

## Verificatie en Validatie van een tunnel

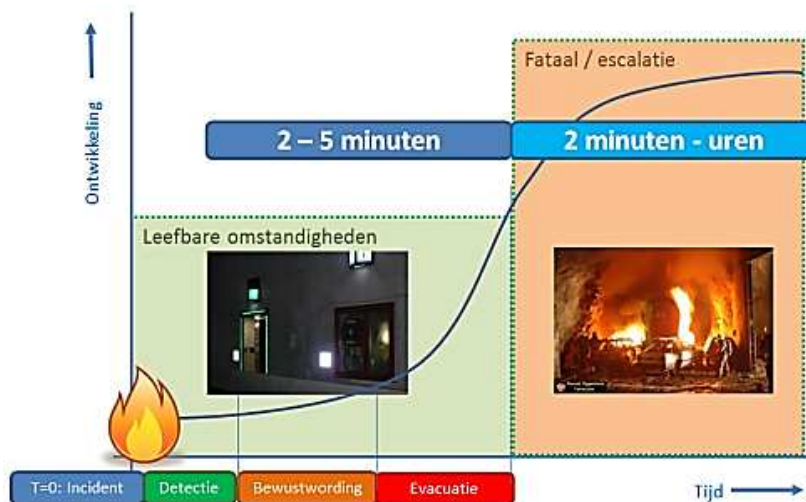
Jeanne Hofmans, Eduard Hartog, Patrick Duisters

Als je door een tunnel rijdt beseft je eigenlijk niet wat daar allemaal mee gemoeid is. Totdat er een keer iets misgaat. Zo ondervond ook onze collega Manon: "Zaterdagavond 23:00. "Wil de bestuurder van de auto met de platte achterband zich melden bij het kastje dat zich enkele meters achter de auto bevindt?" Een half uur later zat de nieuwe achterband erop en was de boa constrictor in de achterbak gelukkig niet te veel afgekoeld."

In dit artikel bespreken we wat een tunnel anders maakt dan een gewone weg. Veiligheid speelt daarin een grote rol. Die veiligheid borg je door verificatie en validatie. Maar hoe dan? In dit artikel gaan we in op de ervaringen van Improve Quality Services bij de verificatie en validatie van tunnels. Dit doen we vanuit twee perspectieven. Ten eerste vanuit het perspectief van een auditor die de V&V toetst. Ten tweede vanuit het perspectief van de projectorganisatie. Het artikel eindigt met suggesties voor de succesvolle verificatie en validatie van een tunnel.

### Wat maakt een tunnel anders dan een weg?

Een tunnel is een gat in de grond waardoor je heen kan om van de ene naar de andere kant te komen. Dat kan zijn te voet, per fiets, met de auto of met de trein. Tunnels worden aangelegd om verschillende redenen: om (vaar)wegen te kruisen of om de leefbaarheid van de omgeving te verhogen. Omdat mensen door tunnels reizen, speelt veiligheid een grote rol.



In tegenstelling tot een normale weg is een tunnel een afgesloten ruimte. Dat heeft vooral impact in geval van een brand. In een tunnel is een brand, door de altijd aanwezige luchtstroom, snel krachtiger. Nog gevaarlijker is de snelle en dodelijke rook die niet weg kan. Een persoon die niet in de juiste richting vlucht is binnen enkele minuten dood.

Een onveilige situatie ofwel calamiteit dient dus zo spoedig mogelijk te worden opgemerkt (gedetecteerd) om escalatie te voorkomen. Daarnaast moeten mensen de mogelijkheid krijgen zichzelf te redden. Hiervoor moeten mensen van de situatie bewust worden gemaakt en worden aangespoord te vluchten. Tenslotte moeten hulpdiensten zoals brandweer en ambulance zo goed mogelijk hun werk kunnen doen. In de tunnel zijn daarom, naast voorzieningen als vluchtwegen, een reeks van installaties aangebracht voor preventie, detectie en afhandeling van calamiteiten. Dit zijn de zogeheten tunnel-technische installaties (TTI). Naast de tunnel technische installaties zijn er installaties voor de goede doorstroming van verkeer: de verkeerstechnische installaties. Samen vormen zij de VTTI.

De operationele aansturing van het tunnelobject gebeurt op basis van bijbehorende werkprocessen zoals die zijn afgesproken met verkeersleiding, weginspecteurs, hulpdiensten, gemeentes, etc.

## Verkeerstechnische en Tunnel Technische installatie (VTTI)

In een tunnel komen meer dan 50 verschillende soorten deelinstallaties voor als onderdeel van de VTTI. Verkeerstechnische installaties zijn installaties die benodigd zijn voor een goede doorstroming van het verkeer. Dit zijn onder andere het stilstanddetectiesysteem, de matrixborden, de Verkeers Regel Installatie (VRI: onder andere verkeerslichten) en slagbomen. Tunneltechnische installaties zijn gericht op het in stand houden van de tunnel en de tunnelveiligheid. Voor instandhouding spelen energie, verlichting, maar ook installaties voor het afpompen van bluswater en eventuele gevaarlijke stoffen een rol. Systemen die specifiek op veiligheid zijn gericht zijn de branddetectie- en zichtmeet- en de communicatiesystemen. Het bediening- en besturingssysteem speelt een centrale rol in de aansturing en bediening van alle systemen.

Sommige installaties komen meerdere keren voor, zoals ventilatoren, hulpposten en noodtelefoons. Andere installaties komen slechts één keer voor, zoals de verbinding met de verkeerscentrale. Sommige installaties hebben een directe relatie met het civiele object. Het belangrijkste voorbeeld hiervan zijn de vluchtdeuren. In onderstaande figuur zijn enkele voorbeelden gegeven van installaties zoals die in een tunnel voorkomen.



De deelinstallaties staan niet op zichzelf. Een slagboom kan pas worden neergelaten als het verkeerslicht (de VRI) voor de slagboom op rood staat. Dat lijkt eenvoudig, maar is in de praktijk lastig. Complexer wordt het in geval van een calamiteit. Juist in het geval van een calamiteit moeten meerdere deelinstallaties correct met elkaar samenwerken. Zo moet de blusapparatuur in gereedheid (op druk) worden gebracht, ventilatie met het juiste vermogen de juiste kant op gaan draaien, verlichting moet worden opgeschaald en vluchtdeuren moeten worden ontgrendeld.

De besturingssoftware is er verantwoordelijk voor dat dit allemaal in de juiste combinaties en in de juiste volgorde gebeurt. In dat integrale aspect zit een belangrijk deel van de complexiteit. En omdat het in het geval van tunnels om de veiligheid van mensen draait, gaan de consequenties in het geval van falen soms veel verder dan tijdverlies, materiële of financiële schade. Het gaat om zwaar letsel en zelfs mensenlevens.

Bij het openen van de Swalmentunnel (A73 bij Roermond) bleek dat de tunnelinstallaties niet goed samenwerkten. De installaties werkten separaat prima, maar het geheel van installaties gaf storingen. Hierdoor kwam de veiligheid in het geding, hoewel de Nederlandse tunnels intrinsiek al veilig zijn door de scheiding van de rijrichtingen in 2 tunnelbuizen. De Swalmentunnel is gedurende langere tijd gesloten geweest om opnieuw de tunnelinstallaties te testen, gericht op de werking van de keten van deelsystemen. Om de veiligheid van nieuwe tunnels te borgen voert Rijkswaterstaat sindsdien audits uit op de verificatie & validatie van de tunnel technische installaties.

## Audits voor Rijkwaterstaat

Om de veiligheid van nieuwe en bestaande tunnels te borgen voert Rijkwaterstaat (RWS) audits uit. Daarvoor heeft RWS Improve Quality Services BV geselecteerd als onafhankelijke partij om audits uit te voeren op de verificatie & validatie (V&V) processen van de tunnel technische installaties VTTI

Improve Quality Services BV heeft inmiddels meerdere tunnelprojecten uitgevoerd (A2, A4, A10, A15, N35). In de audits zijn de V&V processen beoordeeld en is gecontroleerd of aantoonbaar aan de gestelde eisen is voldaan.

Deze audits zijn uitgevoerd op basis van de specialistische kennis van softwarekwaliteit en testen en op basis van de ruime ervaring in andere gereguleerde industrieën, zoals het onder andere het medische domein.

Op basis van de expertise van Improve is in de tunnelprojecten de kwaliteit van het verificatie- en validatieproces onderzocht. Een goed referentiekader daarvoor zijn de software testprocessen zoals gedefinieerd door de International Software Testing Qualification Board (ISTQB) en TMap Next. Maar ook testdocumentatiestandaarden (zoals IEEE-829 en J-STD-016) en (test)volwassenheidsmodellen, zoals CMMI, Testing Maturity Model Integrated (TMMi), IEEE 15504 en Test Process Improvement Next (TPI Next), maken onderdeel uit van het referentiekader.

Een belangrijk onderdeel waar in een audit naar wordt gekeken is de aanwezigheid van een goed V&V proces. Deze begint met het uitvoeren van een productrisicoanalyse. Hierin wordt bepaald welke aspecten, functies of systeemonderdelen het grootste risico vormen. Een groot risico betekent meer diepgang bij de verificatie. Ook bij de audit zelf ligt de focus op de belangrijkste risico's, zoals de veiligheidscritische functies (VKF).

Onderdeel van de toetsing van de V&V processen is het controleren of de beschreven processen ook daadwerkelijk zijn gevolgd. Zijn de resultaten van de productrisicoanalyse aantoonbaar te herleiden naar de testprotocollen? Afwijken van de V&V processen is toegestaan, mits er onderbouwde redenen zijn om dat te doen.



Aantoonbaarheid geldt vooral ook voor het product zelf. Het uiteindelijke tunnelsysteem en al haar deelobjecten dienen aantoonbaar te voldoen aan de gestelde eisen en het ontwerp. De controle van de aantoonbaarheid kenmerkt zich door het traceerbaar kunnen volgen van elke eis via

testspecificaties tot gerapporteerde testresultaten. Dit kan bijvoorbeeld door te controleren of er in de testdocumentatie structureel wordt verwezen naar (de eisen in) het ontwerp. Deze traceerbaarheid onderbouwt dat elke eis gestructureerd is gecontroleerd op de juiste werking.

Een ander belangrijk aspect is de integratie van de deelinstallaties en de daarbij behorende verificatie en validatie. Voor verificatie geldt de vraag: is objectief aangetoond dat de deelinstallaties correct samenwerken (zoals beschreven in de ontwerpen) en daarmee een veilig systeem vormen? In de context van tunnels gaat het om het samenwerken van de detecterende systemen (brand- en stilstanddetectie, zichtmeting), de evacuatiesystemen (vluchtwegen, ventilatie, verlichting en geluidsbakens) en de calamiteit bestrijdende systemen (hulpdiensten en brandblussystemen). Voor validatie is de volgende vraag van belang: zijn de bijbehorende werkprocessen, zoals afgesproken met verkeersleiding, weginspecteurs, hulpdiensten, gemeenten et cetera, vastgelegd en werkbaar? Deze vraag kan worden beantwoord door de beschreven processen te bestuderen, maar ook door belanghebbenden te interviewen.

Tenslotte speelt onderhoudbaarheid een grote rol: is een nieuwe tunnel na openstelling ook in de toekomst veilig? Tijdens de audit worden vragen beantwoord over voorzien en onvoorzien onderhoud. Voor de VTTI is het vooral van belang dat een verificatie-en validatie is geborgd, ook in de onderhoudsfase.

### **Uitvoering van de audit**

De toetsing van het V&V traject begint na de oriëntatie met een documentstudie. Daarbij wordt, naast generieke plannen en processen, gekeken naar diverse ontwerpdocumenten, de Failure Mode and Criticality Analysis (FMECA's) en onderhoudsdocumentatie. Specifiek op het gebied van verificatie en validatie worden (master)testplan(nen) met de teststrategie, testprotocollen en testrapportages bestudeerd. Deze beslaan alle testfasen: van Factory Acceptance Test (FAT) tot integrated Factory Acceptance Test (iFAT) in een fabrieksomgeving, Site Acceptance Test (SAT) tot integrated Site Acceptance Test (iSAT) in de tunnel. De iFAT en de iSAT hebben daarbij betrekking op combinaties van deelinstallaties en het VTTI-systeem als geheel. Omdat het besturingssysteem een centrale rol speelt in de veiligheid speelt deze in de iFAT en iSAT een centrale rol. Of, bij voorkeur, natuurlijk nog eerder, waarbij de koppeling met het besturingssysteem al in de SAT wordt meegenomen.

Na het bestuderen van de testplannen kan worden afgeleid of de testprotocollen conform de teststrategie zijn uitgewerkt.

In de testrapportage ligt de focus op de testresultaten en vastlegging van of verwijzing naar bevindingen. Belangrijk daarbij is dat de protocollen aantoonbaar gevolgd zijn en voorzien van observaties.

Naast de documentstudies worden interviews gehouden met relevante stakeholders. Tijdens de interviews worden auditvragen beantwoord en onduidelijkheden toegelicht. Uiteraard wordt ook getoetst of document, woord en daad overeen komen.

### **Witnessing**

In de laatste fase van een project worden naast de documentstudie en interviews ook witness-testen uitgevoerd. De auditor woont dan testen bij tijdens testen in de feitelijke tunnel. Uit ervaring weten we dat naast functionele testen van (veiligheidskritische) deelinstallaties, de integratietesten het meest interessant zijn. Bij de integratietesten, veelal aangeduid als iSAT, worden deelinstallaties in samenwerking getest,



In het verleden was er minder aandacht voor het testen van het geïntegreerde systeem. Hierdoor kon het voorkomen dat een calamiteitenknop in de praktijk niet deed waarvoor hij bedoeld is: het in gereedheid brengen van diverse deelinstallaties voor het afhandelen van een calamiteit.

De witness-testen geven een goed beeld of de testprotocollen juist zijn. Ook wordt duidelijk of ze correct gevolgd worden, of er bevindingen gelogd worden en hoe het testen verloopt. In sommige gevallen verloopt de test chaotisch en is er veel discussie. Bij andere testen werkt men zeer nauwgezet. Dit hangt sterk af van de kwaliteit van de voorbereiding.

### Inrichting van het testproces bij de Opdrachtnemer

Naast audits heeft Improve Quality Services ook aan de andere kant van de tafel gezeten. Bij de Sluiskiltunnel heeft een consultant van Improve Quality Services het verificatie- en validatie proces bij de opdrachtnemer helpen opzetten. De opdracht was om TMap Next op een pragmatische wijze te gebruiken als testmethode. TMap Next is opgezet vanuit een software achtergrond in een administratieve omgeving. Het was een behoorlijke uitdaging om de methode aan te passen voor gebruik in domein van de civiele techniek en de elektrotechniek. Bijvoorbeeld omdat in deze domeinen gebruik wordt gemaakt van Systems Engineering. Om aansluiting te vinden is gezocht naar overeenkomsten. Net als bij het testen van software worden in deze domeinen product gerelateerde risicoanalyses uitgevoerd (o.a. FMECA). Door hierop aan te sluiten in het testproces wordt goed aangesloten bij het bestaande proces. Om de verschillen tussen VTTI en civiel goed te duiden is een Master Test Plan opgesteld waarin zowel de civiele keuringen als ook de testen van de technische installaties opgenomen zijn. Als apart aandachtspunt is ‘document review’ opgenomen. De reden daarvoor is dat het reviewen van documenten een effectieve en efficiënte vorm van testen is waarmee vroeg fouten gevonden kunnen worden.

Hieronder wordt een schematisch overzicht getoond van de inhoud van het Master Test Plan.

Master Test Plan		
Algemene strategie	Strategie per discipline	Organisatie en control
Visie		Organisatie
Reviewstrategie	Documentreview	Control
Keuringsstrategie	Keuring van civiele objecten	
Teststrategie	Testen van VTTI	
	Testen integrale systeem	

Door onderwerpen specifiek te benoemen moeten zaken duidelijk toegekend worden aan verantwoordelijke personen. Er is daarom een RASCI-tabel<sup>1</sup> en een organogram opgesteld.

Dit heeft zinvolle discussie opgeleverd omdat toen pas duidelijk werd wie verantwoordelijk is voor bepaalde aspecten. Valt een FAT onder de verantwoordelijkheid van de ontwerpmanager, de realisatiemanager of de testmanager? Wat is de rol van Systems Engineering? Door dit samen te bespreken konden alle partijen beter samenwerken om een goed product te leveren!

<sup>1</sup> R= Responsible (verantwoordelijk), A= Accountable (aansprakelijk), S= Support (ondersteuning), C= Consulted (geraadpleegd/geconsulteerd), I= Informed (geïnformeerd)

## Een integraal systeem, bestaande uit civiele objecten en VTTI

Om de integraliteit te borgen is niet alleen gekeken naar de tunneltechnische installaties, maar ook naar het civiele ontwerp- en bouwproces. De uitdaging was om de twee werelden van installatietechniek en civiele techniek zoveel mogelijk op elkaar te laten aansluiten. Niet alleen op het technische vlak, maar ook voor wat betreft samenwerking. Een uitdaging gezien de verschillen in cultuur. Om die cultuurverschillen te overbruggen is het belangrijk om elkaars vertrouwen te winnen. Civiele ingenieurs kijken op een andere wijze tegen veiligheid aan dan informatici en elektrotechnici. In het civiele domein wordt veiligheid vooraf aangetoond op papier (door middel van berekeningen). Als veiligheid mogelijk een discussiepunt is, dan wordt bijvoorbeeld de wand verstevigd. Bij software ook achteraf door testen.

Door als testmanager afwisselend bij Civiel en VTTI te gaan zitten, raak je in gesprek. Door met elkaar te spreken gaan de disciplines elkaar beter begrijpen en kweek je ook begrip hoe de testmanager tegen zaken aankijkt. Bijvoorbeeld dat het redundant uitvoeren van een deelinstallatie een goede veiligheidsmaatregel is, maar dat alleen een vermelding in het ontwerp een onvoldoende borging is. In de praktijksituatie dient getest te worden of de systemen elkaar inderdaad zonder vervelende bijwerkingen kunnen overnemen.

Goed begrip geldt ook voor de overige aanwezige disciplines zoals Systems Engineering (SE), Kwaliteit, Arbeidsomstandigheden en Milieu (KAM) en Onderhoud. Waar liggen de scheidslijnen en waar kun je elkaar versterken?

## Verificatie en validatie van een tunnel: hoe dan?

### Een goede testmanager

Ervaring heeft geleerd dat het laten inrichten en uitvoeren van dit proces door een ervaren testmanager betere resultaten boekt. En met een testmanager wordt dan bedoeld een manager met een test-achtergrond én attitude. Een attitude om effectief te testen in de context van een tunnel: een complex en integraal veiligheid kritisch systeem waarbij veel verschillende disciplines betrokken zijn, die allemaal te maken hebben met V&V.

### Het verificatie- en validatieproces

Op basis van het voorgaande kunnen we concluderen dat het begint met de inrichting van een goed verificatie- en validatieproces. Methodes uit de softwarewereld bieden daarvoor een goede basis, hoewel ze aangepast moeten worden om toegepast te kunnen worden in de wereld van tunnels.

De teststrategie is risico gebaseerd: zwaar testen waar nodig en licht testen waar mogelijk. Een risicogebaseerde teststrategie begint bij een onderbouwde identificatie en analyse van de productrisico's: een productrisicoanalyse. Dit betekent het bepalen van het risico van de verschillende deelinstallaties én van het integrale gebruik. Samen met de stakeholders (zoals bouw, onderhoud, beheer, hulpdiensten) wordt bepaald wat de (veiligheid) kritische deelinstallaties en/of functies zijn. Dit vormt de basis voor een gedifferentieerde risico gebaseerde testaanpak: risicovolle delen worden grondiger getest en bij voorkeur ook als eerste. Een tip bij de productrisicoanalyse is: maak het niet te complex.

Differentiatie in het testproces wordt ook bereikt door in verschillende testfases verschillende aspecten te verifiëren. Naast eisen kunnen logicals, use cases, faalmodi (resultaat FMECA), specifieke risico's, raakvlakken, veiligheidsscenario's et cetera worden getest.

### Traceerbaarheid

Voor RWS is traceerbaarheid van eisen naar testresultaten de belangrijkste manier om objectief aantoonbaar te beoordelen of een tunnel veilig is. Traceerbaarheid is tevens de onderbouwing van de uit te voeren testen en zorgt tevens voor inzicht en onderhoudbaarheid in de toekomst.

Zorg dus voor nauwgezette voorbereiding én uitvoering van de gespecificeerde testen inclusief testrapportage. Opmerkingen, observaties en (verwijzingen naar) bevindingen zijn geen probleem. Ze zijn een toonbeeld van openheid en eerlijkheid. Ook de aanwezigheid van een witness of auditor

hoeft geen probleem te zijn. Indien je een gedegen en onderbouwd testproces hebt ingericht en ook uitvoert bouw je vanzelf aan vertrouwen!

### Negatief testen

Voorzie niet alleen positieve testen (kijk, het werkt!), maar ook alternatieve en negatieve testen (kijk, het is ook robuust!). Een voorbeeld daarvan is use case testing. Met deze techniek kan zelfs in diepgang gedifferentieerd worden. Voor hoog risico deelinstallaties verwachten we testen voor alle mogelijke paden door de use cases, terwijl het voor laag risico deelinstallaties volstaat het om de basis- en alternatieve paden, of zelfs alleen de basispaden af te dekken.

### De tijdslijnen

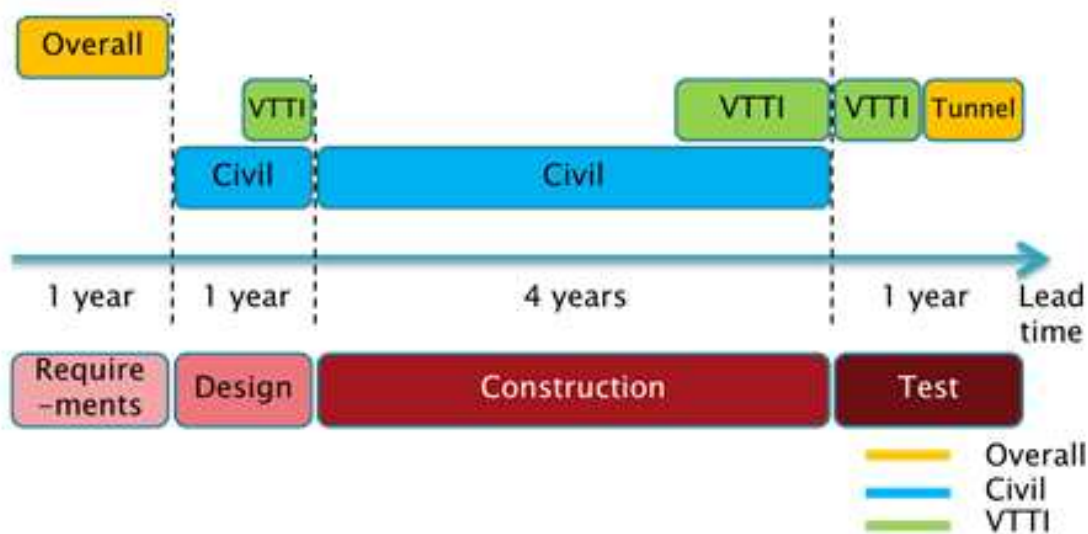
Een uitdaging in tunnelprojecten is het grote verschil in volgordelijkheid. De civiele werkzaamheden zijn vaak al bezig voordat begonnen wordt met het ontwerp voor de technische installaties. Hierdoor kan het gebeuren dat de muur al is gestort zonder ruimte te laten voor het plaatsen van een hulppostkast of vluchtdeur. Wellicht moet in de toekomst eerst de VTTI worden ontworpen en vervolgens het civiele ontwerp plaatsvinden.

Bovendien sluiten de werkzaamheden voor de technische installaties niet op elkaar aan in tijd.

Het ontwerp van de VTTI gebeurt wel in de eerste jaren van het project, maar de uiteindelijke tests gebeuren pas aan het eind van het project. Vaak pas na enkele jaren! Fouten in het ontwerp kunnen daarmee pas laat worden gedetecteerd.

In onderstaande figuur is dit schematisch weergegeven.

In sommige projecten wordt het ontwerp van de VTTI naar voren verschoven. Terwijl de civiele bouw al enkele jaren bezig is, wordt begonnen met het VTTI ontwerp. In dat geval kunnen benodigde wijzigingen op de civiele constructie niet meer worden doorgevoerd. Het is voorgekomen dat de tunnel er al lag, maar er geen uitsparingen waren gemaakt voor de hulppostkasten.



### Conclusie

Een tunnel is toch meer dan een gat in de weg. Door de focus op veiligheid en de complexiteit van een tunnelsysteem komt er bij de verificatie en validatie van een tunnel nogal wat kijken. Niet alleen zijn veel domeinen betrokken, zelfs binnen de VTTI moeten meerdere deelinstallaties samenwerken. In dit artikel hebben we de ervaringen van Improve Quality Services BV op het gebied van tunnelaudits en projectervaringen gedeeld. Mocht je een keer in meer detail ervaringen willen uitwisselen, dan zijn wij daar uiteraard toe bereid.

### Over Improve Quality Services:

Improve Quality Services is een gespecialiseerde organisatie, gericht op innovatieve en hoogwaardige dienstverlening op het gebied van testen en kwaliteitsmanagement. Kwaliteit is leidend bij alles wat wij doen. Improve streeft continu naar verbetering en innovatie en is leidend op zijn vakgebied. Wij bieden Opleidingen, Consultancy en Interim diensten om onze klanten te helpen betere IT-producten te maken.

### Over de auteurs:

**Patrick Duisters:** Patrick heeft ruim 16 jaar ervaring op het gebied van het testen van software en systemen. Hij is internationaal actief als trainer / docent, adviseur en auditor. Hij heeft jaren ervaring als test architect in het medische domein en heeft meerdere tunnelaudits uitgevoerd.



**Eduard Hartog:** Eduard heeft meer dan 15 jaar ervaring met zowel testen als kwaliteitsmanagement in het technische domein. Niet alleen is hij betrokken geweest bij tunnelaudits, ook is hij voor tunnelprojecten betrokken geweest bij het opstellen van Mastertestplannen.



**Jeanne Hofmans:** Jeanne heeft, als tester, testmanager en consultant, ruim 10 jaar ervaring op het gebied van het testen van software en systemen. Zij is voornamelijk actief in technische domeinen, waaronder het medische. Zij heeft meerdere tunnelaudits uitgevoerd en is testmanager geweest voor een tunnel.

