Adviescollege ICT-toetsing

> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Infrastructuur en Waterstaat
t.a.v. de minister, de heer M.G.J. Harbers
Postbus 20904
2500 EX Den Haag

Adviescollege ICT-toetsing

Muzenstraat 95
Den Haag
Postbus 16292
2500 BG Den Haag
adviescollegeicttoetsing.nl

Contactpersoon
info@adviescollegeicttoetsing.nl

Kenmerk
2023-0000435345

Uw kenmerk
RWS 2022/15733

Datum	20 juli 2023
Betreft	Definitief BIT-advies project BEST2DO

Geachte heer Harbers,

U heeft het Adviescollege ICT-toetsing verzocht een onderzoek uit te voeren naar het project BEST2DO van Rijkswaterstaat (RWS). De opdrachtgever van het project is de hoofdingenieur-directeur van de regio West-Nederland Zuid. Het advies kan als volgt worden samengevat:

Het project BEST2DO beoogt de betrouwbaarheid van de besturingssystemen van de Hartelkering en van de locomobiel van de Maeslantkering voor een periode van ongeveer vijftien jaar te borgen. Het project wil hiervoor de software en hardware van beide besturingssystemen vervangen. De kosten daarvan, inclusief vijftien jaar beheer en onderhoud, zijn gebudgetteerd op ruim 32 miljoen euro.

Conclusie
De belangrijkste conclusie uit de toets is dat wij de gekozen aanpak om de betrouwbaarheid van de besturingssystemen te waarborgen onnodig risicovol vinden:

A. De gekozen oplossingsrichting dient onvoldoende het belang van betrouwbare keringen.
B. Er is onvoldoende inhoudelijke basis voor nieuwbouw.
C. De opzet van de aanbesteding biedt weinig zekerheid dat het gewenste resultaat wordt bereikt.

Advies
Gezien de grote veiligheidsbelangen van deze keringen adviseren wij om in de aanpak van BEST2DO de betrouwbaarheid centraal te stellen:

1. Handhaaf de bestaande software, tenzij de betrouwbaarheid niet voldoende blijkt te zijn.
2. Verwijder de discrepanties tussen ontwerp, software en testen.

Hieronder vindt u eerst een korte beschrijving van het project. Daarna werken we bovenstaande conclusie en adviezen nader uit. Wij concentreren ons hierbij op de belangrijkste risico's van het project. In de bijlage vindt u de details van het project.

KORTE OMSCHRIJVING VAN HET PROJECT BEST2DO

De Maeslant- en de Hartelkering zijn twee stormvloedkeringen die in 1997 integraal zijn opgeleverd: de civiele constructie inclusief de systemen voor besturing en bediening. Samen vormen ze de Europoortkering en beschermen ze ruim twee miljoen Nederlanders en het achterland. De Waterwet stelt eisen aan betrouwbaarheid en beschikbaarheid van de keringen. De wettelijke faalkans bij sluiting van de Hartelkering is 1:10 (dat wil zeggen: het sluiten van de kering mag maximaal 1 op de 10 keer falen) en bij de Maeslantkering 1:100.

De twee keringen worden aangestuurd door het Beslis en Ondersteunend Systeem (BOS). Het BOS voorspelt de waterstand op basis van diverse data, zoals windsnelheden en windrichting. Als de voorspelde waterstand in Rotterdam boven 3 meter NAP of in Dordrecht 2,90 meter boven NAP dreigt te komen, besluit het BOS tot sluiting van de kering. Ook kunnen beide keringen lokaal worden bediend, mocht dat nodig zijn. De keringen worden maandelijks getest en jaarlijks vindt er een functioneringssluiting plaats.

De twee systemen die door het BOS worden aangestuurd zijn het besturingssysteem van de Hartelkering (BESH) en het overkoepelende besturingssysteem van de Maeslantkering (BESW). Dit laatste systeem stuurt op zijn beurt weer het bedienings- en besturingssysteem (BESL) van de aandrijving (locomobiel) van de Maeslantkering aan; deze moet de twee sectordeuren aan beide zijden van de Nieuwe Waterweg uit- en invaren.

In 2011 is de hardware van BESH en BESL vervangen en zijn onderdelen van de software gemoderniseerd. Deze opdracht is destijds onderhands aan de huidige leveranciers gegund. Binnen Rijkswaterstaat is destijds de voorwaarde gesteld dat een volgende vervanging volledig Europees zou worden aanbesteed en dat er, om dit mogelijk te maken, bij gebrek aan voldoende documentatie een functiereconstructie zou worden opgeleverd die een gelijk speelveld voor marktpartijen creëert.

Rijkswaterstaat heeft geconstateerd dat de hardware van BESH en BESL over enkele jaren het einde van de technische levensduur bereikt en vervangen moet worden. RWS is van mening dat hiermee ook de software einde levensduur nadert, omdat de firmware verandert (door introductie van nieuwe hardware) en vernieuwde cybersecurityeisen in de software verwerkt moeten worden. Daarom is het project BEST2DO gestart met als gesteld doel het borgen van de betrouwbaarheid van de besturingssystemen BESH en BESL voor een periode van ongeveer vijftien jaar. Daarbij mag de faalkans van de kering niet negatief beïnvloed worden.

BEST2DO wil via een aanbesteding zowel de hardware als de software geheel vervangen. Uitgangspunt daarbij is dat de nieuwe software de komende vijftien jaar over dezelfde functionaliteit beschikt als de huidige.

De aanbesteding, op basis van een concurrentiegerichte dialoog, is medio 2022 gestart en bevindt zich nu in de laatste fase voor de gunning; het aantal partijen wordt teruggebracht van drie naar één. De planning is dat de realisatie en implementatie van BESH en BESL in respectievelijk 2026 en 2027 gereed zijn.

CONCLUSIE: AANPAK ONNODIG RISICOVOL OM BETROUWBAARHEID KERINGEN TE WAARBORGEN

Gezien het grote veiligheidsbelang van de Maeslant- en de Hartelkering begrijpen wij dat Rijkswaterstaat de betrouwbaarheid van de besturingssystemen BESH en BESL voor de komende vijftien jaar wil borgen. Wij constateren een aantal positieve punten, zoals een hoge betrokkenheid van het keringenteam en de inspanningen om het testen te automatiseren. Wij ondersteunen de ambitie van RWS om de testomgeving door te ontwikkelen tot een volwaardige simulatieomgeving. Met het oog op de betrouwbaarheid vinden we de gekozen aanpak van BEST2DO echter onnodig risicovol. Hieronder gaan we in op de redenen daarvoor.

A. Gekozen oplossingsrichting dient onvoldoende belang betrouwbare keringen

De gekozen oplossingsrichting bij de start van BEST2DO is sterk gestuurd vanuit het standaard inkoopkader van RWS. Het belang van de betrouwbaarheid van deze specifieke keringen is minder prominent meegewogen. Als gevolg hiervan maakte BEST2DO twee keuzes waar wij vanuit het perspectief van betrouwbaarheid kritisch over zijn:

- Het *scenario* waarin de huidige software die zich heeft bewezen wordt hergebruikt, is niet onderzocht. Terwijl dit scenario juist in het belang van betrouwbaarheid voor de hand ligt:
  - Uit ons onderzoek komt geen enkele aanwijzing voor een technische noodzaak tot vervanging van de bestaande software. De ervaringen van meerdere betrokkenen zowel binnen en buiten het project als de organisatie zijn positief als het gaat om functionaliteit en betrouwbaarheid. Onze analyse van de storingsoverzichten en deels beschikbare logfiles[1] onderbouwt dit. Van de ongeveer 2.100 incidenten over de afgelopen twaalf jaar in de keringen is er geen enkel incident terug te voeren op fouten in de huidige software of falen hiervan. Van nieuwe software moet de betrouwbaarheid zich eerst nog bewijzen. Zeker in de context van deze keringen, waar zeer betrouwbare software is vereist, vinden wij de vervanging van alleen de hardware een veel minder risicovol scenario. Van de huidige software kan worden aangenomen dat in de afgelopen 25 jaar eventuele residuele fouten zijn gevonden en opgelost. Bovendien zijn onderdelen ervan in 2011 gemoderniseerd zonder enig incident.
  - Hergebruik van de bestaande software is mogelijk, zelfs door andere leveranciers dan de huidige. Dit marktpotentieel wordt nu niet benut. Er zijn partijen gespecialiseerd in het onderhouden, beheren, verbeteren, migreren en herdocumenteren van hard- en software van bestaande industriële automatisering. Daarbij moet uiteraard wel worden voldaan aan de gestelde betrouwbaarheidseisen voor deze systemen.
- De *scope* van BEST2DO, waarbij twee verschillende systemen van twee unieke objecten die sterk van elkaar verschillen in één opdracht worden vervangen, is – vanuit betrouwbaarheid gezien – geen voor de hand liggende keuze:

[1] Het feit dat de logfiles slechts voor een klein deel beschikbaar gemaakt konden worden is overigens een risico voor de beheersing van de systemen, omdat deze informatie nodig is voor empirische analyses van de betrouwbaarheid en beschikbaarheid van de keringen.

- De bundeling van BESH en BESL is met name ingegeven door de aantrekkelijkheid van de opdracht voor marktpartijen door de schaalgrootte. De keringen zijn echter dusdanig verschillend opgebouwd dat een bundeling met het oog op betrouwbaarheid geen voor de hand liggende keuze is. De combinatie van BESL en BESW had met het oog op de betrouwbaarheid meer voor de hand gelegen.
- De gekozen scope leidt tot risico's als gevolg van een nieuw raakvlak waarover verschillende leveranciers moeten afstemmen. Op de Maeslantkering ontstaat namelijk zo'n nieuw raakvlak tussen het beoogde nieuwe besturingssysteem BESL en de huidige hydraulische systemen. In de huidige situatie zijn deze systemen initieel opgeleverd als één geheel en hebben ze nauwe interactie met elkaar: het geheel is meer dan de som der delen. Een nieuwe leverancier moet daarom nauw met de huidige samenwerken met als gevolg weinig ontwerpvrijheid, het risico op communicatiestoringen en het trager doorvoeren van beheermaatregelen.

B. Onvoldoende inhoudelijke basis voor nieuwbouw

Als RWS toch vasthoudt aan nieuwbouw van de software, zien we in de huidige situatie risico's. De nu voorgenomen nieuwbouw is namelijk gebaseerd op onvoldoende uitgewerkte eisen, functioneel ontwerp en functiereconstructie, wat een belangrijk faalrisico van projecten is. Zeker bij nieuwbouw van systemen die een zeer hoge softwarebetrouwbaarheid vereisen, zoals hier het geval is. Wij lichten dit hieronder nader toe:

- De eisen[2] rond betrouwbaarheid en cybersecurity voor de nieuwe software die in de aanbesteding zijn verstrekt, zijn schetsmatig en van onvoldoende kwaliteit (specifiek en meetbaar). Hiermee vormen ze onvoldoende basis voor het integraal ontwerp, de realisatie en verificatie & validatie. RWS loopt hiermee het risico dat het niet de juiste partij selecteert, de eisen verkeerd of onvoldoende ingevuld worden en dat het later onvoldoende kan sturen op functionaliteit, betrouwbaarheid en cyberveiligheid.
- Het functioneel ontwerp biedt onvoldoende basis voor een leverancier om een technisch ontwerp te kunnen maken. De functionele beschrijvingen voor de nieuwe BESH en BESL zijn ontoereikend en sluiten niet volledig aan op de operationele werking van de twee huidige besturingssystemen. Hiermee ontstaat het risico dat de nieuw te bouwen software niet doet wat het moet doen en ook niet voldoet aan eisen ten aanzien van betrouwbaarheid, beschikbaarheid en cyberveiligheid.
- Er staan issues open wat betreft de functiereconstructie:
  - Wij zien een groot risico in het feit dat de nieuwe leverancier later samen met RWS, beiden met beperkte kennis van de functionaliteit en van de huidige software, niet alle openstaande punten uit de functiereconstructie kan oplossen. Voor BESH en BESL zijn er respectievelijk nog 15 en 77 uitzoekpunten die op basis van de documentatie uit 2011 niet kunnen worden opgelost. Daarvoor is de huidige softwarecode nodig. RWS heeft de intentie de bestaande software van BESH en BESL beschikbaar te stellen aan de nieuwe leverancier. Voor BESL is het echter na ruim een jaar nog altijd onduidelijk welke delen van de software RWS beschikbaar mag stellen aan de nieuwe leverancier.
  - Het risico bestaat dat de nieuwe software niet alleen afwijkt in functionaliteit en betrouwbaarheid maar dat dat ook niet waargenomen

[2] Zoals beschreven in de Klanteisspecificatie (KES) als onderdeel van de aanbestedingsstukken.

wordt in de testomgeving, omdat die er een eigen werkelijkheid op nahoudt. Van de automatische testomgeving (ATE) hebben wij namelijk vastgesteld dat die niet is gebaseerd op de reconstructie uit het voorbereidende project 'Functie reconstructie tot Uitvoering' (FRUIT). Dus er bestaan drie verschillende werkelijkheden: de huidige software, de functiereconstructie en de (nieuwe) testomgeving ATE.

C. Opzet aanbesteding biedt weinig zekerheid dat gewenst resultaat wordt bereikt

RWS heeft gekozen om inhoudelijke en contractuele keuzes die normaliter worden gemaakt gedurende een concurrentiegerichte dialoog, in te vullen na de gunning. RWS past hiervoor na de gunning een tweefasenproces toe, waarin de geselecteerde leverancier in de eerste fase, op basis van een proof-of-concept en documentatie, aantoont dat de hardware en de software voldoen aan de vereiste faalkansen. De tweede fase bestaat uit de daadwerkelijke realisatie van de software en het onderhoud. RWS beoogt hiermee het risico te verkleinen dat pas in een laat stadium blijkt dat een geselecteerde leverancier niet voldoet aan de eisen. Wij denken echter dat dit risico niet wordt verkleind, om de volgende redenen:

- De inhoudelijke uitwerking van het ontwerp en het softwareontwikkelproces vindt plaats in fase 1 na de gunning. De gunning zelf vindt daardoor slechts plaats op basis van procesaspecten (bijvoorbeeld het samenwerkingsproces) en faalkansberekeningen die alleen zijn gebaseerd op de voorgestelde hardware-configuratie en een globaal plan om te komen tot een softwareontwikkelplan. Indien in fase 1 blijkt dat een leverancier niet voldoet, zal RWS opnieuw een tweefasenproces moeten doorlopen met een andere leverancier die 'in de wachtkamer' zit. Omdat de tijd ontbreekt voor een dergelijke tweede ronde ontstaat het risico dat RWS niet meer de mogelijkheid heeft om verder te gaan met de leverancier die in de wachtkamer zit.
- Er is voor gekozen om de contractuele voorwaarden te baseren op de 'Uniforme Administratieve Voorwaarden voor Geïntegreerde Contractvormen' (UAV-GC). Deze generieke set van voorwaarden biedt onvoldoende basis om duidelijke afspraken over het eigendoms- en gebruiksrecht te maken. Daarom zijn er RWS-brede aanvullende bepalingen opgesteld. Deze zijn echter niet eenduidig als het gaat om wat wel en niet specifiek voor RWS wordt vervaardigd. Over wat specifiek wordt vervaardigd wil RWS eigendomsrecht; voor niet specifiek wil RWS licenties afsluiten plus een regeling tot toegang tot deze onderdelen als de leverancier onverhoopt failliet gaat. Deze wensen worden pas na gunning besproken, en de kans bestaat dat die dan onvoldoende worden ingewilligd; een risico dat zich in de huidige situatie al heeft voorgedaan.

ADVIES: STEL BETROUWBAARHEID CENTRAAL IN AANPAK BEST2DO

Gezien het grote veiligheidsbelang van beide keringen adviseren wij om de aanpak van BEST2DO te wijzigen. Kies daarbij voor een aanpak die het belang van betrouwbare besturingssystemen en dus betrouwbare keringen centraal stelt.

1. Handhaaf bestaande software van BESH en BESL, tenzij de betrouwbaarheid niet voldoende blijkt te zijn

Uit ons onderzoek blijkt dat zowel betrokkenen van RWS als de huidige leveranciers positief zijn over de betrouwbaarheid van de huidige software. Ons verkennend onderzoek bevestigt dat de software niet aan het einde van de technische levensduur is. Daarom adviseren wij om te kiezen voor het scenario waarin de betrouwbaarheid van beide besturingssystemen het minste risico loopt. Concreet betekent dit dat alleen de hardware wordt vervangen en de bestaande software wordt gemigreerd en hergebruikt. Hoewel wij begrijpen dat het een ingrijpende beslissing is, is het toch verstandig dat RWS heeft besloten om de nu lopende aanbesteding te pauzeren. Het project kan met de volgende stappen eerst zekerheid krijgen over de betrouwbaarheid van de huidige software:

- Zorg dat de softwarecode van BESL binnen enkele maanden beschikbaar komt voor onderzoek en mogelijk hergebruik. Doe bij de huidige leverancier van BESL het formele verzoek tot verkrijging van het volledige intellectueel eigendom en/of de gebruiksrechten. Hecht eventuele issues op dat punt af door bijvoorbeeld licentieafspraken te maken.
- Zorg dat er aanvullende duidelijkheid komt over de betrouwbaarheid en cyberveiligheid van de huidige BESH- en BESL-systemen. Verzoek hiertoe de leveranciers alle defecten- en incidentenadministraties te leveren plus alle historische logfiles als basis voor empirische analyses van de betrouwbaarheid, beschikbaarheid en faalfrequentie over een zo lang mogelijke periode.
- Pas de scope van het project aan door voor BESH en BESL afzonderlijk de meest geëigende vervolgstap te kiezen:
    - Als uit de analyses blijkt dat de betrouwbaarheid met de huidige software voldoende is of met beperkte maatregelen bereikt kan worden, stop dan de huidige aanbesteding. Besteed alleen de voor de huidige software passende hardware- plus software-migratiewerkzaamheden aan, evenals het onderhoud en beheer van die hard- en software.
    - Als de betrouwbaarheid onvoldoende blijkt, zorg dan voor een gedegen basis voor nieuwbouw door de kwaliteit van de eisen en het functioneel ontwerp te verbeteren, een vernieuwde functiereconstructie uit te voeren en testscenario's uit te werken. Deze basis moet klaar zijn voordat een verdere aanbesteding van hard- en software kan plaatsvinden.

2. Verwijder discrepanties tussen ontwerp, software en testen

Zorg dat het ontwerp, de software en de bijbehorende testomgeving consistent zijn met elkaar en met de werking. Dit is een noodzakelijke maatregel voor een duurzaam correcte werking van de systemen en de beheersing daarvan. Meer in detail:

- Zorg dat het functioneel ontwerp volledig en consistent is met de feitelijke werking van BESH en BESL en met de uitgangspunten van de testomgeving ATE. Los alle onduidelijkheden voor BESH en BESL op die uit FRUIT naar voren zijn gekomen. Leg vast hoe de operationele werking van de bedienings- en besturingssystemen nu is en wat de aanvullende eisen zijn, inclusief de onderbouwing van de noodzakelijkheid van deze eisen en de effecten op betrouwbaarheid. Sluit ook de testplannen hierop aan.
- Maak de betrouwbaarheid van de besturing van de keringen meetbaar over de tijd (trendanalyses). Zorg voor inzicht in het operationele gedrag van de bedienings- en besturingssystemen op basis van defecten en/of incidentenadministraties en de loggegevens. Analyseer deze periodiek ten

behoeve van de betrouwbaarheid, preventief en correctief onderhoud en beheer van de gehele kering.
- Breid de testomgeving ATE uit tot een volwaardige simulatieomgeving, die overeenkomt met het functioneel en technisch ontwerp en de software, inclusief de mogelijkheden om uitzonderlijke foutmeldingen te kunnen simuleren.

***

Tot slot danken wij alle geïnterviewden voor hun medewerking. Wij hopen met dit advies een bijdrage te kunnen leveren aan de blijvende betrouwbare werking van de besturingssystemen en daarmee ook aan de betrouwbaarheid van de keringen.

Met de meeste hoogachting,
namens het Adviescollege ICT-toetsing,

w.g.

drs. H.J.A. van Osch
Voorzitter

w.g.

drs. S.J. van Amerongen
Secretaris-directeur

Bijlage

Informatie over project BEST2DO

Nr	Onderwerp	Toelichting
1.	Projectnaam	BEST2DO
2.	Opdrachtgever	Hoofdingenieur-directeur van de regio West-Nederland Zuid
3.	Startdatum project	December 2020
4.	Einddatum project	Maart 2028
5.	Type project	Vervanging
6.	Fase Project	Aanbestedingsfase
7.	Totaal budget	32,1 miljoen euro (dit betreft alleen de 'out-of-pocket' kosten van het project. Interne kosten worden door het project niet geregistreerd)
8.	Reeds uitgegeven per datum 1-6-2023	Onbekend.
9.	Doelstelling	De betrouwbaarheid borgen van de besturingssystemen van de Hartelkering en van de locomobiel van de Maeslantkering voor een periode van ongeveer vijftien jaar.
10.	Maatschappelijke/ beleidsdoelstelling	Bescherming van ruim 2 miljoen Nederlanders en het achterland bij een waterpeil van 3 meter boven NAP of hoger.
11.	Meetbare baten	Betrouwbaarheid van de keringen die neerkomt op een faalkans die niet lager mag zijn dan de huidige situatie
12.	Huidige technologie/ architectuur	Industriële Automatisering (IA), te weten Siemens PLC's, met connecties naar monitoringsystemen in Windows
13.	Doeltechnologie/- architectuur	Vergelijkbare oplossing als in huidige situatie, waarbij de IA-hardware niet beperkt is tot een specifiek merk.
14.	Omvang systeem	Geen informatie bekend over regels code of functiepunten.
15.	Aantal gebruikers	20 tot 30
16.	Belanghebbenden	• Havenbedrijf Rotterdam: beheerder van de Vaarweg Nieuwe Waterweg – Hartelkering. • Provincie Zuid-Holland • Ministerie van Infrastructuur en Waterstaat (Directoraat-generaal Water en Bodem) • Intern RWS – Rijkswaterstaat, Regio (WNZ) afdeling Stormvloedkeringen – Beheerder – Rijkswaterstaat, Programma's Projecten en Onderhoud (PPO) – Rijkswaterstaat, Centrale Informatie Voorzieningen (CIV) / Programma BIK – Rijkswaterstaat Cybersecurity center (SOC) • Marktpartijen
17.	Aanbesteding voorzien	Ja

Informatie over het uitgevoerde onderzoek

Nr	Onderwerp	Toelichting
1.	Type onderzoek	Project; conform artikel 2, lid 2 sub a1 Instellingsbesluit Adviescollege ICT-toetsing
2.	Aanmelddatum	30-05-2022
3.	Start onderzoek	22-02-2023
4.	Afronden onderzoek	22-05-2023
5.	Datum conceptadvies	03-07-2023
6.	Datum definitief advies	20-07-2023
7.	Eerder onderzoek	Nee
8.	Onderzoeksmethode	Interviews, documentenonderzoek, forensische analyses, schouwen Hartelkering en Locomobiel Noordzijde Maeslantkering