Adviescollege ICT-toetsing

> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Infrastructuur en Waterstaat
t.a.v. de minister, de heer V.P.G. Karremans LLM MSc
Postbus 20904
2500 EX Den Haag

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

Contactpersoon
info@adviescollegeicttoetsing.nl

Betreft
Advies project Vervangen BESW

Datum
19 augustus 2026

Kenmerk
2026-0000448355

Uw kenmerk
RWS-2025/19172

Bijlage(n)
1

Geachte heer Karremans,

Uw voorganger heeft het Adviescollege ICT-toetsing verzocht een onderzoek uit te voeren naar het project Vervangen BESW van Rijkswaterstaat (RWS). BESW staat voor Bediening- en Besturingssysteem Waterweg. Middels BESW wordt de Maeslantkering geautomatiseerd bediend en bestuurd. De opdrachtgever van het project is de hoofdingenieur-directeur van de regio West-Nederland Zuid. Het advies kan als volgt worden samengevat:

RWS heeft met het project 'Vervangen BESW' tot doel om - vóór de start van het stormseizoen 2030 - de huidige geautomatiseerde besturing van de Maeslantkering (BESW) te vervangen door een industriële automatiseringsoplossing die aantoonbaar betrouwbaar is, correct functioneert en onderhoudbaar is.

Conclusie

Wij herkennen de noodzaak tot verbetering van BESW; de huidige staat is onacceptabel als besturing van een veiligheidskritisch object als de Maeslantkering. De gekozen aanpak leidt echter tot schijnzekerheid over betrouwbaarheid en niet noodzakelijkerwijs tot een betrouwbaar BESW, want:

A. Kwantitatieve benadering van betrouwbaarheid is ongeschikt voor software.
B. Beoogde aanbesteding is onvoldoende gericht op veiligheidskritische aspecten BESW.
C. Stuurgroep stuurt onvoldoende op functionele veiligheid zoals de IEC 61508-norm voorschrijft.

Advies

Wij adviseren u om het systematisch verbeteren van de betrouwbaarheid van BESW centraal te stellen in plaats van het vooraf kwantificeren van de softwarebetrouwbaarheid:

1. Werk volgens de IEC 61508-norm, gericht op maatregelen die de betrouwbaarheid van software verbeteren.
2. Werk veiligheidseisen en systeemontwerp uit zodat hierop gestuurd kan worden.
3. Versterk inhoudelijke sturing, en benut intern en extern aanwezige kennis.
4. Werk ook na de vervanging doorlopend aan het verhogen van de betrouwbaarheid.

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

Datum
19 augustus 2026

Kenmerk
2026-0000448355

Korte omschrijving van het project Vervangen BESW

Het deltawerk Maeslantkering ligt in de Nieuwe Waterweg bij Hoek van Holland en werd gebouwd tussen 1991 en 1997. Het bouwwerk vormt, met de Hartelkering en de dijkverbreding Rozenburg, de Europoortkering. Samen beschermen ze ruim twee miljoen Nederlanders en het achterland tegen overstromingen.

De Maeslantkering wordt aangestuurd door het Beslis- en Ondersteunend Systeem (BOS). Het BOS voorspelt de waterstand op basis van verschillende data, zoals windsnelheden en windrichting. Als de voorspelde waterstand in Rotterdam 3 meter boven NAP of in Dordrecht 2,90 meter boven NAP dreigt te komen, besluit het BOS tot sluiting van de kering. De kering wordt maandelijks getest en jaarlijks vindt er een functioneringssluiting plaats. Als er zeven jaar lang geen stormsluiting heeft plaatsgevonden (tot op heden is er éénmaal een stormsluiting geweest, in december 2023), voert Rijkswaterstaat een verificatiesluiting uit. Hiertoe verlaagt RWS één keer het officiële sluitpeil zodat geoefend kan worden met het sluiten van de kering onder stormcondities. De stijging van de zeespiegel kan de komende jaren leiden tot een hogere sluitfrequentie.

Op commando van het BOS bestuurt BESW (Bedienings- en Besturingssysteem Waterweg) de kering. In nood kan de kering lokaal worden bediend zonder BOS/BESW, mocht dat nodig zijn. Het sluitproces start met het vollopen van de parkeerdokken waarin de kerende wanden liggen, zodat ze gaan drijven. Vervolgens worden de kerende wanden in de Nieuwe Waterweg ingevaren en afgezonken. Openen gaat in de omgekeerde volgorde.

De Maeslantkering moet voldoen aan een wettelijke faalkanseis bij sluiten van 1:100. Oftewel: de kering mag slechts één keer per *ten minste* 100 keer sluiten falen (onder stormcondities).

In 2012 heeft RWS de hardware van BESW (PLC's[1], met een technische levensduur van circa 15 jaar) en de software vervangen. RWS heeft vervolgens geconstateerd dat bij deze vervanging een aantal fouten is gemaakt en zaken zijn nagelaten, waardoor de faalkans significant werd verhoogd. De software bevat bijna 100 bekende defecten die tot serieus falen kunnen leiden. Uit interviews en gesprekken is dat ook gebleken; bij 17 sluitingen is minstens viermaal handmatig ingegrepen op het besturingssysteem. De organisatie heeft na 2012 drie projecten uitgevoerd om de fouten en omissies in BESW te herstellen; deze projecten zijn allemaal mislukt. Er was geen vertrouwen dat de projecten tot betere resultaten zouden leiden dan de bestaande situatie. Omdat inmiddels ook de in 2012 geplaatste hardware richting het eind van de levenscyclus gaat, wil RWS deze uiterlijk in 2030 vervangen hebben.

RWS heeft met het project 'Vervangen BESW' voor ogen om vóór de start van het stormseizoen 2030 de huidige automatisering van de Maeslantkering te vervangen door een industriële automatiseringsoplossing die aantoonbaar betrouwbaar is, correct functioneert en onderhoudbaar is. Het project start een aanbesteding, met geplande publicatie in september 2026. De aanbesteding richt zich op het ontwerp, de BESW-software en -apparatuur (zoals PLC's, netwerk, voeding en besturings- en bedieningspanelen), en het beheer en onderhoud. BESW krijgt een levensduur tot minimaal 2045 en RWS wordt eigenaar van de broncode.

[1] PLC: Programmable Logic Controller, hardware voor de aansturing van technische installaties.

Conclusie: Gekozen aanpak leidt tot schijnzekerheid over betrouwbaarheid

Datum
19 augustus 2026

Kenmerk
2026-0000448355

Wij herkennen de noodzaak tot verbetering van BESW: de huidige staat is onacceptabel als besturing van een uniek veiligheidskritisch object als de Maeslantkering. We zien een positieve ontwikkeling, namelijk dat RWS de eigen kennis en ervaring heeft gebundeld in het Keringenteam Industriële Automatisering en deze inzet voor de stormvloedkeringen.

Voor het realiseren van software-intensieve systemen die een hoge betrouwbaarheid vereisen, is de internationale norm IEC 61508 ontwikkeld. Deze basisnorm voor functionele veiligheid stelt dat softwarefalen zich anders gedraagt dan hardwarefalen. Softwarefalen laat zich maar moeilijk kwantificeren voor systemen met een lage vraagfrequentie en zeker niet vóór de ontwikkeling ervan. Daarom beveelt de IEC 61508-norm activiteiten aan die de kans op softwarefalen zo ver verlagen als redelijk mogelijk is. En daarmee de betrouwbaarheid zo ver verhogen als redelijk mogelijk is. Dat vergroot het vertrouwen dat de vereiste veiligheidsniveaus bij indienststelling worden gehaald. De norm definieert activiteiten voor de hele ontwikkelcyclus en beheerfase, zoals het gebruik van formele methodes en modelgebaseerd testen. Formele methodes werden dertig jaar geleden ook al toegepast bij de bouw van de Maeslantkering voor het ontwikkelen van het systeem BOS dat BESW aanstuurt [2].

De gekozen aanpak voor het project ‘Vervangen BESW’ voldoet op belangrijke punten niet aan de IEC 61508-norm en gaat niet noodzakelijkerwijs leiden tot een betrouwbaar BESW. Hieronder lichten wij onze conclusie nader toe.

A. Kwantitatieve benadering van betrouwbaarheid is ongeschikt voor software

RWS hanteert voor BESW een werkwijze die niet geschikt is voor de besturing van een veiligheidskritisch object als de Maeslantkering. Dit komt voornamelijk doordat RWS de softwarebetrouwbaarheid van BESW vooraf tracht te kwantificeren met behulp van modellen. Deze modellen zijn gebaseerd op de foutenboomanalyse (fault tree analysis, FTA), een methode geschikt voor hardware, maar niet voor software. FTA gaat uit van typisch hardwarefalen zoals slijtage. In de FTA van de Maeslantkering die we hebben onderzocht, worden softwareonderdelen op dezelfde manier als hardware-onderdelen gemodelleerd, waarbij ook aan softwareonderdelen faalkansen worden toegekend. Dit kan niet, omdat software zich anders gedraagt dan hardware; softwarefalen is systematisch, en kan dus niet vooraf gekwantificeerd worden en op dezelfde manier in een FTA worden opgenomen als hardwarefalen. Bovendien zijn de ontwikkelde FTA-modellen te complex om er verantwoorde conclusies aan te verbinden. We zien dan ook dat BESW (het besturingssysteem van de kering) in werkelijkheid veel vaker faalt dan de modellen van RWS voorspellen.

Voor de vervanging van BESW wil RWS dat het project dergelijke modellen toepast om (vooraf) de softwarebetrouwbaarheid te kwantificeren. Daardoor is de kans groot dat het project resulteert in schijnzekerheid, namelijk een systeem dat volgens de RWS-modellen wel veilig zou zijn, maar in werkelijkheid onbetrouwbaar is. Bovendien wil RWS deze werkwijze na oplevering blijvend toepassen om, met een modelmatig berekend getal, periodiek aan het ministerie van IenW aan te tonen dat de kering voldoet aan de wettelijke faalkanseis van 1 op ten minste 100 bij sluiting, hetgeen niet mogelijk is.

[2] Tretmans, J., Wijbrans, K. and Chaudron, M., 2001. Software engineering with formal methods: The development of a storm surge barrier control system - Revisiting seven myths of formal methods. *Formal methods in system design*, *19*(2), pp.195-215.

B. Beoogde aanbesteding is onvoldoende gericht op veiligheidskritische aspecten BESW

De aanbesteding moet leiden tot keuze van een leverancier (of consortium) die een betrouwbaar BESW gaat realiseren, maar biedt daartoe onvoldoende zekerheid. Het realiseren van BESW vraagt hoog-specialistische kennis en een stevige inhoudelijke regie, maar de gekozen aanbestedingsaanpak sluit onvoldoende aan op deze situatie. De aanpak bestaat uit diverse onderdelen zoals het beschikbaar stellen van het Detail Software Ontwerp (DSO) en een klanteisenspecificatie, en het uitvoeren van een proof of concept (PoC).

- RWS zet wederom de eigen modellen in om voorgestelde oplossingen van leveranciers te beoordelen en op basis daarvan de leverancier te selecteren. Hierdoor ontstaat het risico dat er een leverancier geselecteerd wordt wiens voorgestelde oplossing wel goed scoort op deze modellen, maar uiteindelijk niet de benodigde kwaliteit heeft.
- Hoewel de inhoudelijke expertise binnen het projectteam groeit, wordt deze expertise slechts beperkt ingezet voor inhoudelijke regie op de beoogde aanbesteding en realisatie. De impliciete aanname van RWS is dat een opdrachtnemer over alle expertises beschikt en hierop inhoudelijke regie kan voeren om een betrouwbaar BESW te realiseren. Een expliciete uitvraag van hoog-specialistische expertise in verschillende kennisgebieden (bijvoorbeeld functionele veiligheid en betrouwbaarheid) ontbreekt.
- Pas als de resultaten van de toekomstige leverancier achterblijven, wil RWS de betrokkenheid van de huidige experts binnen het projectteam verhogen en hen de inhoudelijke regie laten voeren op de realisatie. Zij kunnen er dan voor zorgen dat functionele omschrijvingen eenduidig worden geïnterpreteerd, en zorgvuldig worden uitgewerkt en vertaald naar implementatie en code.
- De aanbesteding is alleen in het Nederlands opgesteld. Dit verlaagt de kans op het binnenhalen van de benodigde expertise, omdat internationale, gespecialiseerde partijen minder goed worden bereikt.

C. Stuurgroep stuurt onvoldoende op functionele veiligheid zoals de IEC 61508-norm voorschrijft

In de afgelopen periode heeft RWS het Keringenteam Industriële Automatisering opgezet waarin de eigen kennis en ervaring gebundeld is, en dat ingezet wordt voor de stormvloedkeringen. Wij zien dat hierdoor op operationeel/tactisch niveau in het project veel kennis aanwezig is. Dat is een positieve ontwikkeling. Het ontbreekt echter aan sturing en focus op functionele veiligheid conform de IEC 61508-norm:

- De stuurgroep stuurt dominant op een harde deadline in plaats van op een zo betrouwbaar mogelijk BESW.
- De stuurgroep past RWS-richtlijnen en -processen toe voor standaardprojecten. Zo moet er in de huidige aanpak onder andere voldaan worden aan een standaardproces voor het definiëren van de eisen, waardoor bijvoorbeeld veiligheidseisen van het systeem niet traceerbaar zijn naar veiligheidseisen van de software. Het realiseren van een veiligheidskritisch besturingssysteem vraagt echter een aanpak gericht op betrouwbaarheid die van standaardprocedures kan afwijken.
- De stuurgroep heeft de kwaliteit van de eisen onvoldoende in beeld, terwijl de eisen de basis vormen voor de aanbesteding:
  - De functionele eisen (klanteisen) zijn tot nu toe onvoldoende uitgewerkt. Dit kan leiden tot veiligheidsrisico's en hoge herstelkosten.
  - De niet-functionele eisen zijn onvoldoende vastgelegd. De softwarebetrouwbaarheidseisen zijn niet expliciet gemaakt. Er is alleen op basis van de eerder genoemde modellen een faalkans voor de software berekend.
  - Het ontbreekt aan de inzet van externe kennishouders die goed kunnen bijdragen aan de juiste sturing en focus op functionele veiligheid.

Advies: Stel systematisch verbeteren betrouwbaarheid BESW centraal in plaats van kwantificering

Datum
19 augustus 2026

Kenmerk
2026-0000448355

De huidige staat van BESW is sinds de vervanging van hardware en software in 2012 onacceptabel als besturing van de Maeslantkering en de gekozen aanpak gaat niet noodzakelijkerwijs leiden tot een betrouwbaar BESW. Daarom adviseren wij u het systematisch verbeteren van de betrouwbaarheid van BESW centraal te stellen in plaats van het vooraf kwantificeren van de softwarebetrouwbaarheid. Die aanpak leidt namelijk tot schijnzekerheid.

1. Werk volgens de IEC 61508-norm, gericht op maatregelen die de betrouwbaarheid van software verbeteren

Om de betrouwbaarheid systematisch centraal te stellen, adviseren wij de inkoopstrategie zodanig te wijzigen dat inkoop en inhuur zijn gericht op de hoogste kwaliteit per kennisgebied:

- Onderscheid verschillende kennisgebieden, zoals formele technieken, modelgebaseerd testen, veiligheidskritische software-ontwikkeling, systeemintegratie, begeleiding en certificering inzake functionele veiligheid, hardware, cyberveiligheid en multi-technische dienstverlening. Kies voor een wijze van inkoop die zorgt voor optimale betrouwbaarheid. Werf actief in binnen- en buitenland omdat kennis en kunde over de verschillende gebieden schaars zijn.
- Stem de wijze van beoordeling van aanbieders af op het betreffende kennisgebied en de gekozen inkoop- of samenwerkingsvorm. Stel softwarebetrouwbaarheid centraal tijdens de beoordeling, onder andere door de IEC 61508-norm met beleid te volgen, en laat de kwantitatieve beoordeling met eigen faalkansmodellen los.
- Zorg dat de inbreng van de experts op bovengenoemde kennisgebieden leidend is bij inhoudelijke besluitvorming op het project.
- Tref voorbereidingen voor tegenvallers:
  - Ga alvast in overleg met de huidige leverancier, met het oog op een verlengde ondersteuning van het bestaande systeem inclusief hardware-support.
  - Maak, voor zover het nog niet is gebeurd, plannen voor de aanschaf van extra hardware om het huidige systeem operationeel te houden, op basis van een inventarisatie van benodigde apparatuur, de bijbehorende kosten en de verwachte levertermijnen.

2. Werk veiligheidseisen en systeemontwerp uit zodat hierop gestuurd kan worden

Een van de maatregelen die de IEC 61508-norm stelt voor het verhogen van de betrouwbaarheid en functionele veiligheid van een systeem, is het eenduidig vastleggen van eisen, zodat deze volledig en toetsbaar zijn, het ontwerp en de implementatie correct worden uitgevoerd en het systeem ook in randgevallen functioneert zoals bedoeld. Om dit te bewerkstelligen zijn de volgende stappen noodzakelijk:

- Benut de kennis binnen RWS over de huidige systeemarchitectuur van BESW door deze te verankeren in een formele specificatie. Zorg dat experts op het gebied van formele methoden dit proces leiden. Pas formele specificatie toe voor het eenduidig vastleggen van de eisen voor de vervanging van BESW, naast de uitgebreide functionele beschrijvingen in het bestaande DSO. Beleg de besluitvorming bij experts in formele technieken, zodat hun oordeel leidend is bij keuzes rondom de specificatietaal, de methodiek, de mate van formalisering, de mate van bewijsvoering en de inzet van tooling. Pas formele verificatie en validatie toe op deze specificatie, als basis voor het realiseren van BESW. Standaardiseer de uitkomsten voor toekomstige codegeneratie.
- Breid de mogelijkheden binnen RWS uit om het gedrag van BESW te simuleren in een representatieve (hardware)omgeving om onvolkomenheden en fouten tijdig te detecteren. De al aanwezige Automated Test Environment (ATE) en digital twin zijn een goed startpunt daarvoor.

- Behoud de huidige terugvalmogelijkheden (noodbediening via de Alternatieve Bediening Kerende Wand en de bijbehorende Opleiding-Training-Oefening), omdat dergelijke redundantie essentieel is voor een zo hoog mogelijke betrouwbaarheid. Zorg daarnaast dat het personeel hiervoor beschikbaar blijft.

3. Versterk inhoudelijke sturing, en benut intern en extern aanwezige kennis

Stel zeker dat de stuurgroep in staat is vanuit de inhoud te sturen. Hanteer daarbij de volgende aanpak:

- Versterk de expertise binnen de stuurgroep zodat die met gezag en onderbouwd besluiten kan nemen over softwarebetrouwbaarheid.
- Betrek experts in de besluitvorming en laat deze aan de stuurgroep rapporteren, bijvoorbeeld als het gaat om onderwerpen als systeemarchitectuur, inzet formele methoden, modelgebaseerd testen of doorontwikkeling van alternatieve noodbedieningen. Zorg ervoor dat als er wordt afgeweken van de adviezen van experts, de consequenties en risico's expliciet door de stuurgroep worden geaccepteerd.
- Faciliteer als stuurgroep het project bij het zo spoedig mogelijk doorvoeren van initiatieven die de betrouwbaarheid verbeteren, bijvoorbeeld door snelle inhuur van specialistische kennis.
- Laat onafhankelijke experts periodiek rapporteren over het wel of niet halen van de wettelijke faalkanseis aan RWS en de minister. De stuurgroep neemt de verantwoordelijkheid om te beslissen wat wel of niet redelijk is voor RWS in de toepassing van het ALARP[3]-principe op basis van leidende adviezen van de experts. Zorg daarbij voor:
  - begeleiding ten aanzien van conformiteit met de IEC 61508-norm door een onafhankelijke partij vanaf de start van het project en gedurende het gehele realisatietraject;
  - verplichte certificering ten aanzien van conformiteit met de IEC 61508-norm door een onafhankelijke partij in een aparte opdracht.

4. Werk ook na de vervanging doorlopend aan het verhogen van de betrouwbaarheid

Om grip te krijgen op de toekomstige betrouwbaarheid van BESW adviseren wij de volgende maatregelen:

- Verbeter - samen met de experts - de na de vervanging aanwezige specificatie en het ontwerp zodat deze duurzaam, compact en implementatie-onafhankelijk worden. Gebruik deze vervolgens als basis voor codegeneratie zodat de volgende vervanging (over weer circa 15 jaar) beperkt blijft tot voornamelijk hardware. Dat doet recht aan de beoogde levensduur van 100 jaar.
- Gebruik de logdata van de kering en de simulator voor inzicht in de feitelijke werking van BESW en in de empirische betrouwbaarheid van de kering.
- Gebruik de uitkomsten van simulaties met de digital twin (duur-, stress- en regressietests) als grondslag om de betrouwbaarheid van BESW te verhogen.

***

[3] ALARP staat voor "As Low As Reasonably Practicable", een zo laag als redelijkerwijs mogelijke kans op falen.

Adviescollege ICT-toetsing

Tot slot danken wij alle geïnterviewden voor hun medewerking en openheid. Wij hopen met dit advies bij te dragen aan een duurzame verbetering van de betrouwbaarheid van BESW.

Datum
19 augustus 2026

Kenmerk
2026-0000448355

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

w.g.

Adri de Bruijn
Voorzitter

w.g.

Sander van Amerongen
Secretaris-directeur

Adviescollege ICT-toetsing

Bijlage

Datum
19 augustus 2026

Kenmerk
2026-0000448355

Informatie over project Vervangen BESW

Nr.	Onderwerp	Toelichting
1.	Projectnaam	Vervangen BESW
2.	Opdrachtgever	Hoofdingenieur-directeur van de regio West-Nederland Zuid
3.	Startdatum project	04-06-2025
4.	Einddatum project	31-12-2030
5.	Type project	Vervanging software en hardware
6.	Fase Project	In uitvoering
7.	Totaal budget	Vertrouwelijk
8.	Reeds uitgegeven per 30 maart 2026	€713.358
9.	Doelstelling	De huidige automatisering van de Maeslantkering vervangen door een industriële automatiseringsoplossing die aantoonbaar betrouwbaar is, correct functioneert en onderhoudbaar is
10.	Maatschappelijke/ beleidsdoelstelling	Bescherming van ruim 2 miljoen inwoners van Zuid-Holland bij een waterpeil in van 3 meter of hoger boven NAP in Rotterdam of 2,90 meter boven NAP of hoger in Dordrecht
11.	Meetbare baten	• Onderhoudbaar BESW • Sneller oplossen van storingen • Minder benodigd personeel • Mogelijkheid tot uitbreiding van functionaliteit
12.	Huidige technologie/ architectuur	Industriële Automatisering (IA), te weten ABB PLC's en SCADA-systemen
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	• 2 miljoen inwoners van Zuid-Holland die tegen overstroming beschermd worden door de kering • Ministerie van Infrastructuur en Waterstaat • Rijkswaterstaat • Marktpartijen
17.	Aanbesteding voorzien	Ja

Informatie over het uitgevoerde onderzoek

Nr.	Onderwerp	Toelichting
1.	Type onderzoek	Project; conform artikel 7, lid 1 sub a2 Wet Adviescollege ICT- toetsing
2.	Aanmelddatum	7 juli 2025
3.	Start onderzoek	1 december 2025
4.	Afronden onderzoek	29 mei 2026
5.	Datum concept advies	25 juni 2026
6.	Datum definitief advies	19 augustus 2026
7.	Eerder onderzoek	Onderzoek naar project BEST2DO (2023). Dit project beoogde de betrouwbaarheid van de besturingssystemen van de Hartelkering en van de locomobiel van de Maeslantkering voor een periode van ongeveer vijftien jaar te borgen
8.	Onderzoeksmethode	Desk research, interviews, data-analyse