



Rapportage Sectordialoog Softwarebetrouwbaarheid

In het kader van de Richtlijn Softwarebetrouwbaarheid

Datum: Juni 2021

Status: Definitief





Inhoudsopgave

1	Voorwoord	5
2	Managementsamenvatting	7
3	Leeswijzer	7
4	Terugkerende onderwerpen	8
4.1	Versie 0.8 wordt goed ontvangen	8
4.2	Geef nog meer how-to informatie	8
4.3	Deel het stuk op in kwaliteits-, opdrachtgevend- en audit onderdelen ..	8
4.4	Voeg toe wat bij goed opdrachtgeverschap hoort.....	8
4.5	Integreer Cybersecurity.....	8
4.6	Kwaliteit van de mensen maakt de kwaliteit van de software	8
4.7	Maak het aanbesteden 'softwarebetrouwbaarheid vriendelijker'	8
4.8	Bouw kalibratiemomenten in het proces in.....	9
4.9	Rijkswaterstaat vormt een kennis speerpunt in de internationale markt	9
5	Dialoog 1.....	10
5.1	Leesbaarheid en bruikbaarheid.....	10
5.1.1	Korter en gericht	10
5.1.2	Prioriteiten aangeven	10
5.1.3	Illustreer	10
5.2	Inhoudelijk	10
5.2.1	V-Model prima. Waterval voorschrijven niet nodig	10
5.2.2	ISO25010.....	10
5.2.3	Integreer cyberveiligheid	11
5.2.4	Ga software als onderdeel van COTS betrekken.....	11
5.2.5	Sturen op kwaliteitssysteem en externe audits	11
5.2.6	Testen.....	11
5.3	Samen leren	11
5.3.1	Neem de lead.....	11
5.4	Aanbesteden.....	11
5.4.1	Werk samen met opdrachtnemer aan de eisenspecificatie.....	11
5.4.2	Expertise	12
5.4.3	Relevantie zoeken en niet vast zitten aan één aanbestedingsvorm	12
6	Dialoog 2.....	13
6.1	V-Model ok.	13
6.1.1	Waterval relatie V-Model	13
6.1.2	Stapeling staat beste oplossing in de weg	13



6.1.3	Haal tijdsdruk weg, zorg voor voldoende en tijdig inzetbare expertise	13
6.1.4	Beperk je in overeenkomsten tot de essentie	13
6.1.5	Opdrachtnemer extern laten auditen: prima	14
6.1.6	Audit met de juiste competenties op software betrouwbaarheid (en vermijd placebo's)	14
6.1.7	Aanbesteden: Dilemma dat de meterprijs meeweegt	14
6.1.8	Investeer in de samenwerking	14
6.1.9	MDD en Centraliseer de requirements repository	14
6.1.10	Design for testability	14
7	Dialoog 3	15
7.1	Volledig	15
7.2	Aanbesteden	15
7.2.1	Software apart	15
7.2.2	Lifecycle in de EMVI criteria	15
7.2.3	Kun je meer standaard oplossingen uitvragen	15
7.2.4	Uitvragen ISO61508 heeft gewenste filterwerking	15
7.2.5	SRA fase in aanbesteding meenemen	15
7.3	Na aanbesteding	16
7.3.1	Dubbelcheck en kalibreren van de opdracht in SRA fase	16
7.3.2	Verdieping aannemer in bestaande situatie belangrijk: Veldinventarisatie	16
7.4	Ontwikkeling en beheer (hfdst. 6)	16
7.4.1	SIG tools – meer ruimte geven	16
7.5	Testen(hfdst.7)	16
7.5.1	Traceerbaarheid naar de testcases	16
7.5.2	ISTQB en TMAP	16
7.5.3	Simulaties opnemen	16
7.5.4	Lever ook de complete ontwikkel- en teststraat op	16
7.6	Wijzigingsbeheer (hfdst.8)	16
7.6.1	Lifecycle management voor standaard bouwblokken	16
8	Dialoog 4	17
8.1	Leesbaarheid	17
8.2	Gehanteerde normen	17
8.2.1	V-Model /waterval	17
8.2.2	61508 is niet gelijk aan softwarebetrouwbaarheid	17
8.2.3	Integreer cybersecurity	17
8.2.4	Compartimenteer	17
8.3	Safety critical vs. mission critical	17
8.3.1	Safety critical systeemontwikkeling vergt ervaring	17



8.4 Samenwerking met opdrachtnemers	17
8.4.1 Vaste afstem- en kalibratie momenten benoemen	17
8.4.2 Impact op de organisatie	18
8.4.3 Meer concrete handvatten voor implementatie	18
8.5 Overige	18
8.5.1 Tooling	18
8.5.2 Proven technology voor safety-critical toepassingen.....	18
9 Bijlage: 0.8 versie	19



1 Voorwoord

Rijkswaterstaat werkt aan een richtlijn softwarebetrouwbaarheid en is voornemens deze structureel te hanteren in toekomstige projecten waarin steeds vaker expliciet eisen zullen worden gesteld aan de betrouwbaarheid en aantoonbaarheid van de faalkans van de op te leveren software.

Rijkswaterstaat hecht grote waarde aan de mening van marktpartijen en heeft hen daarom vroegtijdig en actief betrokken via deze sectordialoog. Om een substantieel gesprek te kunnen aangaan gebeurde dit aan de hand van een eerste voorzet van de richtlijn softwarebetrouwbaarheid 0.8.

Doelstellingen Sectordialoog Softwarebetrouwbaarheid

- a) inzicht te verkrijgen in de reële randvoorwaarden waaronder het aspect softwarebetrouwbaarheid van een project kan worden uitgevoerd;
- b) input te vergaren ten behoeve van eisen aan aanbestedingen waar softwarebetrouwbaarheid een onderdeel van uit maakt;
- c) de markt in een vroeg stadium bij het project te betrekken om de mogelijkheid te hebben om de richtlijn zo goed mogelijk af te kunnen stemmen op de marktsituatie;
- d) inzicht te verkrijgen in de mate van uitdagingen die verschillende leveranciers beleven met betrekking tot software betrouwbaarheid en faalkans tijdens ontwikkeling, exploitatie en verwerving van gerelateerde opdrachten;
- e) inzicht te verkrijgen in bestaande oplossingen en aanpakken specifiek gericht op software betrouwbaarheid en software faalkans bij verschillende leveranciers in de sector;
- f) zicht te krijgen op de mate van kennis in de markt;
- g) een indruk te krijgen in hoeverre de markt in staat is om aan de eisen rondom software betrouwbaarheid te voldoen.

Rijkswaterstaat heeft hiervoor via diverse kanalen, onder andere via de gangbare aanbestedingsplatformen en brancheverenigingen, haar intentie kenbaar gemaakt en de sector uitgenodigd voor deze Sectordialoog Softwarebetrouwbaarheid.

Uit de geïnteresseerde partijen zijn een vijftal gekozen die het beste aan de criteria voldeden. Aan deze partijen werd de 0.8 versie van de richtlijn softwarebetrouwbaarheid ter voorbereiding verstrekt. De dialogen zijn gevoerd in de maanden April en Mei 2021 met vertegenwoordigers per gekozen partij en een viertal leden van het Rijkswaterstaat schrijfteam richtlijn softwarebetrouwbaarheid, en vervolgens tot dit rapport verwerkt.



De input die op deze manier is verzameld, wordt door het schrijfteam van de Richtlijn Softwarebetrouwbaarheid gebruikt om te komen tot een definitieve eerste versie.

Wij willen expliciet alle partijen die met ons mee willen en wilden denken danken voor de grote belangstelling, de open en productieve houding, en de ingebrachte kennis en ervaring.



2 Managementsamenvatting

Rijkswaterstaat stelt een richtlijn softwarebetrouwbaarheid op. Deze richtlijn moet Rijkswaterstaat en leveranciers in staat stellen om uniformer en beter met het onderwerp softwarefaalkans¹ en softwarebetrouwbaarheid om te gaan.

In dit kader zijn er aan de hand van de 0.8 conceptversie van de richtlijn softwarebetrouwbaarheid 4 dialogen gevoerd met geselecteerde marktpartijen.

Deze dialogen hebben tot het inzicht geleid dat de versie 0.8 van de richtlijn goed wordt ontvangen. Rijkswaterstaat presenteert een actuele en complete 'Body of Knowledge'. De 0.8 versie is hiermee een stabiele basis voor de definitieve versie.

De deelnemers hebben onafhankelijk van elkaar een aantal vergelijkbare opmerkingen gemaakt voor verfijning en verbetering. Daarnaast zijn vanuit de verschillende achtergronden en invalshoeken waardevolle opmerkingen geplaatst.

Het schrijfteam van de richtlijn softwarebetrouwbaarheid zal alle opmerkingen wegen en keuzes maken over de verwerking in de richtlijn softwarebetrouwbaarheid 1.0.

3 Leeswijzer

Als eerste hoofdstuk worden terugkerende onderwerpen apart opgenoemd.

In de volgende hoofdstukken worden achtereenvolgend de in het kader van de richtlijn softwarebetrouwbaarheid relevante opbrengsten van vier sectordialogen als destillaat weergegeven. De lezer zal vaststellen dat deze elkaar deels tegen kunnen spreken, er heeft bewust geen redactie op inhoud plaatsgevonden voor dit rapport.

De bijlage is op verzoek beschikbaar en bestaat uit de 0.8 versie van de richtlijn, die ook ter voorbereiding op de dialogen beschikbaar werd gemaakt aan de deelnemers.

De onverkorte dialoogverslagen zijn door de partijen ingezien en becommentarieerd. Deze zijn voor intern gebruik binnen het Rijkswaterstaat schrijfteam 'richtlijn softwarebetrouwbaarheid' beschikbaar om traceerbaarheid en volledigheid te borgen.

¹ Softwarefaalkans en softwarebetrouwbaarheid worden hier specifiek bedoeld in de definitie zoals door TOPAAS gehanteerd. Niet te verwarren met begrip 'Reliability' uit de ISO 25010.



4 Terugkerende onderwerpen

Alhoewel elk dialoog telkens andere inzichten heeft opgeleverd zijn er ook een aantal thema's die in drie of meer gesprekken naar voren zijn gekomen. Deze zijn opgenomen in de paragrafen in dit hoofdstuk

4.1 Versie 0.8 wordt goed ontvangen

De 0.8 versie van de richtlijn softwarebetrouwbaarheid geeft een vrijwel compleet, gedetailleerd en actueel inzicht in het onderwerp software betrouwbaarheid en software faalkans in relatie tot systems engineering en de software life cycle.

4.2 Geef nog meer how-to informatie

De beschrijving is compleet. Voor degene die moet implementeren zouden meer how-to aanwijzingen gegeven mogen worden. Bijvoorbeeld hoe configuratie- en wijzigingsbeheer ingericht moet worden, of hoe traceerbaarheid geborgd moet worden.

4.3 Deel het stuk op in kwaliteits-, opdrachtgevend- en audit onderdelen

De richtlijn omvat nu stukken voor verschillende doelgroepen. Overweeg als schrijfteam om het stuk per doelgroep in te delen, of zelfs aparte delen te maken per doelgroep.

4.4 Voeg toe wat bij goed opdrachtgeverschap hoort

Aangedragen wordt het idee om een deel te schrijven voor de aanbestedende en opdrachtgevende rollen binnen Rijkswaterstaat.

4.5 Integreer Cybersecurity

Software faalkans en software betrouwbaarheid worden niet in samenhang met cybersecurity gezet. De sector stelt dat deze twee niet apart van elkaar gehanteerd moeten worden en ziet graag een integratie van deze twee onderwerpen.

4.6 Kwaliteit van de mensen maakt de kwaliteit van de software

In elk gesprek komt naar voren dat voor een groot deel de kwaliteit van betrokkenen bij de software in de ruime zin als ook de kwaliteit van de interacties tussen de verschillende betrokkenen het resultaat bepalen.

4.7 Maak het aanbesteden 'softwarebetrouwbaarheid vriendelijker'

Aanbestedingen en EMVI criteria hebben de eigenschap dat de softwarebetrouwbaarheid minder zwaar weegt dan andere parameters waardoor, als softwarebetrouwbaarheid het doel is, deze onbedoeld onder druk komt te staan qua prioriteit.



4.8 Bouw kalibratiemomenten in het proces in

Aannames over de bedoeling van eisen gerelateerd aan softwarebetrouwbaarheid, de interpretatie van de IEC 61508, de wijze van realiseren spelen over en weer tussen opdrachtgever en opdrachtnemers als ook onderaannemers.

Investeer expliciet tijd in het kalibreren van de vraag achter de vraag en de beoogde en gerealiseerde wijze van daaraan invulling geven.

4.9 Rijkswaterstaat vormt een kennis speerpunt in de internationale markt

Het bepalen, meten en werken naar een specifieke orde van grootte van softwarefaalkans is een vak apart. Rijkswaterstaat en TOPAAS worden nationaal en internationaal als toonaangevend waargenomen op dit gebied.

Dit betekent dat Rijkswaterstaat een bijzondere rol toe zou kunnen of moeten komen in dit speelveld van kennisontwikkeling, kennisborging en toepassing.



5 Dialoog 1

5.1 Leesbaarheid en bruikbaarheid

5.1.1 Korter en gericht

Het stuk is waardevol, inhoudelijk sterk, maar te omvangrijk. Niet voor elke doelgroep is elk hoofdstuk even relevant. Mensen gunnen zich de tijd niet om dit door te lezen. Het is hele interessante informatie, het is meer een Body of Knowledge document, alles wordt wel geraakt. Overweeg om

- het gedeelte voor aanbestedingen voor Rijkswaterstaat intern beschikbaar te maken in een apart stuk;
- één stuk te richten op wat opdrachtnemer in zijn kwaliteitssysteem moet borgen voor ontwikkeling en beheer, met extra aandacht voor de QA manager rol;
- en één stuk hoe daarop moet worden geaudit;
- de tekst in te korten waar het kan, voor voorbeelden naar een bijlage te verwijzen;
- een stuk toevoegen, specifiek voor Rijkswaterstaat als opdrachtgever, dat mist nu.

5.1.2 Prioriteiten aangeven

Probeer prioriteiten aan te geven, in een soort MoSCoW waardering, misschien met symbolen naast de betreffende teksten.

5.1.3 Illustreer

Maak meer gebruik van illustraties. Geef via illustraties de samenhang tussen verschillende onderdelen aan.

5.2 Inhoudelijk

5.2.1 V-Model prima. Waterval voorschrijven niet nodig

Het V-Model is passend omdat het de verschillende disciplines weergeeft die betrokken zijn en de stukken/transities van probleem- naar oplossing goed beschrijft.

- Het is niet nodig om dit ook als waterval proces af te dwingen. Laat dit over aan de opdrachtnemer in afstemming. Wij zien waterval en iteratieve methoden met goed succes toegepast worden;
- Ga dan ook meer schrijven over Agile/Iteratief en hoe de software betrouwbaarheid daarin te borgen;
- Beschrijf de lifecycle voor beheer meer anticiperend. Dit moet in het instandhoudingsplan worden opgenomen, beschrijf hoe. Software kun je niet 10 jaar hetzelfde houden.

5.2.2 ISO25010

Overweeg voor betere aansluiting aan de markt door gebruik te maken van de ISO25010.



5.2.3 Integreer cyberveiligheid

Cybersecurity, safety en betrouwbaarheid kunnen niet los worden gezien. Laat de risicoanalyse integraal zijn. Neem dit ook mee in de beheerfase, met monitoring, patch beleid, wijzigingsbeheer.

Correctieve maatregelen verdienen hier meer nadruk.

5.2.4 Ga software als onderdeel van COTS betrekken

Software in een ventilatiesysteem hoort ook onderhouden te worden. Rijkswaterstaat beschouwt dit nu niet mee. Trek het onderwerp binnen de richtlijn.

Heb ook aandacht voor 'hardening' van componenten.

5.2.5 Sturen op kwaliteitssysteem en externe audits

Rijkswaterstaat mag best verder sturen op het kwaliteitssysteem van opdrachtnemer. En zie dit los van contractbeheersing met bijzondere aandacht voor onderaannemer constructies. Systeemgerichte contractbeheersing werkt erg goed.

Het door opdrachtnemer zelf regelen van een externe audit, in overleg met Rijkswaterstaat, is prima.

'Examengericht leren' komt voor en is een zaak die zowel bij opdrachtnemer als ook bij opdrachtgever speelt. Want ook opdrachtgever is soms gericht op het 'af kunnen vinken' van een opdracht.

5.2.6 Testen

Geef aandacht aan test driven development (TDD) in het stuk.

Testaandacht ook voor bouwblokken. Opnieuw testen bij hergebruik.

5.3 Samen leren

Rijkswaterstaat staat aan frontlinie van kunnen en weten. Het onderwerp is hoogst relevant, en de relevantie blijft alleen maar toenemen.

Het is een goed initiatief van Rijkswaterstaat om deze richtlijn op te stellen. Trek het leren breder, vergelijkbaar met cybersecurity.

5.3.1 Neem de lead

Rijkswaterstaat is van alle partijen het verst als het gaat om het sturen op en aantonen van softwarebetrouwbaarheid. Hierdoor is Rijkswaterstaat dé partij om het onderwerp breder te borgen.

- bouw een community rond softwarebetrouwbaarheid op;
- overweeg om de richtlijn als open source te positioneren;
- vertaal TOPAAS en de richtlijn ook naar het Engels.

5.4 Aanbesteden

5.4.1 Werk samen met opdrachtnemer aan de eisenspecificatie

Zorg dat je de dialoog met elkaar ook opzoekt om te komen tot smart gedefinieerde eisen. Dat gaat vaak tijdens de aanbesteding zelf onvoldoende.



5.4.2 Expertise

Zorg voor voldoende inhoudelijke kennis en ervaring binnen Rijkswaterstaat om de opdrachtnemer te kunnen spiegelen. Iemand schrijft nu iets op zonder te beseffen wat dat nou betekent in het vervolg. Je zult wel een 'demand organisatie' moeten hebben die daartoe instaat is en kan sturen en meer de diepte in met een ON die de diepte ingaat en ook vragen stelt.

Stel eisen aan Rijkswaterstaat hierin.

5.4.3 Relevantie zoeken en niet vast zitten aan één aanbestedingsvorm

Het stapelen van standaarden in ruwe vorm en het aan de opdrachtnemer overlaten van het op maat maken en ontdebellen is niet doeltreffend. Het aanhalen van slechts een aanbestedingsvorm kan als een beperking worden ervaren.

- De stapeling van standaarden terugbrengen tot een aantal 'key controls' en het verwerken van de stapeling niet overlaten aan de opdrachtnemer;
- Beschrijf ook alternatieve contract- en aanbestedingsvormen.



6 Dialoog 2

6.1 V-Model ok.

6.1.1 Waterval relatie V-Model

Waterval of V-Model, maak duidelijk wat bedoeld wordt.

Is V-model bedoeld of Waterval? Want het staat bij projectmanagement. Voor het begrip: V-model biedt veel houvast. Ook voor dit onderwerp passend.

6.1.2 Stapeling staat beste oplossing in de weg

Als je normen hard afdwingt en daarop audit, staat dat de beste oplossing soms in de weg. Jullie willen eigenlijk J-STD-016 en V-Model, uiteindelijk hebben we toch een FO (Functioneel Ontwerp) gemaakt.

Heroverweeg J-STD, misschien obsoleet.

Cybersecurity moet er wel in, dat wordt nu gemist.

6.1.3 Haal tijdsdruk weg, zorg voor voldoende en tijdig inzetbare expertise

Hebben meegeschreven aan de System/Subsystem Specification (SSS), Rijkswaterstaat had zelf de regie. Wat lastig is en blijft door het hele project heen is dat het vaak onder tijdsdruk gebeurt. Je begint met het SSS al onder tijdsdruk. Dat wil nog eens lastig zijn met kwaliteit.

De tijdsdruk komt mede door de schaarste en inzetbaarheid van expertise bij Rijkswaterstaat.

Bij keringen zit je specifiek ook nog aan stormseizoenen, een keer een venster gemist betekent gelijk een jaar uitstel.

Ook besluitvorming duurt onnodig en onverwacht lang, zelfs voor Rijkswaterstaat begrippen.

Rijkswaterstaat is beperkt in het aantal mensen dat daadwerkelijk software ontwikkeling kan beoordelen.

6.1.4 Beperk je in overeenkomsten tot de essentie

We hebben de overeenkomst maar dan ca. 40 bijlagen. Een aantal zitten erbij die zijn heel ouderwets. Onleesbaar kopie van kopie de MIL standaard bijvoorbeeld. Ook lastig in te vullen. De MIL schrijft voor hoe de CDR eruit moet zien, maar Rijkswaterstaat kijkt er dan toch anders tegen aan. We dachten aan twee weken werk, Rijkswaterstaat aan twee uur.

Heel veel druk ontstaat bij het afdwingen van heel veel documenten die er niet toe doen. Het gaat ook meer om procesproducten, en niet engineering producten of engineering proces producten.

Weglaten kan niet, de auditor kijkt er voor Rijkswaterstaat namelijk wel naar vanuit procesoptiek.



6.1.5 Opdrachtnemer extern laten auditen: prima

Je kunt het auditen ook bij de opdrachtnemer neerleggen. Je kunt ook eisen om een specifieke audit score te halen. Heeft allerlei voordelen, het stuurt ook het proces naar mijlpalen toe harder dan zonder audit. Ook voor de opdrachtnemer.

6.1.6 Audit met de juiste competenties op software betrouwbaarheid (en vermijd placebo's)

Er is een verschil tussen bijvoorbeeld Prorail en Rijkswaterstaat. Bij Prorail gaat het erg over de inhoud van het tot stand komen van de software. Bij Rijkswaterstaat gaat het meer om het proces: 'Houden jullie ook maandelijks overleg, en hebben jullie daar een verslag van'. Bij Prorail meer over: 'Hoe weet je dat je ontwerp klopt en dat de software overeen komt met het ontwerp.'

6.1.7 Aanbesteden: Dilemma dat de meterprijs meeweegt

Probeer voor de kwaliteit van de software aanbieder tot een soort Michelin Ster te komen.

6.1.8 Investeer in de samenwerking

Kwaliteit van de samenwerking: Als die goed verloopt heeft dat een goed gevolg voor alle aspecten. Betrouwbaarheid komt uit het hele team.

Systeemgerichte contractbeheersing is soms stroef met discussies binnen/buiten scope, meerwerk. Dat betekent een negatieve uitwerking op de opdracht.

Wat niet werkt is het contract letterlijk en op afstand volgen. En niet elke afwijking moet een VTW worden, dat levert te veel rompslomp op.

6.1.9 MDD en Centraliseer de requirements repository

Wijd ook een stuk aan model driven development, beheer van de tooling. Het liefste wil je een centrale repository voor requirements en andere artefacten waar je in kunt loggen.

6.1.10 Design for testability

Dit mag meer aandacht krijgen in het hoofdstuk over testen: Test Driven Development (TDD) en 'design for testability'.



7 Dialoog 3

7.1 Volledig

Allereerst complimenten voor de volledigheid, raakt werkveld prima. Software kwaliteit is echt belangrijk.

7.2 Aanbesteden

7.2.1 Software apart.

Overweeg om altijd software apart aan te besteden van de objecten. Bij 10ct per strekkende meter beton verschillen de kwaliteitscriteria voor IA snel in de EMVI criteria.

Tevens kun je zo ook expliciet voor een goede technologiepartner kiezen, en verdwijnt het niet in onderaannemerschap bij de gegunde partij.

Beschrijf wie onder welke omstandigheden de rol systeemintegrator heeft. De rol kan feitelijk schuiven door deze ingreep.

7.2.2 Lifecycle in de EMVI criteria

Nog een ander aspect, dat is ook al goed verwoord in de IA strategie, dat je naar de hele lifecycle /TCO kijkt. Dat doet Rijkswaterstaat goed bij keringen en tunnels. Ook voor cybersecurity.

7.2.3 Kun je meer standaard oplossingen uitvragen

Bij de bruggen, volgens 2014 2015 onderzoek, kom je aan een groot portfolio verschillende oplossingen. Voor beheer en gebruik best wel een puzzel om functioneel congruent te zijn en op de zelfde manier beheer inrichten. Wel een uitdaging, maar wel minder bij bruggen en keringen.

Met name in beheer en onderhoud levert het behoorlijke schaalvoordelen op als je daar met universele standaard componenten kunt werken. Maar je trekt dan ook veel naar jezelf toe als Rijkswaterstaat.

7.2.4 Uitvragen ISO61508 heeft gewenste filterwerking

Ben verheugd om te zien dat je zwaar leunt op normen die er zijn, zoals de 61508. Ik zou geneigd zijn om dat in de EMVI criteria uitvragen of de aanbieder ervaring ermee heeft. Daarmee kun je de 'elektroboer op de hoek' de pas afsnijden.

7.2.5 SRA fase in aanbesteding meenemen

Rijkswaterstaat heeft de neiging om standaarden uit te vragen, en aannemers de neiging om deze zomaar over te nemen af te vinken. Dit is niet doeltreffend.

Belangrijk is: Niet klakkeloos opstellen en volgen van eisen. Dialoog voeren en definitief bestendigen dat er daadwerkelijk de juiste eisen worden gesteld en op welke manier er vervolgens aan wordt voldaan.



7.3 Na aanbesteding

7.3.1 Dubbelcheck en kalibreren van de opdracht in SRA fase

Om zeker te zijn dat je elkaar goed begrijpt zou je na selectie in overleg over de eisen moeten treden en met opdrachtgever en opdrachtnemer / inschrijver goed na gaan of je ook dezelfde visie hebt op de eisen en de manier van invullen.

Kijk in een open sfeer naar de vraag achter de eis en kijk ook eventueel naar een betere oplossing.

7.3.2 Verdieping aannemer in bestaande situatie belangrijk: Veldinventarisatie

Brownfield. Ik heb de ervaring met MOBZ, geen fijne ervaring, maar van groot belang dat de gegunde partij zich goed verdiept in de bestaande situatie.

In 2007/2008 kwam niet voldoende uit de verf dat de partij met de laarzen aan daar naartoe is gegaan en gekeken heeft hoe de situatie echt is. In het proces ook benoemen en prominenter maken dat de aannemer de inventarisatie van de installatie maakt. Bij Rijkswaterstaat zijn de areaalgegevens ook niet echt op orde.

7.4 Ontwikkeling en beheer (hfdst. 6)

7.4.1 SIG tools – meer ruimte geven

Kan wel helpen maar er zijn bottlenecks:

- Niet goed passend op PLC programmatuur;
- Vaak in de knel met genereren en standaardiseren;
- Kan niet omgaan met bibliotheken.

7.5 Testen(hfdst.7)

7.5.1 Traceerbaarheid naar de testcases

Traceerbaarheid staat nu in de tekst verwijzend naar testplannen, maar het zou moeten zijn: naar testcases. Of Testscripts.

7.5.2 ISTQB en TMAP

ISTQB en TMAP kunnen iets beter worden aangehaald.

7.5.3 Simulaties opnemen

Ook aandacht hebben voor simulatie van de proceskant.

7.5.4 Lever ook de complete ontwikkel- en teststraat op

Overgang naar Beheer. Het zou fraai zijn dat je ook de regressietesten mede overdraagt. Plus de hele ontwikkelstraat en tooling.

7.6 Wijzigingsbeheer (hfdst.8)

7.6.1 Lifecycle management voor standaard bouwblokken

Standaard blokken. Hier gaat het om één asset, maar wat doe je met standaard componenten en bibliotheken? Beschrijf taken die hierbij horen.



8 Dialoog 4

8.1 Leesbaarheid

De tekst is goed volgen, herkenbare thematiek, herleidbaar naar dagelijkse praktijk. Goed leesbaar, en goed dat er een richtlijn komt.

8.2 Gehanteerde normen

8.2.1 V-Model /waterval

[geïnterpreteerd als waterval model] Nog geen alternatieve aanpak gevonden. Je moet bijna naar het V-model gaan omdat je je fasering en traceability wilt regelen.

Wat goed is aan de agile aanpak is een hoge mate aan automatisering. Alleen ga je in net iets minder detail bij het ontwerp aan de voorkant. Dat zijn voordelen.

8.2.2 61508 is niet gelijk aan softwarebetrouwbaarheid

61508 is geen vervanging voor softwarebetrouwbaarheid, wordt heel regelmatig aangehaald. 61508 heel goed, heel uitgebreid, maar als je hem toe gaat passen heb je het altijd over een mechatronisch systeem. Altijd hard- én software. Je kunt ze niet los van elkaar beschouwen, daar zit de paradox dan ook.

Misschien aansluiten aan 9001, 2700x, 25010, 12207. DOE-178.

8.2.3 Integreer cybersecurity

Integreer cybersecurity in het stuk. Cybersecurity kan eigenlijk niet los worden gezien van softwarebetrouwbaarheid, ook de 2700x speelt een rol.

8.2.4 Compartimenteer

Maak duidelijk op welke systeemonderdelen de richtlijn in welke mate van toepassing is, voorkom dat je alles over een kan scheert.

8.3 Safety critical vs. mission critical

8.3.1 Safety critical systeemontwikkeling vergt ervaring

Niet elke leverancier komt met safety critical systeemontwikkeling in aanraking. Het is een apart vak. Maak misschien meer onderscheid tussen missie-kritiek en safety-kritiek in de aanbesteding en uitvoering.

8.4 Samenwerking met opdrachtnemers

8.4.1 Vaste afstem- en kalibratie momenten benoemen

Synchroniseren tussen opdrachtgever en opdrachtnemer belangrijk op de interpretatie van de 61508. Na gunning met gekozen leverancier nog een keer zitten en doorlopen: Hoe hebben jullie nu geïnterpreteerd. Kun je niet tijdens de aanbesteding doen, maar daarna wel. Om aan beide kanten de verwachtingen nog een keer bijstellen.



8.4.2 Impact op de organisatie

We zouden eerst een safety persoon aan moeten stellen en bewustzijn moeten kweken. Betrouwbaarheid haal je uit je proces. Als je hoger op de ladder gaat ga je testen uitbreiden, testcoverage is bijvoorbeeld beperkt. Andere tooling, andere kennis nodig.

8.4.3 Meer concrete handvatten voor implementatie

Ook meer handvatten voor het op maat maken van de ontwikkel- en beheeromgeving in het licht van Softwarebetrouwbaarheid gevraagd. Maar wordt ook niet te specifiek op de oplossing.

8.5 Overige

8.5.1 Tooling

Gebruik van de hele ontwikkel- en beheerstraat tooling meenemen, niet alleen de gecertificeerde compiler. Laat een degelijke omgeving neerzetten voor alle disciplines zowel tijdens ontwikkeling als ook tijdens beheer.

8.5.2 Proven technology voor safety-critical toepassingen

Ik merk dat de druk toeneemt om de automatisering met soft PLC's en dergelijke aan te pakken. Blijf bij goed compartimenteren en gebruiken van de juiste bewezen technieken voor safety critical systems.



9 Bijlage: 0.8 versie

Deze bijlage is op te vragen via de kaderbeheerder TOPAAS bij Rijkswaterstaat.