Bijlage O Faalkansprestatie BEST2DO

Deze bijlage beschrijft wat de Inschrijver die met de gunningsbeslissing als eerste in de rangorde is geëindigd nog moet aantonen alvorens kan worden overgegaan tot gunning (onder opschortende voorwaarden) van de Realisatieovereenkomst fase 1 en Realisatieovereenkomst fase 2.

Faalkansberekening ten behoeve van gunning Realisatieovereenkomst fase 1:
De inschrijver die voor opdracht in aanmerking komt, voordat kan worden overgegaan naar gunning onder opschortende voorwaarden (stap 5 van de aanbesteding) dient de inschrijver aan te tonen dat het systeem BESH en BESL voldoet aan de volgende Faalkanseisen:

Faalkanseisen voor BESH:
1. De gecombineerde faalkans van de BESH Hardware en software moet lager worden dan 2,91e-3.
2. De faalkansbijdrage voor Software BESH moet lager worden dan 2,55e-3 [failure on demand].
3. De faalkansbijdrage voor Hardware BESH moet lager worden dan 3,56e-4 [failure on demand].

Faalkanseisen voor BESL:
1. De gecombineerde faalkans van de BESL-hardware en software samen moet lager worden dan 9,96e-4 (voor Noord en Zuid samen), oftewel 4,98e-4 per zijde;
2. De faalkansbijdrage voor Software BESL moet lager worden dan 4,24e-4 per zijde [failure on demand]. Omdat de BESL-software verschillende deuren aanstuurt, en dus ook verschillende toestanden zal kennen, wordt uitgegaan van het onafhankelijk falen van de zijdes.
3. De faalkansbijdrage voor Hardware BESL moet lager worden dan 7,40e-5 per zijde [failure on demand].

De huidige faalkanseis van software kan maar deels gebaseerd worden op het huidige budget uit de foutenboom. Gegeven de grote impact van de software van BESL heeft op de veiligheid van het achterland en het feit dat software betrouwbaarheid in praktijk alleen in gehele ordergroottes realistisch kan worden ingeschat, wordt voor de software van het nieuwe systeem een ondergrens van minste 1e-4 voor de BESL-software gehanteerd (dit geeft aanleiding tot een SIL-4 systeem conform IEC61508

Randvoorwaardelijk:
De faalkans van BESL en voor BESH beperkt zich tot hardware en software van het besturingssysteem, zonder de elektro-, mechanische- en hydraulische installatie.

Onderbouwing bij de faalkansberekening:
1) *Architectuur views:* De Opdrachtnemer dient bij de aanbesteding de architectuur van de oplossing te beschrijven in een aantal ‘views’. Deze views betreffen minimaal:
    a. Een context beschrijving;
    b. een functionele (dynamische) beschrijving (hoe werkt het);
    c. Een systeem-decompositie (statische) beschrijving (waar bestaat het uit)

2) *Foutenboom:* Voor de bepaling van de gecombineerde faalkans van de hardware en software op architectuurniveau dient een initiële foutenboom opgesteld te worden welke bestaat uit:
    a. Een analyse voor de faalkansbudgettering van de software over de verschillende deelsystemen en PLC’s als onderdeel van de architectuur, waarbij een initiële faalkansbudgettering per deelsysteem wordt bepaald en de bijdrage aan de gecombineerde faalkans wordt beschouwd
    b. Op basis van de faalkansbudgettering voor deelsystemen dient in een analyse vervolgens de SIL-allocatie per geïdentificeerd subsysteem bepaald worden.
    c. De Opdrachtnemer dient foutenbomen zodanig te coderen dat deze aansluit op de gebruikte coderingen van de faalwijzen uit de FMEA en de analyse externe gebeurtenissen.
    d. Onderkende TUBs (zie TOPAAS, Deel 1 Handleiding (Kader), 28 maart 2018) die kunnen leiden tot falen of niet-beschikbaar zijn van BeSL, worden per module in de vorm van aparte basisgebeurtenissen in de foutenboom opgenomen.
    e. Aanvullend dient in de foutenboomanalyse te worden aangegeven of, en zo ja welke, latente onderhoudsfouten kunnen worden gemaakt. Hieronder worden fouten verstaan

die worden gemaakt tijdens onderhoud waarbij de installatie niet (volledig) operationeel wordt achtergelaten.

3) *FMEA:* Op basis van een Failure Mode and Effect Analyses (FMEA) tot op componentniveau dienen alle faalmanieren en de bijbehorende effecten en maatregelen van de onderlaag van BESL en voor BESH geanalyseerd worden waardoor:
    a. Dat de toegepaste componenten geschikt zijn voor hun functie en dat het risico van desbetreffende failure mode binnen de gestelde faalkansdoelstellingen past.
    b. De desbetreffende ongewenste gebeurtenis relevant is voor de faalkansanalyse.
    c. Hierbij dienen onderliggende cijfers/aannames/keuzes over; betrouwbaarheid van de toegepaste componenten (1/MTTF); hersteltijden; testintervallen (gerelateerd aan deurbewegingen, maar ook automatische testen zoals die bijvoorbeeld in het huidige systeem maandelijks worden uitgevoerd); coveragefactoren (deel van MTTF dat wordt afgedekt door zelfdiagnose) en aannames aangaande Common Cause Failure (CCF) factoren onderbouwd te worden.

4) S*oftware Safety Management Plan (SFMP) (BPKV-criteria):* Ten behoeve van de software betrouwbaarheid en de productiewijze om tot foutarme software te komen wordt gevraagd om een SFMP. Hiervoor gelden de volgende eisen/uitgangpunten:
    a. Voor het opstellen van het SFMP dient de IEC61508 te worden gevolgd.
    b. Het SFMP is onderdeel van Software Development Plan (SDP), waarbij het SDP wordt opgesteld na aanbesteding.

ad 1. De views dienen gebaseerd te zijn op de huidige SCADA-PLC-oplossing voor BESH en BESL. De architectuur dient alle hardwarecomponenten inclusief netwerkcomponenten (het betreft alleen componenten om te koppelen met de ‘netwerkbackbone’ m.a.w. geen glasvezelbekabeling en glasvezel nodes) te bevatten.

ad 3. De risico’s en de mitigerende maatregelen zullen na gunning in fase1-voorbereiding met een Proof-of-concept (POC) in een testopstelling worden getoetst of de getroffen maatregelen afdoende zijn om de faalkansprestatie te bereiken.

Faalkansprestatie ten behoeve van gunning Realisatieovereenkomst fase 2:
Om over te kunnen gaan naar gunning fase 2 dient de Opdrachtnemer een proof-of-concept te leveren voor BESH en voor BESL:

1) *Proof-of-concept:* Het proof-of-concept bestaat uit het in een testopstelling aantonen van de juiste samenwerking van de door de Opdrachtnemer gekozen kritische hardware en software, hierbij wordt gebruik gemaakt van de FMEA. Bijvoorbeeld bij de keuze van redundantie, waarbij kan worden aangetoond dat er zonder tijdverlies omgeschakeld wordt (hot-standby principe).

2) *Faalkansbudgettering:* De functionele view dient alle taakuitvoeringen te benoemen die nodig zijn voor de (kritische) functionaliteit. Dit zijn de TUB’s (Taak Uitvoerings Blokken) in TOPAAS-terminologie. Per TUB moet ook een budgettering zijn opgenomen voor hun bijdrage aan de faalwijzen van BESL en voor BESH, en de mate van onafhankelijkheid van falen indien er gebruik gemaakt wordt van redundantie. Ook dient de Opdrachtnemer in de voorbereidingsfase alle onderdelen uit de systeemdecompositie-view uit te werken in systeemeisen, aspecteisen, interfacespecificaties en ontwerp, en via vastgelegde testcases op de interfacespecificatie getest te worden.

3) Een *herijkt SFMP*, op basis van de concretere eisen die voortkomen uit faalkansbudgettering, de IEC61508 en TOPAAS om te komen tot een kwalitatief voldoende invulling van de TUBs. Hiermee kan de opdrachtnemer dus op basis van de gekozen faalkansbudgettering van de verschillende (klasses van) TUBs en de mogelijk nieuwe inzichten aannemelijk maken dat de beoogde faalkans ook gehaald gaat worden.

4) *Betrouwbaarheid Groei Model (Reliability Growth Model)* en *een borgingsplan:* Gevraagd wordt om het Betrouwbaarheid Groei Model op te zetten, in de KES worden de eisen aan dit model specifiek gemaakt. TOPAAS wordt normaliter toegepast nadat een (software)product gereed is. RWS wil dat bij het ontwikkelen van BESL en BESH in de voorbereidings- en realisatiefase zicht

krijgen op het voortbrengingsproces om te kunnen oordelen over de betrouwbaarheid van de (tussen)producten. Dus tussentijdse TOPAAS-toetsen hebben een belangrijke meerwaarde voor RWS, wat vastgelegd wordt in het borgingsplan.

Te gebruiken tooling:
Foutenboom: ISO-Graph RWB Faulttree+ versie 15 of hoger