie inherent veilig tunnelontwerp en het verkeerssysteem (MTM) dat snelheidsverlaging instelt bij detectie langzaam rijdend of stilstaand verkeer. Er zou kunnen worden voorzien in een geautomatiseerd systeem (beschermingslaag 4) om nagenoeg stilstaand verkeer in de tunnel te voorkomen, en daarmee de kans op botsingen op de staart van een file in de tunnel (met mogelijk nog brand als gevolg) te verkleinen. Dit heeft met name zin bij tunnels waarbij de kans op een file benedenstrooms van de tunnel relatief hoog is.	Eventueel voorkomen van nagenoeg stilstaand verkeer in de tunnels, als gevolg van een file benedenstrooms van de tunnel: – SOS-detectie – Beperken toestroom verkeer tunnel in bij detectie (MTM, tunneldosering e.d.), of: – Stimuleren doorstroming verkeer benedenstrooms van de tunnel (b.v. openstellen spitsstrook).

Nr.	Gevaren (hazards)	Protection Layers + toelichting 1 = Inherent veilig ontwerp 2 = Automatische beschermingslaag 3 = Menselijke beschermingslaag 4 = Autonome beschermingslaag 5 = Actieve beschermingslaag 6 = Passieve beschermingslaag 7 = Hulpverleningslaag	Functionele veiligheidssystemen (in betekenis IEC-61508)
A.4	Botsing tegen obstakel op weg (incl. bijvoorbeeld voertuigen die reeds zijn gebotst)	1, 2, 3, 7 Automatische afkruising van een rijstrook bij detectie van een blokkade, conform hoofdstuk 9 van de VRC, vindt niet plaats, omdat deze functie vooralsnog buiten de scope van het gecertificeerde MTM-systeem valt en ook niet is opgenomen in de tunnel-standaard van de Landelijk tunnelregisseur.	N.v.t.
A.5	Zijdelingse botsing	1, 3, 7 Risico kan desgewenst worden beheerst door maatregelen als inhaalverbod, "keep your lane" of scheiding door barrier (inherent veilig ontwerp). Geen verdere geautomatiseerde veiligheidssystemen om in te grijpen bij dreigende botsing (is op de open weg ook geen sprake van).	N.v.t.
A.6	Botsing tegen tunnelwand	1, 3, 7 Risico wordt met name beheerst door overzichtelijk wegontwerp en barriers (inherent veilig ontwerp).	N.v.t.
B.	Meteo		
B.1	Verblinding door zonlicht	1, 2 Zonodig maatregelen om zonlicht af te schermen bij oost-west oriëntatie tunnel (inherent veilig ontwerp).	N.v.t.
B.2	Zwart gat (ongelijkmatige overgang van licht naar donker bij binnen rijden tunnel)	1, 2, 3, 4 Risico's worden met name beheerst door eventuele snelheidsverlaging (MTM + evt. operator) in combinatie met automatische regeling verlichting tunnelingang (overgangszone) op basis van meting daglicht (beschermingslaag 4). Is overdag van belang, met name op zonnige dagen.	Automatisch regelen verlichting overgangszone tot juiste niveau, afhankelijk van lichtniveau buiten
B.3	Slecht zicht (neerslag, mist, beslagen voorruit e.d.)	2 Risico wordt beheerst door voertuigtechniek en door MTM-systeem, dat automatisch snelheidsbeperking instelt bij detectie langzaam rijdend of stilstaand verkeer.	N.v.t.
B.4	Water op wegdek	3 Beheersing van dit risico vindt plaats door de operator (afsluiten tunnel), op basis van camerabeelden en/of meldingen van het niveau in de waterkelders. Er is verder geen aanvullend geautomatiseerd veiligheidssysteem dat ingrijpt bij (dreigend) water op wegdek.	N.v.t.

Nr.	Gevaren (hazards)	Protection Layers + toelichting 1 = Inherent veilig ontwerp 2 = Automatische beschermingslaag 3 = Menselijke beschermingslaag 4 = Autonome beschermingslaag 5 = Actieve beschermingslaag 6 = Passieve beschermingslaag 7 = Hulpverleningslaag	Functionele veiligheidssystemen (in betekenis IEC-61508)
B.5	Gladheid (sneeuw, ijzel e.d.)	2 Gladheid zal met name optreden buiten de tunnel. Risico wordt beheerst door voertuigtechniek en door MTM-systeem, dat automatisch snelheidsbeperking instelt bij detectie langzaam rijdend of stilstaand verkeer.	N.v.t.
B.6	Wind	1 Risico eventueel te beheersen met windschermen o.l.d.	N.v.t.
B.7	Blikseminslag	1 Invloed van bliksem op ongevalskans is verwaarloosbaar. TTI zijn beschermd tegen blikseminslag (inherent veilig ontwerp). Kans dat blikseminslag juist optreedt op moment dat er een ongeval in de tunnel plaatsvindt is eveneens verwaarloosbaar.	N.v.t.
C.	Waterhuishouding en geofysica		
C.1	Inundatie tunnel	1 Als de polder waarin de tunnel zich bevindt onderloopt (inclusief tunnel) is tunnelveiligheid niet relevant meer.	N.v.t.
C.2	Aardbeving	1 Wordt beheerst door inherent veilig ontwerp. Constructie moet volgens normen (eurocode e.d.) bestand zijn tegen aardbeving. Indien netstroom en/of besturing uitvallen wordt de tunnel gecontroleerd afgesloten. Kans dat aardbeving juist optreedt op moment dat er een ongeval in de tunnel plaatsvindt is eveneens verwaarloosbaar.	N.v.t.
D.	Disfunctioneren tunnelsysteem		
D.1	Uitval energievoorziening	1, 3, 4 Kans op algehele stroomuitval wordt beperkt door toepassing noodstroomvoorziening naast netstroomvoorziening (inherent veilig ontwerp). Indien de netstroomvoorziening en de noodstroomvoorziening beiden falen, wordt de tunnel automatisch beheerst afgesloten, met behulp van de energie van de no-break (beschermingslaag 4). Als de no-break ook faalt moet de tunnel "handmatig" door het wegpersoneel worden afgesloten.	Automatisch beheerst afsluiten tunnel bij uitval netstroom + noodstroomvoorziening

Nr.	Gevaren (hazards)	Protection Layers + toelichting 1 = Inherent veilig ontwerp 2 = Automatische beschermingslaag 3 = Menselijke beschermingslaag 4 = Autonome beschermingslaag 5 = Actieve beschermingslaag 6 = Passieve beschermingslaag 7 = Hulpverleningslaag	Functionele veiligheidssystemen (in betekenis IEC-61508)
D.2	Uitval centrale bediening	1, 4 Bij uitval centrale bediening wordt de tunnel automatisch gecontroleerd afgesloten (beschermingslaag 4), door de "heartbeat" of "watchdog", die continu controleert of de centrale bediening nog functioneert.	Automatisch afsluiten tunnel bij falen centrale bediening
D.3	Uitval besturing	1, 3 Tunnel kan in dat geval gecontroleerd worden afgesloten (door de operator) via de noodbediening.	N.v.t.
D.4	Onbedoeld functioneren VeVa	1, 3 Moet bij voorkeur worden beheerst door inherent veilig ontwerp (fysieke vergrendeling o.l.d.). Aangezien VeVa in het dagelijks proces niet wordt gebruikt, (alleen in onderhoudssituatie e.d.) is dit in principe mogelijk (voor gebruik ter plekke ontgrendelen).	N.v.t.
D.5	Onbeheerst neergaan afsluitboom	1, 3, 4 Indien de tunnel (automatisch) wordt afgesloten bij een (vermoeden van) calamiteit, dient dit beheerst te gebeuren: eerst snelheidsverlaging met MTM, daarna VRI op "rood" en daarna afsluitboom neer. De kans op een ongeval bij het onbeheerst neergaan van een afsluitboom is vrij groot: een voertuig botst tegen de afsluitboom en/of een achterop komend voertuigen botst tegen een voertuig dat remt voor de afsluitboom. De kans op doden bij een dergelijk ongeval is relatief groot. Er kan hier dus niet worden volstaan met een inherent veilig ontwerp, zoals bijvoorbeeld een lichte afsluitboom die afbreekt bij aanrijding. Er moeten maatregelen worden getroffen om het onbeheerst neergaan van de afsluitboom tegen te gaan (beschermingslaag 4).	Bewaking onbeheerst neergaan afsluitboom
D.6	Onbedoeld functioneren VRI	1, 3, 4 Betreft het onbeheerst op "rood" gaan van de VRI, dat wil zeggen voordat eerst een snelheidsverlaging is ingesteld (MTM) met het bijbehorende risico van kop-staart botsingen. Net als bij de afsluitboom (D.5) moeten maatregelen worden genomen om dit te voorkomen (beschermingslaag 4).	Bewaking onbeheerst op "rood" gaan VRI

Nr.	Gevaren (hazards)	Protection Layers + toelichting 1 = Inherent veilig ontwerp 2 = Automatische beschermingslaag 3 = Menselijke beschermingslaag 4 = Autonome beschermingslaag 5 = Actieve beschermingslaag 6 = Passieve beschermingslaag 7 = Hulpverleningslaag	Functionele veiligheidssystemen (in betekenis IEC-61508)
D.7	Vallende objecten (TTI e.d.)	1 Risico wordt beheerst door inherent veilig ontwerp: deugdelijke bevestiging aan het plafond, al dan niet met een extra veiligheidskabel om te voorkomen dat installaties naar beneden vallen bij losraken van plafond. De ventilatoren vormen het grootste risico, deze kunnen losraken door bijvoorbeeld trillingen bij het in- en uitschakelen. Daarnaast kunnen installaties, bijvoorbeeld signaalgevers, los raken door bijvoorbeeld aanrijding.	N.v.t.
E.	Brand en gevaarlijke stoffen		
E.1	Vlammen, warmtestraling	6, 7 Beheersing brand in voertuigen (en daarmee bescherming direct betrokken slachtoffers) valt buiten de scope van tunnelsysteem. Omvang plasbrand wordt beperkt door het rioleringsstelsel (beschermingslaag 6). tunnel).	N.v.t.
E.2	Rook (hitte, toxiciteit)	1, 3, 5, 7 Voor de mensen voor het brandongeval is de langsventilatie van belang. Voor de mensen voorbij het brandongeval zijn de vluchtvoorzieningen van belang. Het starten van de ventilatie en het in gereedheid brengen van de veilige vluchtweg kan door de operator worden geïnitieerd. Daarnaast wordt volgens de VRC de ventilatie automatisch opgestart en wordt de veilige vluchtweg automatisch in gereedheid gebracht (beschermingslaag 5). Tevens wordt de tunnelbuis automatisch afgesloten (beschermingslaag 4).	Automatische opstart ventilatie incidentbuis (al dan niet als onderdeel van stand-by fase na detectie of calamiteitenbedrijf) op basis van zichtmeting, of branddetectie, of slanghaspel uitnemen, of draagbaar brandblusapparaat uitnemen. Automatisch inschakelen ventilatie nevenbuis (om kortsluiting rook te voorkomen) Automatisch in gereedheid brengen vluchtweg Automatisch afsluiten tunnel
E.3	Explosie instantaan	1, 7 Risico kan alleen worden beheerst door categoriekeuze tunnel (A, B, C, D of E conform ADR), dus inherent veilige maatregelen. Overige maatregelen vallen buiten scope tunnelsysteem.	N.v.t.

Nr.	Gevaren (hazards)	Protection Layers + toelichting 1 = Inherent veilig ontwerp 2 = Automatische beschermingslaag 3 = Menselijke beschermingslaag 4 = Autonome beschermingslaag 5 = Actieve beschermingslaag 6 = Passieve beschermingslaag 7 = Hulpverleningslaag	Functionele veiligheidssystemen (in betekenis IEC-61508)
E.4	Explosie met vertraging	1, 3, 7 In tegenstelling tot instantane explosie kan bij een met vertraging optredende explosie (of een risico daartoe) nog worden ingegrepen door de operator.	N.v.t.
E.5	Toxische gassen en dampen	1, 3, 7 Voor de mensen voor het ongeval is de langsventilatie van belang. Voor de mensen voorbij het ongeval zijn de vluchtvoorzieningen van belang. Het starten van de ventilatie en het in gereedheid brengen van de veilige vluchtweg moet door de operator worden geïnitieerd. Aangezien er geen detectiemiddelen in de tunnel zijn voor toxische dampen is er hierbij geen sprake van ondersteuning door een geautomatiseerd veiligheidssysteem, zoals dat bij brand wel het geval is (zie bij E.2).	N.v.t.
F.	Terrorisme	Bij terroristische actie worden een of meer van de bovengenoemde gevaren/hazards manifest. Kans op terroristische acties is dermate klein dat het risicoprofiel van de gevaren hier niet wezenlijk door wordt gewijzigd.	N.v.t.

Bijlage B Berekening Risk Reduction Factoren

Algemene uitgangspunten

Voor de berekening van de RRF's is gebruik gemaakt van RWSQRA versie 2.0. Daarbij is als referentie uitgegaan van een tunnelbuis met de configuratie en verkeerssituatie conform buis Oost 2 van de Tweede Coentunnel:

Geometrie				
Naam	Waarde	Eenheid	Domein	Omschrijving
L_buis	765	m	[80; 20000]	Lengte (gesloten deel) van de tunnelbuis
L_neer	382.5	m	[0; L_buis]	Lengte neergaand deel van de tunnelbuis
L_hor	0	m	[0; L_buis - L_neer]	Lengte horizontale deel van de tunnelbuis
L_op	382.5	m	[0; L_buis]	Lengte opgaand deel van de tunnelbuis
B_buis	15	m	[3; 30]	Breedte van het wegdek (tussen opstaande randen)
L_hart	100	m	[30; L_buis]	Hart-op-hart afstand van de vluchtdeuren
N_rij	3	-	[1; 6]	Aantal rijstroken in de tunnelbuis
N_tot_rijstroken	5	-	[N_rij; 30]	Totaal aantal rijstroken in de tunnelbuizen voor verkeer van de tunnel
N_vlucht	1	-	[0; 2]	Aantal vluchtstroken in de tunnelbuis

Periode en verkeersintensiteiten				
Naam	Waarde	Eenheid	Domein	Omschrijving
T_spits	11	uur	(0; 12)	Gemiddeld aantal uren 'spits' per etmaal in de tunnelbuis
T_nacht	6	uur	(0; 12)	Gemiddeld aantal uren 'nacht' per etmaal in de tunnelbuis
T_dag	7	uur	(0; 24)	Aantal uren per etmaal dat het 'dag' (niet spits of nacht) is
I_buis	27300000	mvt/jaar	[1E3; 1E9]	Verkeersintensiteit per jaar in de tunnelbuis
I_max	2000	mvt/uur	[1; 3000]	Maximale verkeerscapaciteit per rijstrook
I_spitsuur	4487.67	mvt/uur	(0; I_max . N_rij]	Gemiddelde verkeersintensiteit in de buis per spitsuur
I_spits	18017995.05	mvt/jaar	(0; 1E9]	Verkeersintensiteit tijdens de 'spits' per jaar
I_nachtuur	747.945	mvt/uur	(0; I_max . N_rij]	Gemiddelde verkeersintensiteit in de buis per nachtuur
I_nacht	1637999.55	mvt/jaar	(0; 1E9]	Verkeersintensiteit tijdens de 'nacht' per jaar
I_dag	7644005.4	mvt/jaar	(0; 1E9]	Verkeersintensiteit tijdens de 'dag' per jaar
I_daguur	2991.782935	mvt/uur	[0; 1E9]	Gemiddelde verkeersintensiteit per 'daguur'

Verkeerssamenstelling				
Naam	Waarde	Eenheid	Domein	Omschrijving
A_auto_s	0.89	-	[0; 1]	Fractie personenauto's (of motor) tijdens de 'spits'
A_auto_d	0.89	-	[0; 1]	Fractie personenauto's (of motor) tijdens de 'dag'
A_auto_n	0.89	-	[0; 1]	Fractie personenauto's (of motor) tijdens de 'nacht'
A_bus_s	0.01	-	[0; 1]	Fractie bussen tijdens de 'spits'
A_bus_d	0.01	-	[0; 1]	Fractie bussen tijdens de 'dag'
A_bus_n	0.01	-	[0; 1]	Fractie bussen tijdens de 'nacht'
A_vracht_s	0.1	-	[0; 1]	Fractie vrachtauto's tijdens de 'spits'
A_vracht_d	0.1	-	[0; 1]	Fractie vrachtauto's tijdens de 'dag'
A_vracht_n	0.1	-	[0; 1]	Fractie vrachtauto's tijdens de 'nacht'
I_vracht	2730000	mvt/jaar	[0; 1E9]	Totaal aantal vrachtauto's per jaar in de tunnelbuis

Gevaarlijke stoffen				
Naam	Waarde	Eenheid	Domein	Omschrijving
I_expl	0	mvt/jaar	[0; 0,1 . I_vracht]	Aantal vrachtwagens geladen met explosieven (E) per jaar in de tunnelbuis
I_LF1	5585	mvt/jaar	[0; 0,3 . I_vracht]	Aantal (volle) tankwagens met stofcategorie LF1 (brandbare vloeistof gevaarsklasse 1) per jaar in de tunnelbuis
I_LF2	18768	mvt/jaar	[0; 0,3 . I_vracht]	Aantal (volle) tankwagens met stofcategorie LF2 (brandbare vloeistof gevaarsklasse 2) per jaar in de tunnelbuis
I_LT	60	mvt/jaar	[0; 0,1 . I_vracht]	Aantal (volle) tankwagens met toxische vloeistof (LT) per jaar in de tunnelbuis
I_GF	0	mvt/jaar	[0; 0,1 . I_vracht]	Aantal (volle) druktankwagens met brandbaar tot vloeistof verdicht gas (GF) per jaar in de tunnelbuis
I_GT	0	mvt/jaar	[0; 0,1 . I_vracht]	Aantal (volle) druktankwagens met toxisch tot vloeistof verdicht gas (GT) per jaar in de tunnelbuis

Voorzieningen				
Naam	Waarde	Eenheid	Omschrijving	
A_oper	Ja	-	Houdt een operator (in controlekamer) toezicht op de tunnel?	
A_vent	Ja	-	Is een langsventilatiesysteem aanwezig?	
A_luid	Ja	-	Is een HF en/of luidsprekersysteem aanwezig?	
A_bekl	Ja	-	Is hittewerende bekleding aanwezig?	
A_blus	Ja	-	Zijn brandblusmiddelen aanwezig?	
A_comm	Ja	-	Is alarmering door weggebruiker mogelijk (noodtelefoon in hulppost aanwezig en/of mobiele telefonie mogelijk)?	
A_snel	Ja	-	Is een snelheidsdetectiesysteem aanwezig?	
A_brand_temp	Ja	-	Is branddetectie met temperatuurmeting aanwezig?	
A_brand_CO	Nee	-	Is branddetectie met CO-meting aanwezig?	
A_brand_zicht	Ja	-	Is branddetectie met zichtmeting aanwezig?	
H_zicht	370	m	Hart-op-hart afstand van zichtmeting	
A_calam	Ja	-	Beschikt de operator over een calamiteitenknop?	
A_sluit	Verkeerslicht en slagboom	-	Is het afsluiten van de tunnelbuis mogelijk?	
L_afsluit	285	m	De afstand tussen de plaats waar de tunnelbuis wordt afgesloten en de ingang van de tunnelbuis	
A_deur	Altijd ontgrendeld	-	Zijn er vluchtdeuren in de verkeersbuis, en zo ja, welk type?	
T_vertontgr	0	min	Tijdsvertraging bij het ontgrendelen van de vluchtdeuren	
K_vlucht	middenwand	-	Wand waarin de vluchtdeuren zijn aangebracht	
C_autventsnel	Nee	-	Wordt ventilatiesysteem aangestuurd door snelheidsdetectie?	
C_autventbrand	Ja	-	Wordt ventilatiesysteem aangestuurd door branddetectie?	
C_autdeursnel	Nee	-	Worden vluchtdeuren ontgrendeld bij snelheidsdetectie?	
C_autdeurbrand	Nee	-	Worden vluchtdeuren ontgrendeld bij branddetectie?	
C_calvent	Ja	-	Start ventilatie bij gebruik calamiteitenknop?	
C_calsluit	Ja	-	Wordt de verkeersbuis afgesloten bij gebruik calamiteitenknop?	
C_caldeur	Nee	-	Worden vluchtdeuren ontgrendeld bij gebruik calamiteitenknop?	
C_riool	4	m3/min	Capaciteit van de riolering	
T_snelaut	0	min	Tijdsduur tussen snelheidsdetectie en automatisch opstarten	

Overige basisuitgangspunten

- Bij de berekening van de RRF van een bepaalde voorziening is de faalkans van de betreffende voorziening op "0" gezet (default waarde is veranderd in "0"), om de RRF zuiverder te kunnen berekenen. De default-faalkansen van de overige voorzieningen zijn daarbij gehandhaafd.
- Frequentie file in spits benedenstrooms van de tunnel: 0,2 x per etmaal
- Systeem vermijding nagenoeg stilstaand verkeer in tunnel als gevolg van file benedenstrooms: ingreep na 5 minuten (dus file kan zich 5 minuten lang opbouwen voordat ingreep plaatsvindt)
- Bij falen of ontbreken systeem vermijding nagenoeg stilstaand verkeer in tunnel kan de file zich 60 minuten lang opbouwen (lees: er vindt geen belemmering van de fileopbouw plaats).
- Bij falen of ontbreken riolering worden de plasgroottes bij uitstroming brandbare en toxische stoffen 2x zo groot ten opzichte van situatie met riolering.
- Bij falen of ontbreken regeling ingangsverlichting wordt de letselonevals kans over de eerste 210m van het gesloten deel van de tunnel op jaarbasis een factor 25 hoger (210m is de afgelegde afstand bij 120 km/u, gedurende de tijd die de ogen nodig hebben om te accommoderen bij het binnen rijden van de tunnel; dit is zeer conservatief gerekend, aangezien de ongevalskans alleen overdag zal toenemen, met name als er sprake is van een heldere zonnige dag).
- Overige default-waarden zijn altijd gehandhaafd.

RRF's veiligheidsmaatregelen Tweede Coentunnel, buis Oost 2

Voorzieningen	Punt dichtste bij normlijn		Oriëntatie-waarde f[Or.,N]	Factor met f[N]/ f[Or.,N]	Factor zonder f[N]/ f[Or.,N]	RRF	SIL
	N	f[N]					
Compleet	26	1.2100E-05	1.4793E-04	12.23	n.v.t.	n.v.t.	n.v.t.
Geen operator	26	1.2167E-05	1.4793E-04	12.23	12.16	1.01	0
Geen ventilatie	80	7.8173E-06	1.5625E-05	12.23	2.00	6.12	0 of 1
Geen luidspreker/HF	26	1.2100E-05	1.4793E-04	12.23	12.23	1.00	0
Geen hittew. bekl.	26	1.2100E-05	1.4793E-04	12.23	12.23	1.00	0
Geen blusvoorz.	26	1.2100E-05	1.4793E-04	12.23	12.23	1.00	0
Geen alarmering weggebruiker	26	1.2116E-05	1.4793E-04	12.23	12.21	1.00	0
Geen snelheidsdetectie	26	1.2134E-05	1.4793E-04	12.23	12.19	1.00	0
Geen temp.meting	26	1.2227E-05	1.4793E-04	12.23	12.10	1.01	0
Geen zichtmeting	26	1.2233E-05	1.4793E-04	12.23	12.09	1.01	0
Geen calamiteitenknop	26	1.2101E-05	1.4793E-04	12.23	12.22	1.00	0
Geen afsluiting tunnel	26	1.2100E-05	1.4793E-04	12.23	12.23	1.00	0
Geen vent. Branddetect.	26	1.2735E-05	1.4793E-04	12.23	11.62	1.05	0
Geen vent. door CK	26	1.2101E-05	1.4793E-04	12.23	12.22	1.00	0
Geen afsluiting door CK	26	1.2100E-05	1.4793E-04	12.23	12.23	1.00	0
Geen vluchtdeuren	160	8.2471E-06	3.9063E-06	12.23	0.47	25.81	1
Geen vermijding file benedenstrooms	26	1.23E-05	1.4793E-04	12.23	12.06	1.01	0
Geen riolering	52	1.21E-05	3.70E-05	12.23	3.06	4.00	0
Geen regeling ingangsverlichting	26	1.24E-05	1.4793E-04	12.23	11.90	1.03	0

Betrouwbaarheidseisen beheerst afsluiten tunnel (MTM, VRI en afsluitboom)

In het voorgaande is onderzocht wat het effect is op het risico als de tunnel niet wordt afgesloten in geval van calamiteit. Voor het afsluiten van de tunnel wordt gebruik gemaakt van de MTM, een VRI en de afsluitboom. De afsluitboom en de VRI kunnen echter ook falen in de zin dat de afsluitboom onbeheerst neer gaat (zonder eerst de snelheid te verlagen met de MTM en daarna de VRI op "rood" te zetten, dus in een situatie met op normale snelheid rijdend verkeer) en de VRI onbeheerst op "rood" gaat, zonder snelheidsverlaging door de MTM. In beide gevallen is er sprake van gevaarlijk falen.

De betrouwbaarheidseisen die aan deze wijzen van falen worden gesteld kunnen echter niet worden afgeleid met Risk Reduction Factoren met RWSQRA. Dit falen effect heeft op de letselonevals frequentie (een invoerparameter in RWSQRA) en RWSQRA bovendien rekening houdt met tunneleffecten, die bij een ongeval buiten de tunnel niet optreden. De betrouwbaarheidseisen die worden gesteld aan het onbeheerst neergaan van de afsluitboom en het onbeheerst op "rood" gaan van de VRI worden dus op andere wijze afgeleid, door het vaststellen van het maximaal aantal doden dat mag optreden als gevolg van deze faalwijzen. Hiervoor wordt gebruik gemaakt van de verwachtingswaarde voor het aantal doden per jaar in de buis Oost 2 van de Tweede Coentunnel. Met RWSQRA 2.0 is berekend dat deze verwachtingswaarde 0,08044115 per jaar bedraagt.

Als nu wordt aangenomen dat het aantal doden dat valt door het disfunctioneren van de afsluitboom of de VRI maximaal 1% hiervan mag bedragen, dan mag het aantal doden door het ongevraagd neergaan van de afsluitboom of het ongevraagd op "rood" gaan van de VRI maximaal 0,8044E-03 per jaar bedragen. De betrouwbaarheidseisen kunnen dan als volgt worden afgeleid.

Afsluitboom:

Er wordt aangenomen dat er iedere keer dat de afsluitboom onbeheerst naar beneden gaat een letselongeval plaatsvindt, ofwel omdat een voertuig tegen de afsluitboom botst, ofwel omdat achteropkomende voertuigen opbotsen tegen een voertuig dat tijdig remt. Als daarbij tevens conservatief wordt aangenomen dat de kans op een dodelijk ongeval bij een dergelijk letselongeval ongeveer 25% bedraagt, dan is het maximale aantal keren dat een afsluitboom ongevraagd naar beneden mag gaan: $4 * 0,8044E-03 = 0,0032176$ per jaar (ongeveer 3x per 1000 jaar).

Automatische afsluiting van de tunnel vindt plaats op basis van diverse detecties, die wijzen op een grote waarschijnlijkheid dat er sprake is van brand (zie hoofdstuk 9 VRC). De kans op brand is gelijk aan $2,0E-08$ / mvtkm.

De verkeersintensiteit in de tunnelbuis bedraagt 27.300.000 mvt per jaar. De kans op brand is derhalve: $27.300.000 * 0,765 * 2,0E-08 = 0,41769$ per jaar.

De toegestane faalkans (met betrekking tot onbeheerst afsluiten) bedraagt derhalve: $0,0032176 / 0,41769 = 0,0077$ per aanvraag.

Als nog rekening wordt gehouden met valse meldingen, en wordt aangenomen dat er sprake is van evenveel valse meldingen als terechte meldingen, dan is de toegestane faalkans $0,0077 / 2 = 0,00385$ per aanvraag.

Deze faalkanseis vraagt om beheersmaatregelen die zich bevinden op het niveau

SIL 2.

N.B.: ook in geval van een ernstige technische storing (uitval netstroom + noodstroom, of uitval bediening of besturing) moet de tunnelbuis automatisch en beheerst worden afgesloten. De kans op een ernstige technische storing wordt echter vooralsnog verwaarloosbaar geacht ten opzichte van de kans op detectie van een mogelijke brand.

VRI:

De kans dat er een letselongeval plaatsvindt als de VRI onbeheerst op "rood" gaat (zonder snelheidsverlaging door de MTM) zal lager zijn dan bij het onbeheerst neergaan van de afsluitboom, omdat er geen sprake is van een fysiek obstakel en omdat er in algemene zin sprake is van een "rood-negatie" door de weggebruikers. Omdat er geen sprake is van een fysiek obstakel zal ook de kans dat er sprake is van een dodelijk ongeval bij een letselongeval ook lager dan bij het onbeheerst sluiten van de afsluitboom. Er wordt hier conservatief aangenomen dat het onbeheerst op "rood" gaan van de VRI in 50% van de gevallen leidt tot een letselongeval en dat een letselongeval in 12,5% van de gevallen leidt tot een dodelijk slachtoffer. Dit betekent dat de toegestane faalkansen factor 4 hoger is dan bij de afsluitboom: $4 \times 0,00385 = 0,0154$ per aanvraag. Dit komt overeen met beheersmaatregelen conform niveau **SIL 1**.

RRF's veiligheidsmaatregelen Tweede Coentunnel, buis Oost 2 bij lengte 2500m

(Lengte tunnelbuis 2500m in plaats van 765m, verder alle parameters hetzelfde)

Voorzieningen	Punt dichtste bij normlijn		Oriëntatie-waarde f[Or.,N]	Factor met f[N]/f[Or.,N]	Factor zonder f[N]/f[Or.,N]	RRF	SIL
	N	f[N]					
Compleet	26	1.2105E-05	1.4793E-04	12.22	n.v.t.	n.v.t.	n.v.t.
Geen operator	26	1.2177E-05	1.4793E-04	12.22	12.15	1.01	0
Geen ventilatie	80	9.6574E-06	1.5625E-05	12.22	1.62	7.55	0 of 1
Geen luidspreker/HF	26	1.2105E-05	1.4793E-04	12.22	12.22	1.00	0
Geen hittew. bekl.	26	1.2105E-05	1.4793E-04	12.22	12.22	1.00	0
Geen blusvoorz.	26	1.2105E-05	1.4793E-04	12.22	12.22	1.00	0
Geen alarmering weggebruiker	26	1.2125E-05	1.4793E-04	12.22	12.20	1.00	0
Geen snelheidsdetectie	26	1.2138E-05	1.4793E-04	12.22	12.19	1.00	0
Geen temp.meting	26	1.2247E-05	1.4793E-04	12.22	12.08	1.01	0
Geen zichtmeting	26	1.2254E-05	1.4793E-04	12.22	12.07	1.01	0
Geen calamiteitenknop	26	1.2106E-05	1.4793E-04	12.22	12.22	1.00	0
Geen afsluiting tunnel	26	1.2105E-05	1.4793E-04	12.22	12.22	1.00	0
Geen vent. Branddetect.	26	1.2865E-05	1.4793E-04	12.22	11.50	1.06	0
Geen vent. door CK	26	1.2106E-05	1.4793E-04	12.22	12.22	1.00	0
Geen afsluiting door CK	26	1.2100E-05	1.4793E-04	12.22	12.23	1.00	0
Geen vluchtdeuren	220	1.4164E-05	2.0661E-06	12.22	0.15	83.78	1
Geen vermijding file benedenstrooms	850	5.22E-07	1.3841E-07	12.22	0.27	46.11	1
Geen riolering	52	1.21E-05	3.70E-05	12.22	3.06	4.00	0
Geen regeling ingangsverlichting	320	6.12E-08	9.7656E-07	12.22	15.95	1	0

RRF's veiligheidsmaatregelen Tweede Coentunnel, buis Oost 2 bij lengte 2500m, hoge kans file benedenstrooms en GEEN systeem vermijding nagenoeg stilstaand verkeer in tunnel

(Lengte tunnelbuis 2500m in plaats van 765m, filekans 1x per etmaal in plaats van 0,2 x per etmaal, en geen vermijding stilstaand verkeer in tunnel; verder alle parameters hetzelfde)

Voorzieningen	Punt dichtste bij normlijn		Oriëntatie-waarde	Factor met $f[N]/f[Or.,N]$	Factor zonder $f[N]/f[Or.,N]$	RRF	SIL
	N	f[N]					
Compleet	850	2.6110E-07	1.3841E-07	0.53	n.v.t.	n.v.t.	n.v.t.
Geen ventilatie	80	1.1551E-04	1.5625E-05	0.53	0.14	3.92	0
Geen vluchtdeuren	675	1.3410E-04	2.1948E-07	0.53	0.00	323.89	2
Geen vermijding file benedenstrooms	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Geen regeling ingangsverlichting	850	7.88E-07	1.3841E-07	0.53	0.18	3.02	0

RRF's veiligheidsmaatregelen Keizer Karel tunnel

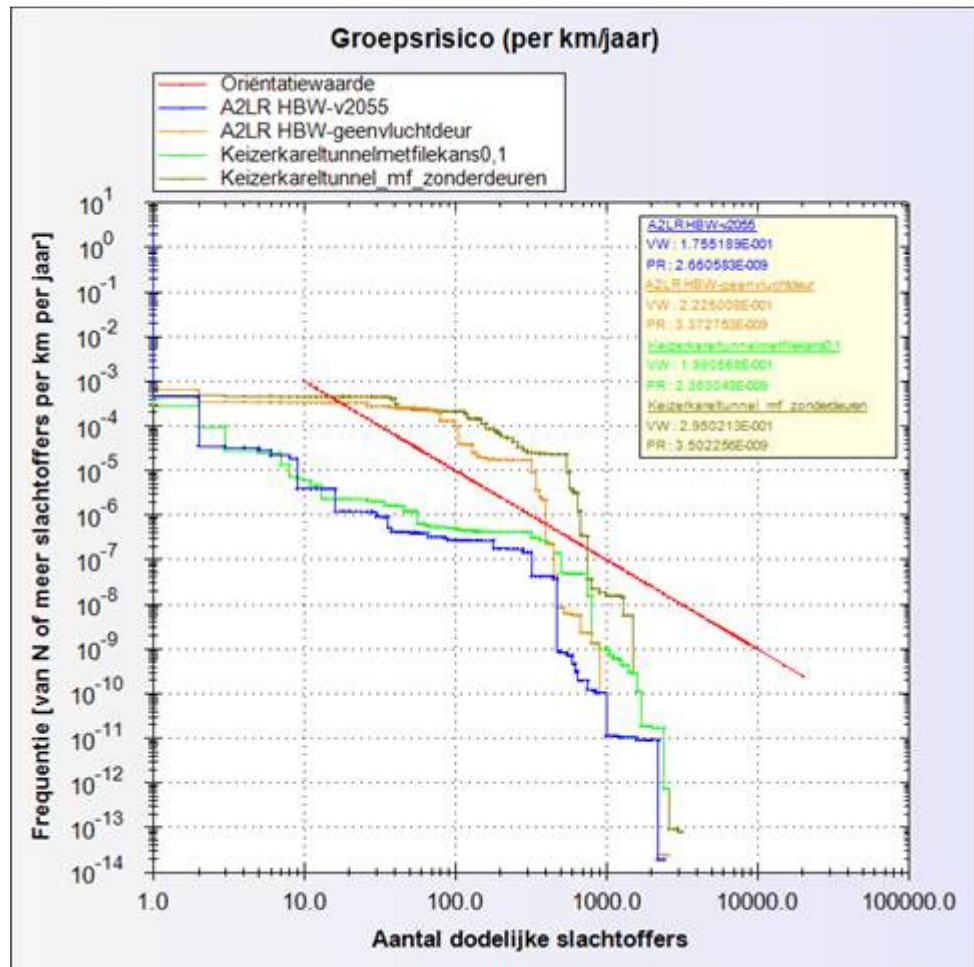
Geometrie				
Naam	Waarde	Eenheid	Domein	Omschrijving
L_buis	1827	m	[80; 20000]	Lengte (gesloten deel) van de tunnelbuis
L_neer	344	m	[0; L_buis]	Lengte neergaand deel van de tunnelbuis
L_hor	1139	m	[0; L_buis - L_neer]	Lengte horizontale deel van de tunnelbuis
L_op	344	m	[0; L_buis]	Lengte opgaand deel van de tunnelbuis
B_buis	18,5	m	[3; 30]	Breedte van het wegdek (tussen opstaande randen)
L_hart	100	m	[30; L_buis]	Hart-op-hart afstand van de vluchtdeuren
N_rij	4	-	[1; 6]	Aantal rijstroken in de tunnelbuis
N_tot_rijstroken	8	-	[N_rij; 30]	Totaal aantal rijstroken in de tunnelbuizen voor verkeer van de tunnel
N_vlucht	1	-	[0; 2]	Aantal vluchtstroken in de tunnelbuis

Periode en verkeersintensiteiten				
Naam	Waarde	Eenheid	Domein	Omschrijving
T_spits	4	uur	(0; 12)	Gemiddeld aantal uren 'spits' per etmaal in de tunnelbuis
T_nacht	8	uur	(0; 12]	Gemiddeld aantal uren 'nacht' per etmaal in de tunnelbuis
T_dag	12	uur	(0; 24)	Aantal uren per etmaal dat het 'dag' (niet spits of nacht) is
I_buis	28200000	mvt/jaar	[1E3; 1E9]	Verkeersintensiteit per jaar in de tunnelbuis
I_max	2300	mvt/uur	[1; 3000]	Maximale verkeerscapaciteit per rijstrook
I_spitsuur	6180	mvt/uur	(0; I_max . N_rij]	Gemiddelde verkeersintensiteit in de buis per spitsuur
I_spits	9022800	mvt/jaar	(0; 1E9]	Verkeersintensiteit tijdens de 'spits' per jaar
I_nachtuur	772	mvt/uur	(0; I_max . N_rij]	Gemiddelde verkeersintensiteit in de buis per nachtuur
I_nacht	2254240	mvt/jaar	(0; 1E9]	Verkeersintensiteit tijdens de 'nacht' per jaar
I_dag	16922960	mvt/jaar	(0; 1E9]	Verkeersintensiteit tijdens de 'dag' per jaar
I_daguur	3863.689498	mvt/uur	[0; 1E9]	Gemiddelde verkeersintensiteit per 'daguur'

Verkeerssamenstelling				
Naam	Waarde	Eenheid	Domein	Omschrijving
A_auto_s	0.85	-	[0; 1]	Fractie personenauto's (of motor) tijdens de 'spits'
A_auto_d	0.85	-	[0; 1]	Fractie personenauto's (of motor) tijdens de 'dag'
A_auto_n	0.85	-	[0; 1]	Fractie personenauto's (of motor) tijdens de 'nacht'
A_bus_s	0.01	-	[0; 1]	Fractie bussen tijdens de 'spits'
A_bus_d	0.01	-	[0; 1]	Fractie bussen tijdens de 'dag'
A_bus_n	0.01	-	[0; 1]	Fractie bussen tijdens de 'nacht'
A_vracht_s	0.14	-	[0; 1]	Fractie vrachtauto's tijdens de 'spits'
A_vracht_d	0.14	-	[0; 1]	Fractie vrachtauto's tijdens de 'dag'
A_vracht_n	0.14	-	[0; 1]	Fractie vrachtauto's tijdens de 'nacht'
I_vracht	3948000	mvt/jaar	[0; 1E9]	Totaal aantal vrachtauto's per jaar in de tunnelbuis

Gevaarlijke stoffen				
Naam	Waarde	Eenheid	Domein	Omschrijving
I_expl	0	mvt/jaar	[0; 0,1 . I_vracht]	Aantal vrachtwagens geladen met explosieven (E) per jaar in de tunnelbuis
I_LF1	1878	mvt/jaar	[0; 0,3 . I_vracht]	Aantal (volle) tankwagens met stofcategorie LF1 (brandbare vloeistof gevaarsklasse 1) per jaar in de tunnelbuis
I_LF2	2017	mvt/jaar	[0; 0,3 . I_vracht]	Aantal (volle) tankwagens met stofcategorie LF2 (brandbare vloeistof gevaarsklasse 2) per jaar in de tunnelbuis
I_LT	11	mvt/jaar	[0; 0,1 . I_vracht]	Aantal (volle) tankwagens met toxische vloeistof (LT) per jaar in de tunnelbuis
I_GF	1453	mvt/jaar	[0; 0,1 . I_vracht]	Aantal (volle) druktankwagens met brandbaar tot vloeistof verdicht gas (GF) per jaar in de tunnelbuis
I_GT	0	mvt/jaar	[0; 0,1 . I_vracht]	Aantal (volle) druktankwagens met toxisch tot vloeistof verdicht gas (GT) per jaar in de tunnelbuis

Voorzieningen: conform Coentunnel.



Voorzieningen	Punt dichtste bij normlijn		Oriëntatie-waarde	Factor met	Factor zonder	RRF	SIL
	N	f[N]					
Compleet	425	2,29E-07	4,94E-07	0,46	n.v.t.	n.v.t.	n.v.t.
Geen operator	1000	3,02E-07	9,07E-08	0,46	3,33	7,17	1
Geen ventilatie	280	6,42E-07	1,11E-06	0,46	0,58	1,24	0
Geen snelheidsdetectie	400	2,85E-07	5,54E-07	0,46	0,51	1,11	0
Geen zicht- en temperatuurmeting	425	2,58E-07	4,94E-07	0,46	0,52	1,13	0
Geen calamiteitenknop	400	2,80E-07	5,54E-07	0,46	0,50	1,09	0
Geen slagbomen	425	2,79E-07	4,94E-07	0,46	0,57	1,22	0
Geen vluchtdeuren	525	2,26E-05	3,31E-07	0,46	68,24	146,97	2

RRF's veiligheidsmaatregelen tunnel A2 Leidsche Rijn (Hoofdbuis West)

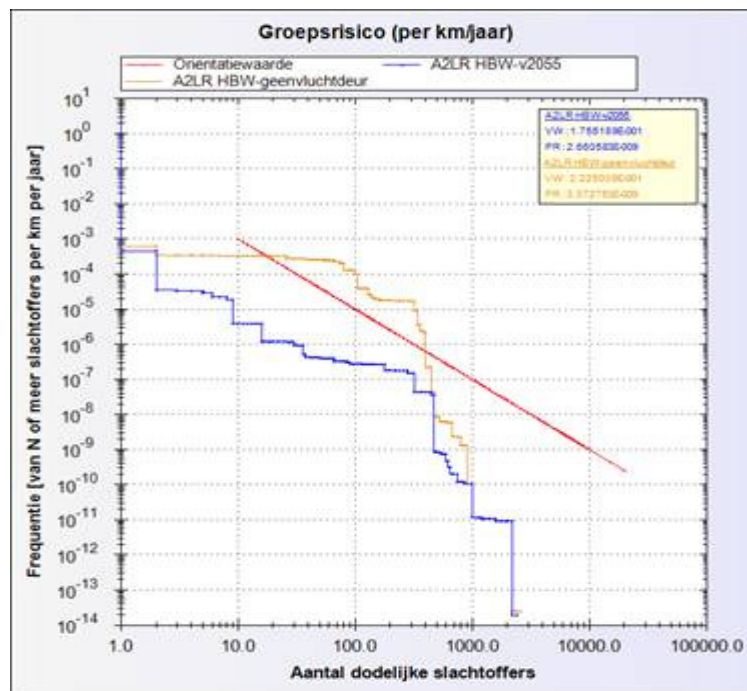
Geometrie				
Naam	Waarde	Eenheid	Domein	Omschrijving
L_buis	1650	m	[80; 20000]	Lengte (gesloten deel) van de tunnelbuis
L_neer	0	m	[0; L_buis]	Lengte neergaand deel van de tunnelbuis
L_hor	1650	m	[0; L_buis - L_neer]	Lengte horizontale deel van de tunnelbuis
L_op	0	m	[0; L_buis]	Lengte opgaand deel van de tunnelbuis
B_buis	13,5	m	[3; 30]	Breedte van het wegdek (tussen opstaande randen)
L_hart	100	m	[30; L_buis]	Hart-op-hart afstand van de vluchtdeuren
N_rij	3	-	[1; 6]	Aantal rijstroken in de tunnelbuis
N_tot_rijstroken	6	-	[N_rij; 30]	Totaal aantal rijstroken in de tunnelbuizen voor verkeer van de tunnel
N_vlucht	1	-	[0; 2]	Aantal vluchtstroken in de tunnelbuis

Periode en verkeersintensiteiten				
Naam	Waarde	Eenheid	Domein	Omschrijving
T_spits	4	uur	(0; 12]	Gemiddeld aantal uren 'spits' per etmaal in de tunnelbuis
T_nacht	8	uur	(0; 12]	Gemiddeld aantal uren 'nacht' per etmaal in de tunnelbuis
T_dag	-1	uur	(0; 24)	Aantal uren per etmaal dat het 'dag' (niet spits of nacht) is
I_buis	27411500	mvt/jaar	[1E3; 1E9]	Verkeersintensiteit per jaar in de tunnelbuis
I_max	2300	mvt/uur	[1; 3000]	Maximale verkeerscapaciteit per rijstrook
I_spitsuur	5632	mvt/uur	(0; I_max . N_rij]	Gemiddelde verkeersintensiteit in de buis per spitsuur
I_spits	-1	mvt/jaar	(0; 1E9]	Verkeersintensiteit tijdens de 'spits' per jaar
I_nachtuur	1036	mvt/uur	(0; I_max . N_rij]	Gemiddelde verkeersintensiteit in de buis per nachtuur
I_nacht	-1	mvt/jaar	(0; 1E9]	Verkeersintensiteit tijdens de 'nacht' per jaar
I_dag	-1	mvt/jaar	(0; 1E9]	Verkeersintensiteit tijdens de 'dag' per jaar
I_daguur	-1	mvt/uur	[0; 1E9]	Gemiddelde verkeersintensiteit per 'daguur'

Verkeerssamenstelling				
Naam	Waarde	Eenheid	Domein	Omschrijving
A_auto_s	0.8286	-	[0; 1]	Fractie personenauto's (of motor) tijdens de 'spits'
A_auto_d	0.8286	-	[0; 1]	Fractie personenauto's (of motor) tijdens de 'dag'
A_auto_n	0.8286	-	[0; 1]	Fractie personenauto's (of motor) tijdens de 'nacht'
A_bus_s	0.01	-	[0; 1]	Fractie bussen tijdens de 'spits'
A_bus_d	0.01	-	[0; 1]	Fractie bussen tijdens de 'dag'
A_bus_n	0.01	-	[0; 1]	Fractie bussen tijdens de 'nacht'
A_vracht_s	0.1614	-	[0; 1]	Fractie vrachtauto's tijdens de 'spits'
A_vracht_d	0.1614	-	[0; 1]	Fractie vrachtauto's tijdens de 'dag'
A_vracht_n	0.1614	-	[0; 1]	Fractie vrachtauto's tijdens de 'nacht'
I_vracht	4424216	mvt/jaar	[0; 1E9]	Totaal aantal vrachtauto's per jaar in de tunnelbuis

Gevaarlijke stoffen				
Naam	Waarde	Eenheid	Domein	Omschrijving
I_expl	0	mvt/jaar	[0; 0,1 . I_vracht]	Aantal vrachtwagens geladen met explosieven (E) per jaar in de tunnelbuis
I_LF1	4550	mvt/jaar	[0; 0,3 . I_vracht]	Aantal (volle) tankwagens met stofcategorie LF1 (brandbare vloeistof gevaarsklasse 1) per jaar in de tunnelbuis
I_LF2	5621	mvt/jaar	[0; 0,3 . I_vracht]	Aantal (volle) tankwagens met stofcategorie LF2 (brandbare vloeistof gevaarsklasse 2) per jaar in de tunnelbuis
I_LT	65	mvt/jaar	[0; 0,1 . I_vracht]	Aantal (volle) tankwagens met toxische vloeistof (LT) per jaar in de tunnelbuis
I_GF	1055	mvt/jaar	[0; 0,1 . I_vracht]	Aantal (volle) druktankwagens met brandbaar tot vloeistof verdicht gas (GF) per jaar in de tunnelbuis
I_GT	0	mvt/jaar	[0; 0,1 . I_vracht]	Aantal (volle) druktankwagens met toxisch tot vloeistof verdicht gas (GT) per jaar in de tunnelbuis

Voorzieningen: conform Coentunnel.



Voorzieningen	Factor met	Factor zonder	RRF	SIL
	f[N]/f[Or.,N]	f[N]/f[Or.,N]		
Compleet	0,15	n.v.t.	n.v.t.	n.v.t.
Geen vluchtdeuren	0,15	17,32	114	2