



RWS BEDRIJFSVERTROUWELIJK

Deelsysteemontwerp Bediening- en Besturingssysteem

Renovatie project; ZD B Sluizen
Zaaknummer 31159162

Datum 18 mei 2022
Versie 1.0
Status definitief

Colofon

Uitgegeven door	Programma's, Projecten en Onderhoud ZD B Sluizen
Auteur	Rob Petie
Informatie	Frank Leeman
E-mail	ZD-B-Sluizen@rws.nl
Datum	18 mei 2022
Versie	1.0
Status	definitief

Versiebeheer

0.1	18 februari 2021	Eerste versie
0.2	11 maart 2021	Versie na review commentaar
0.3	22 april 2021	Versie na review commentaar
0.4	11 maart 2022	Verdiepingsslag / integratie BPP 2.0+
0.5	28 april 2022	Verwerking intern review commentaar
1.0	18-05-2022	Definitief gemaakt

Inhoud

	Inleiding	4
1	Positionering deelsysteem	7
2	Input	8
2.1	Scope	8
2.2	Klanteisen	8
2.3	Referentiedocumenten	8
2.4	Onderzoeken en externe besluitvorming	9
2.5	Overige input	9
3	Ontwerp	10
3.1	Nu en straks	10
3.2	Afbakening en functiebeschrijving objecten	10
3.3	Ontwerpbesluiten	11
3.4	Eisen uit de LBS	17
3.5	Beschouwing raakvlakken	17
4	Output	19
4.1	Specificaties	19
4.2	Referentie ontwerp	20
4.3	Raakvlakken	21
4.4	Aandachtspunten voor het proces	21
4.5	Kansen en risico's	22
4.6	BTO-keuzes	22
5	Openstaande punten	23
A	Systemen versus bedieningen	24
B	Referentie ontwerp hardware Bediening en Besturing	25
C	Referentie ontwerp software Bediening en Besturing	26

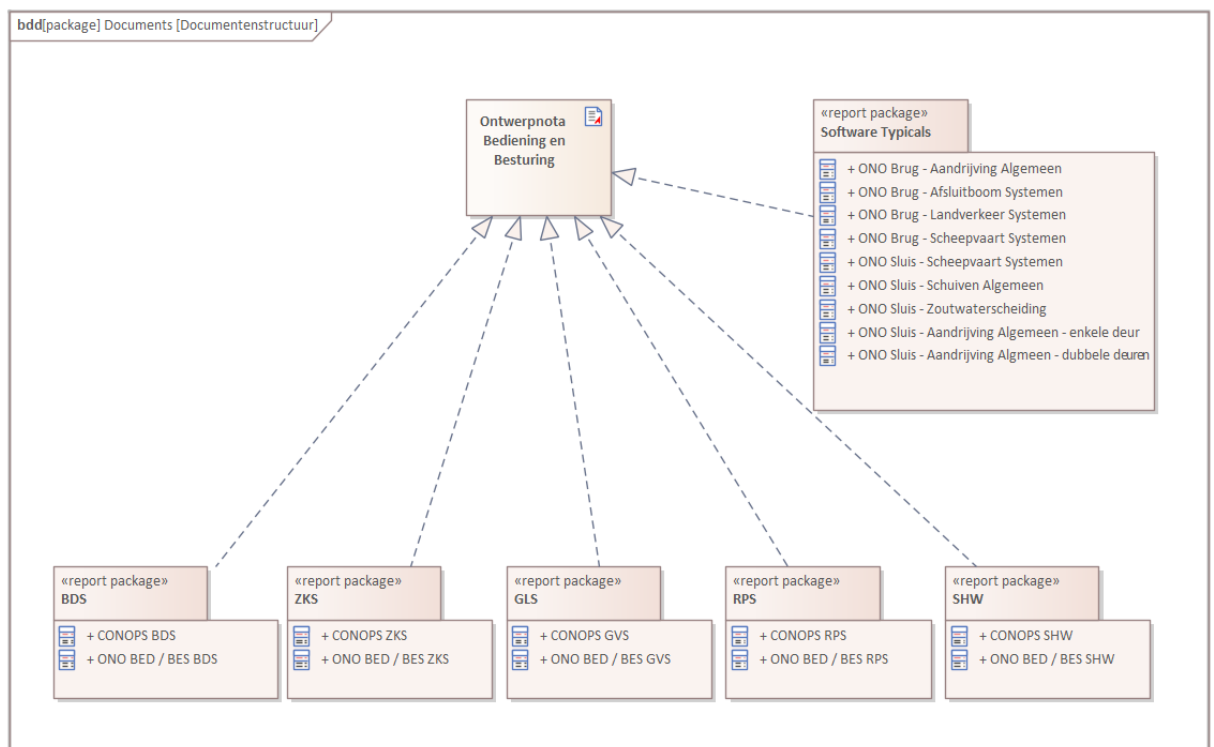
In dit generieke deelsysteemontwerp wordt het deelsysteem Bediening- en Besturingssysteem van de nautisch objecten ontworpen. Beschreven wordt wat we al weten, wat we belangrijk vinden, wat te veel tijd zou kosten om tijdens de Ontwerpfase uit te zoeken, wat risicovol is, enzovoort. Het ontwerp leidt uiteindelijk tot een set aan systeemspecificaties, kansen, risico's, BTO-keuzes e.d. op het niveau van een voorlopig ontwerp/referentieontwerp. De output is *uitdrukkelijk geen compleet ontwerp*! Samen met de originele scope, klanteisenset en de resultaten van diverse vooronderzoeken vormt dit de basis voor het ontwerp in de Ontwerpfase van het contract.

Er is gekozen om één generieke ontwerpnota voor het Bedienings- en Besturingssysteem op te stellen wat voor elk nautisch object van toepassing is. Bij dit deelsysteemontwerp behoren de volgende onderdelen:

- Concept of Operation (CONOPS) per nautisch object, hierin is de functionele werking van het nautisch object beschreven;
- Ontwerpnota's van de zogenaamde software typicals waarin per deelsysteem de generieke software architectuur is beschreven. Deze moeten toegepast worden in de deelsysteemontwerpen van een nautisch object;
- Ontwerpnota per nautisch object, dit ontwerp beschrijft onder meer de specifieke ontwerpkeuzes van het betreffende nautisch object, het ontwerp van de bedienings- en besturingssoftware en de systeemspecificaties voor de volgende ontwerpstappen.

Vanwege de beperkte doorlooptijd van de Ontwerp- en Uitvoeringsfase is al een aanvang gemaakt met het opstellen van een hardware- en software architectuur voor de verschillende nautische objecten. Hierbij is zoveel mogelijk getracht het ontwerp zo te structureren dat delen daarvan hergebruikt kunnen worden voor de verschillende nautische objecten binnen ZD B Sluizen (en eventueel zelfs voor andere projecten). De typicals worden aangeleverd en in de Ontwerpfase verder uitgewerkt en aangevuld en toepasbaar gemaakt.

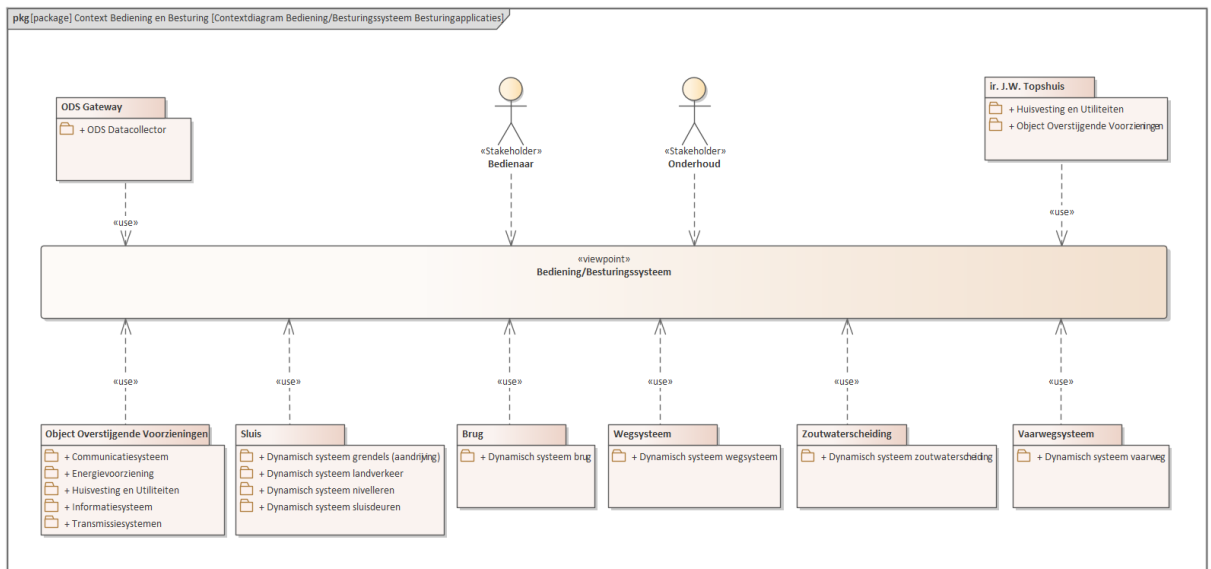
De samenhang van deze ontwerpstukken is in de volgende figuur weergegeven.



Figuur 2: Documentstructuur Bedienings- en Besturingssysteem

1 Positionering deelsysteem

De positionering van het deelsysteem is in onderstaande figuur weergegeven, hierbij is de relatie met bovenliggende en onderliggende objecten beschreven.



Figuur 3: Positionering deelsysteem

Opmerking: niet alle objecten en onderliggende objecten zijn weergegeven in deze objectdecompositie, noch zijn alle weergegeven objecten aanwezig op elk sluiscomplex. In Grip is per nautisch object de objectdecompositie onderliggend aan het Bedienings- en Besturingssysteem verder uitgewerkt.

Daarnaast vallen de bediensystemen van het Bewakingssysteem (gebouw/terreinbewaking, brandbeveiliging, klimaatinstallaties e.d.) niet onder het Bedienings- en Besturingssysteem van deze ontwerpnota. Zie daarvoor de ontwerpnota's Veiligheidssystemen.

2 Input

Dit hoofdstuk bevat de input vanuit de projectopdracht, waaronder scope en klantwensen. Daarnaast wordt verwezen naar relevante referentiedocumenten en overige input. Uitgangspunt is dat de Richtlijn Procesautomatisering gevolgd wordt, waarbij de aanvullingen en/ of afwijkingen daarop binnen dit document zijn beschreven.

2.1 Scope

De scope en omvang van het Bediening en Besturingssysteem van het betreffende te renoveren nautisch object wordt gespecificeerd in het deelsysteemontwerp (ONO) van het betreffende nautisch object.

2.2 Klanteisen

De klanteisen van het Bediening en Besturingssysteem voor het te renoveren nautisch object wordt per object gespecificeerd in het deelsysteemontwerp (ONO) van het betreffende nautisch object.

2.3 Referentiedocumenten

Onderstaande referentiedocumenten worden gebruikt bij dit ontwerp.

2.3.1 *Kaders, normen, richtlijnen*

Code	Titel	Versie
[RPA]	Richtlijn Procesautomatisering	22-02-2021 / V1.0
[SGBPO]	Style Guide Bedienplek Onderhoud en Beheer	22-02-2021 / V1.0
[RET]	Richtlijn Elektrotechniek	22-02-2021 / V1.0
[LBS]	RWS WVL, Landelijke Brug- en Sluisstandaard	V4.0
[CSIR]	RWS CIV, Cybersecurity Implementatierichtlijn Objecten – RWS	23-04-2021 / v2.4

2.3.2 *Overige documenten*

Code	Titel	Versie
	ONO Brug - Aandrijving Algemeen	1.0
	ONO Brug - Afsluitboom Systemen	1.0
	ONO Brug - Landverkeer Systemen	1.0
	ONO Brug - Scheepvaart Systemen	1.0
	ONO Sluis - Aandrijving Algemeen - enkele deur	1.0
	ONO Sluis - Aandrijving Algemeen - dubbele deuren	1.0
	ONO Sluis - Scheepvaart Systemen	1.0
	ONO Sluis - Schuiven Algemeen	1.0
	ONO Sluis - Verlengd schutten	1.0
	ONO Sluis - Zoutwaterscheiding	1.0
[KES]	Klanteisen rapportage Bergse Diepsluis	1.0 / 01-08-2019
[KES]	Klanteisen rapportage Zandkreeksluis	
[BopA]	Handboek Architectuur en Installaties BopA	1.0 / 14-04-2021
	RWS MOBZ, Systeemspecificaties MOBZ ¾ Kleine Sluizen	

RWS PPO, Verslag van klantwensgesprek E/IA Bergse
Diepsluis en Zandkreeksluis, Verdieping klantwensen
m.b.t. statussen en logging in SCADA, HB #3768236

06-11-2019

2.4 Onderzoeken en externe besluitvorming

In deze paragraaf worden relevante onderzoeken en externe besluitvorming beschreven welke input leveren voor het ontwerp van dit deelsysteem.

2.4.1 LBS Eisen (Object specifiek)

Voor het overzicht van de geïmplementeerde van de LBS eisen is er een mapping gemaakt met daarin de LBS-eisen per object uit de objectdecompositie van de nautische objecten Bergse Diepsluis en Zandkreeksluis. Daarin is ook aangegeven welke LBS eisen van toepassing zijn welke niet. Deze mapping is als onderdeel van een vooronderzoek door een ingenieursbureau uitgevoerd.

In de volgende fases van het project zal deze tracering verder meegenomen moeten worden. Op die manier kan later aangetoond worden hoe de eisen uit de LBS verwerkt zijn bij de renovatie.

2.5 Overige input

n.v.t.

3 Ontwerp

3.1 Nu en straks

3.1.1

Nu

Tijdens MOBZ fase ½ in de periode 2008 – 2010 zijn bij de vier 'kleine' sluizen (BDS, ZKS, GLS, RPS) [tekst weggelaten omwille van beveiligingsredenen; wordt op verzoek gedeeld na trechtering] Binnen deze producten zijn variaties qua aantallen PLC's, etc. over de nautische objecten. Omdat de gehele besturing en bediening vervangen wordt, zijn deze niet van belang voor het nieuwe ontwerp en worden derhalve in de ontwerp niet gedetailleerd in kaart gebracht. In het technisch dossier MOBZ ½ is meer informatie over de huidige configuraties terug te vinden.

De objecten worden voornamelijk bediend vanuit de Nautische Centrale Neetje Jans, met uitzondering van Sluis Hansweert welke nog lokaal bediend wordt. [tekst weggelaten omwille van beveiligingsredenen; wordt op verzoek gedeeld na trechtering] De installaties zijn einde levensduur en dienen vervangen te worden.

3.1.2

Straks

De functies van het Bedienings- en Besturingssysteem voor het primaire proces zijn niet of nauwelijks aangepast t.o.v. de aanvangssituatie. De huidige functionele werking is aangevuld met gewenste en noodzakelijke aanpassingen vanuit de beheerder en VWM. Deze is beschreven in de CONOPS (Concept of Operations) van het betreffende nautisch object.

Voor beheer en onderhoud is er een significante uitbreiding van de functionaliteiten, zodat deze minimaal in lijn zijn met wat in het project MOBZ fase ¾ is gerealiseerd, plus de recente ontwikkelingen in de LBS, BPP 2.0+ en overige inzichten in efficiënt beheer en onderhoud.

Er is een compleet nieuw Bedienings- en Besturingssysteem opgeleverd door de Opdrachtnemer, gebaseerd op de referentiedocumenten opgesomd in hoofdstuk 2.

Het ontwerp van het Bedienings- en Besturingssysteem van een nautisch object is gebaseerd op het referentieontwerp zoals in deze ontwerpnota is opgenomen.

Voor bediening op afstand is BPP 2.0+ toegepast.

Er worden geen¹ RWS-bouwblokken van het IA Sourcing-programma toegepast of ontwikkeld in het Bedienings- en Besturingssysteem.

3.2 Afbakening en functiebeschrijving objecten

In de deelsysteemontwerpen per nautisch object wordt er een functiebeschrijving gegeven van de objecten.

¹ Het bouwblok Object Data Services (ODS) wordt (als enige RWS-bouwblok) wél toegepast, maar dit valt onder de ontwerpnota's Informatiesysteem.

3.3 Ontwerpbesluiten

Deze paragraaf beschrijft de algemene ontwerpbesluiten zoals deze zijn opgesteld op basis van de volgende input:

- Richtlijn Procesautomatisering,
- LBS kader 12 gerelateerd aan de geëiste MOBZ $\frac{3}{4}$ -architectuur,
- MOBZ 3/4 verbeterpunten,
- KES Nautische objecten,
- Ervaring van de adviseurs IA.

De ontwerpbesluiten dienen ook opgenomen te worden door de Opdrachtnemer in het definitieve ontwerp en gedurende de doorlooptijd van het project aangetoond en gevalideerd te worden. Afwijkingen op deze ontwerpbesluiten zijn alleen na overleg met en goedkeuring van de Opdrachtgever toegestaan.

Nummer	Ontwerpbesluit titel	Revisie Nr.
Dec-0001	Referentie architectuur hardware	0.1
Besluit	De architectuur van de hardware van het bedienings- en besturingssysteem is gebaseerd op de architectuur van MOBZ ¾ (zoals beschreven in TD MOBZ) en op de inrichtingsprincipes van de LBS (zoals beschreven in kader 12): - Definitief ontwerp Sluizencomplex Kreekrak Besturingshardware en Machineveiligheidhardware (TD MOBZ) - Opdeling in systeemplagen, horizontaal (LBS kader 12 par. 6.3.1) - Opdeling in ketens, verticaal (LBS kader 12 par. 6.3.2) - Scheiding in primaire en secundaire keten (LBS kader 12 par. 6.3.3) Hierbij geldt dat de architectuur van MOBZ ¾ prevaleert boven de inrichtingsprincipes van de LBS. Deze keuze is gemaakt om de uniformiteit van technische oplossingen in het areaal te vergroten. Samengevat bestaat deze hardware architectuur uit de volgende besluiten: - Voor het bedieningssysteem ten behoeve van het primaire proces wordt gebruik gemaakt van BPP 2.0+. - Voor het bedieningssysteem ten behoeve van onderhoudsbediening in de technische ruimtes wordt gebruik van separate SCADA-clients (BPO) en van mobile panels (conform MOBZ ¾). - Per machine zoals gedefinieerd in het hoofddocument bij de risicobeoordeling Machineveiligheid wordt een proces-PLC ingezet. - Proces- en veiligheidsfuncties zijn gecombineerd in één proces-PLC waarbij onderscheid is gemaakt in een procesdeel en een veiligheidsdeel (conform B3.3 van kader 12, maar afwijkend van MOBZ 3/4). - Afhankelijk van de beschikbaarheidseisen wordt de proces-PLC redundant gemaakt, dit wordt per nautisch hoofdobject bepaald. De technische beschikbaarheid voor een nautisch object wordt bepaald door de geldende faaldefinities uit de LBS en de ge-eiste prestaties uit de klanteisen. Deze faaldefinities dienen met faalcriteria per functie en logisch object verder te worden uitgewerkt in onderliggende technische specificaties. - Onderhoudsbediening verloopt net als de procesbediening via de procesbesturing. - Om dubbele programma's (ontwerp, realisatie, test, beheer onderhoud) te voorkomen maakt de technische noodbesturing gebruik van de veiligheidsfuncties zoals geïmplementeerd in de veiligheidsdeel van de proces-PLC (afwijkend van B4.8 van kader 12, afwijkend van MOBZ 3/4). In specifieke gevallen kunnen echter eigen sensoren en/of actuatoren nodig zijn, zoals uit een RAMS-analyse moet blijken. - Technische noodbediening vindt plaats m.b.v. mobile panels (conform MOBZ ¾). - De architectuur van de noodstopketen is conform de noodstoparchitectuur uit MOBZ 3/4. - Afhankelijk van de omvang en complexiteit van de utiliteitenbesturing wordt deze onderdeel van de proces-PLC of krijgt deze een separate utiliteiten-PLC. Dit wordt per nautisch object bepaald. De op deze inrichtingsprincipes gebaseerde referentie-architectuur is opgenomen in hoofdstuk 4 van dit ontwerp. Afwijken van deze architectuur is alleen toegestaan na afstemming met Opdrachtgever.	

Nummer	Ontwerpbesluit titel		Revisie Nr.
Dec-0001	Referentie architectuur hardware		0.1
Toelichting			
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat het ontwerp gebaseerd is op de referentie architectuur en is traceerbaar opgenomen waar en waarom hiervan afgeweken is.	
Uitvoeringfase			

Nummer	Ontwerpbesluit titel		Revisie Nr.
Dec-0002	Referentie architectuur software		0.1
Besluit	De architectuur van de software van het bedienings- en besturingssysteem is gebaseerd op de architectuur van MOBZ ¾ (zoals beschreven in TD MOBZ) en op de inrichtingsprincipes van de LBS (zoals beschreven in kader 12): - Definitief ontwerp Sluizencomplex Kreekrak Besturingshardware en Machineveiligheidhardware (TD MOBZ) - Opdeling in systeemlagen, horizontaal (LBS kader 12 par. 6.3.1) - Opdeling in ketens, verticaal (LBS kader 12 par. 6.3.2) - Scheiding in primaire en secundaire keten (LBS kader 12 par. 6.3.3) - Richtlijn Proces Automatisering ZD Hierbij geldt dat de architectuur van MOBZ 3/4 (met daarbij de RPA) prevaleert boven de inrichtingsprincipes van de LBS. Afwijken van deze architectuur is alleen toegestaan na afstemming met Opdrachtgever.		
Toelichting			
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat het ontwerp gebaseerd is op de referentie architectuur en is traceerbaar opgenomen waar en waarom hiervan afgeweken is.	
Uitvoeringfase			

Nummer	Ontwerpbesluit titel		Revisie Nr.
Dec-0003	Integratie bedienplek BPP 2.0+		0.1
Besluit	De procedurele integratie van de bedienplekken voor het primair proces verloopt via in het inkoopproces zoals met ZD A Vaarwegen is afgestemd en nog verder afgestemd moet worden. Voor de technische integratie van deze bedienplekken in de systemen van het nautisch object is de demarcatie zoals in het Handboek Systemen en Installaties [BopA] (het voormalige Handboek BopA) leidend, afwijken hiervan mag alleen na afstemming met Opdrachtgever.		
Toelichting			
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat de integratie van BPP 2.0+ in het ontwerp is opgenomen en afgestemd met ZD A Vaarwegen.	
Uitvoeringfase			

Nummer	Ontwerpbesluit titel		Revisie Nr.
Dec-0004	Opdeling safety en non-safety applicatiesoftware		0.1
Besluit	Safety software ten behoeve van de veiligheidsfuncties, zoals benoemd in de LBS en zoals deze vanuit de risicobeoordeling zijn geïdentificeerd, bevindt zich zo veel als mogelijk alleen binnen de laag Equipment Modules. Deze laag moet duidelijk zichtbaar/aanwijsbaar zijn zodanig dat duidelijk is dat deze gescheiden is van de andere lagen. Alleen op deze laag mogen Equipment Modules horizontaal communiceren. Eisen vanuit verschillende kaders en inputdocumenten (met name LBS en maatregelen / veiligheidsfuncties vanuit risicobeoordelingen) zullen in de laag Equipment Modules geïmplementeerd worden.		
Toelichting	Applicaties t.b.v. veiligheidsfuncties (zowel voor primair proces als voor technische noodbediening) en van het reguliere proces worden geïmplementeerd binnen één proces-PLC. Ten behoeve van structuur en scheiding van belangen is het dan beter om generiek af te spreken waar de verschillende software delen geïmplementeerd moeten worden. De verwachting is dat dit niet altijd één-op-één gaat passen, een voorbeeld hiervan is de veiligheidsfunctie m.b.t. negatief keren. Tijdens de Ontwerpfase moet daarom met de Opdrachtnemer besproken gaan worden wat de beste oplossing voor dit situaties is.		
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat de safety deel zich beperkt tot de equipment module laag. Indien hiervan afgeweken is, is dat traceerbaar in het ontwerp meegenomen.	
Uitvoeringfase			

Nummer	Ontwerpbesluit titel		Revisie Nr.
Dec-0005	Inlezen sensoren en terugmeldingen		0.1
Besluit	Het inlezen van signalen die zowel voor safety als non-safety functies nodig zijn, worden via het safety deel van de PLC doorgestuurd naar het non-safety deel van de PLC. Hetzelfde geldt voor uitgangen die zowel voor safety als non-safety functies nodig zijn: deze worden vanuit het non-safety deel via het safety deel naar de fysieke werktuigen gestuurd		
Toelichting	Eenduidige opzet van de interface tussen veld en besturing		
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat er geen IO dubbel ingelezen of geschreven wordt in meerdere PLC's of in meerdere programma delen.	
Uitvoeringfase			

Nummer	Ontwerpbesluit titel		Revisie Nr.
Dec-0006	Object-georiënteerd programmeren		0.1
Besluit	Er wordt gebruik gemaakt Object Georiënteerd programmeren binnen het PLC programma. Het bewust afwijken hiervan is niet toegestaan. Hierdoor krijgt ieder fysiek object een interface, welke gestandaardiseerd kan worden over het areaal. En ook generiek kan worden toegepast.		
Toelichting	Het verkrijgen van een leesbaar en overzichtelijk PLC programma voor de toekomst om in stand te houden. En is een verdieping van RPA6016 uit de RPA.		
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat object georiënteerd programmeren toegepast gaat worden.	
Uitvoeringfase			

Nummer	Ontwerpbesluit titel		Revisie Nr.
Dec-0007	Software Bibliotheek toepassing		0.1
Besluit	De software objecten die generiek voor de objecten binnen het areaal nodig zijn, dienen ontwikkeld te worden binnen een bibliotheek, waarbij versiewijzigingen vanuit deze bibliotheek kan worden doorgevoerd binnen de geïntanceerde software blokken. Deze worden verder uitgewerkt in de ONO software typicals.		
Toelichting	Het kunnen hergebruiken van software componenten, waardoor de uniformiteit binnen het areaal verbeterd wordt. Ook is versiebeheer hierdoor zeer makkelijk en overzichtelijk uit te voeren in het kader van instandhouding, mochten er nadien nog wijzigingen noodzakelijk zijn aan deze standaard bouwstenen. Te denken bouwstenen die hieronder vallen kunnen zijn: SVS invar, SVS uitvar, LVS, ASB,		
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat er typicals ontworpen zijn conform de ONO software typicals.	
Uitvoeringfase			

Nummer	Ontwerpbesluit titel	Revisie Nr.
Dec-0008	Toepassen van state machines en waarheidstabellen	0.1
Besluit	De software objecten dienen middels state machines aangestuurd te worden. Voor zowel het non-safe als het safe softwaredeel. Hierdoor kan er op een eenduidige manier gewerkt worden dan binnen het PLC programma. Indien er niet met een statemachine gewerkt kan worden mag er gebruik gemaakt worden van waarheidstabellen.	
Toelichting	Transparante en efficiënte manier van het DO omzetten naar UO en programmatie / testen.	
V&V Fase	Methode	Criterium
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat state machines zijn toegepast om de functionaliteit te bewerkstelligen.
Uitvoeringfase		

Nummer	Ontwerpbesluit titel	Revisie Nr.
Dec-0009	1oo2 diagnose safetysoftware	0.1
Besluit	Indien er voor de safety-software een 1 out of 2 evaluatie van IO uitgevoerd dient te worden, dan dient dit binnen in de HW configuratie van de PLC kaart gedaan te worden. Niet middels separate software blokken, wat ervoor zorgt dat extra functieblokken ontwikkeld en onderhouden moeten worden binnen het PLC programma.	
Toelichting	Zo efficiënt mogelijk PLC programma structuur, waarbij duidelijke leesbaarheid voorop staat.	
V&V Fase	Methode	Criterium
Ontwerp		
Uitvoeringfase		

Nummer	Ontwerpbesluit titel	Revisie Nr.
Dec-0010	Demping analoge signaalwaarde	0.1
Besluit	Indien er demping toegepast dient te worden op analoge meetwaarden (bijvoorbeeld kolk niveaumetingen), dient deze demping in de transmitter ingesteld te worden. Alleen gemiddelde waarde mogen in de PLC berekend worden.	
Toelichting	Dit brengt eenvoud en overzicht in de PLC configuratie. Dit aspect moet wel in relatie met onderhoudbaarheid beschouwd te worden, transmitters moeten dan wel goed bereikbaar zijn (fysiek of via netwerk).	
V&V Fase	Methode	Criterium
Ontwerp		
Uitvoeringfase		

Nummer	Ontwerpbesluit titel	Revisie Nr.
Dec-0011	Digitaal ingangssignaal vertraging	0.1
Besluit	Indien er een vertraging op een digitaal signaal toegepast dient te worden, ten behoeve van een denderend contact. Dient dit bij voorkeur in de hardware configuratie van de IO-kaarten geconfigureerd te worden.	
Toelichting	Dit brengt eenvoud en overzicht in de PLC configuratie	
V&V Fase	Methode	Criterium
Ontwerp		
Uitvoeringfase		

Nummer	Ontwerpbesluit titel		Revisie Nr.
Dec-0012	Doorsturen diagnostische gegevens		0.1
Besluit	De diagnostische gegevens van de PLC's, en onderliggend IO-netwerken inclusief componenten dient doorgestuurd te worden naar een lange termijn opslag.		
Toelichting	Borgen dat onderhoudsinformatie voor een langere periode beschikbaar is, zodat er goede analyses uitgevoerd kunnen worden.		
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat alle mogelijke diagnostische gegevens doorgestuurd en opgeslagen worden. Alsmede dat deze raadpleegbaar zijn voor storingsanalyse.	
Uitvoeringfase			

Nummer	Ontwerpbesluit titel		Revisie Nr.
Dec-0013	Gegevens uitwisseling SCADA		0.1
Besluit	De SCADA-systemen kunnen informatie direct uit de componenten uitlezen, dit hoeft niet doorgegeven te worden via de verschillende lagen van de bovenliggende software blokken in de besturingssoftware.		
Toelichting	De bediening en gegevens uitwisseling van bijvoorbeeld het software blok van de afsluitboom, zal direct met het MMI plaatsvinden, dit hoeft niet via het softwareblok afsluitbomen algemeen, brug, enz. naar boven doorgegeven te worden alvorens het naar het MMI gestuurd wordt.		
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat de gegevens niet getunneld doorgestuurd worden naar en van het MMI.	
Uitvoeringfase			

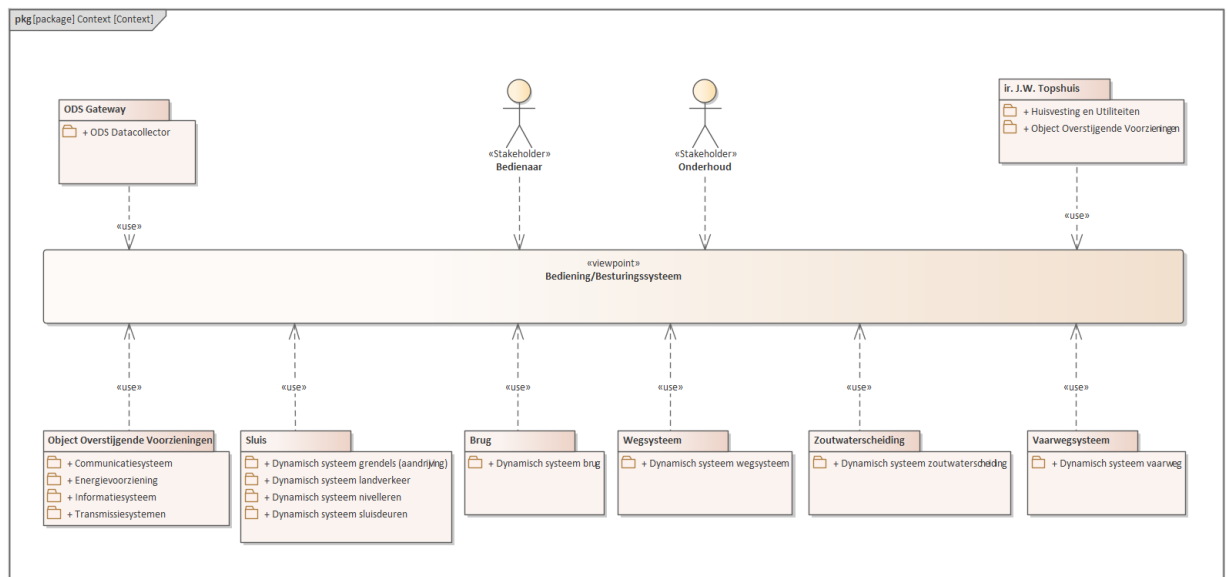
3.4 Eisen uit de LBS

Vanuit de LBS zijn veel eisen gealloceerd aan het Bediening en Besturing. Ten behoeve van de leesbaarheid zijn niet al deze eisen in deze ontwerpnota herhaald. In het overzicht met de verwerking van de LBS-eisen is aangegeven hoe de eisen verwerkt zijn of nog moeten gaan worden. Hierbij zijn de volgende verwerkingsmethodes gehanteerd:

- Eisen welke behoren bij deze ontwerpnota hebben als opmerking "Verwerkt in ontwerpnota ALG Bediening en Besturing", indien nodig is een verdere verduidelijking toegevoegd.
- Eisen welke behoren bij de bedienplekken of richtlijnen procesautomatisering zijn gealloceerd aan de virtuele deelsystemen "BPP 2.0" of "Richtlijnen PA / E / Styleguide"

3.5 Beschouwing raakvlakken

De raakvlakken voor het Bediening/Besturingssysteem zijn weergegeven in onderstaand figuur. De raakvlakken vanuit deze systemen zijn beschreven in de ontwerpnota's van de betreffende (dynamische) systemen en derhalve niet in deze ontwerpnota beschreven. Alleen het totaal overzicht is visueel weergegeven.



Figuur 4: Raakvlakken voor het Bediening/Besturingssysteem

4 Output

Hieronder wordt de output beschreven. Dit wordt gezien als het voorlopig ontwerp/referentieontwerp van dit deelsysteem. De output is *uitdrukkelijk geen compleet ontwerp* en moet altijd in samenhang met de scope en klanteisen beschouwd worden.

4.1 Specificaties

Hieronder staan de algemene outputspecificaties bij dit voorontwerp inclusief de verificatievoorschriften beschreven.

Bron	Specificatie titel		Revisie Nr.
n.v.t.	Bediening en signalering		0.1
Specificatie	Vanuit de ontwerpnota's van de verschillende dynamische systemen wordt globaal het raakvlak tussen deze systemen en Bediening en Besturing beschreven. Het gaat dan vooral om welke bedieningen mogelijk moeten zijn. Deze bedieningen zijn meer in detail beschreven in Bijlage A Systemen versus bedienvormen. Deze moet als basis gebruikt worden voor de verdere invulling in het ontwerp. Als het gaat om de signaleringen op de bedienschermen voor primair proces en voor onderhoud moeten de styleguide voor primair proces (onderdeel van LBS) en de styleguid voor beheer en onderhoud (document [SGBPO]) toegepast worden.		
Toelichting			
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat de signaleringen op bedienschermen gebaseerd zijn op de genoemde styleguides.	
Realisatie			
Oplevering			

Bron	Specificatie titel		Revisie Nr.
KES-0698	Functionele instandhouding		0.1
Specificatie	De componenten van het Bedienings- en Besturingssysteem dienen door de Opdrachtgever zo veel als mogelijk voorzien te kunnen worden van patches, updates en uitbreidingen zonder dat het nautische object daarvoor gestremd dient te worden. Dit omvat ook de firmware van de desbetreffende componenten.		
Toelichting			
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat updates en de mogelijkheid voor uitbreidingen meegenomen is in de ontwerpkeuzes.	
Realisatie			
Oplevering			

Bron	Specificatie titel		Revisie Nr.
KES-0497, KES-0698	Uniforme componenten		0.1
Specificatie	De Bedienings- en Besturingssystemen over de verschillende sluiscomplexen dienen zoveel mogelijk uniforme hardware te bevatten om de voor instandhouding benodigde kennis en reservematerialen beperkt te houden. Voor componenten met gelijke functionaliteit en eisen dient hetzelfde merk en type gekozen te worden. Het Bediening- en Besturingssysteem sluiscomplex dient uitgevoerd te worden met I/O modules die voldoen aan de gestelde/afgeleide eisen voor beschikbaarheid, veiligheid (SIL) en toepassing/functie. Er mogen geen verschillende fabricaat en type I/O modules voor I/O met gelijkwaardige eisen/functie worden toegepast (uniformiteit).		
Toelichting	Dit is een uitbreiding van RPA6034 uit de RPA		
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat identieke componenten gebruikt zijn door het project, voor dezelfde functionaliteiten.	
Realisatie			
Oplevering			

Bron	Specificatie titel		Revisie Nr.
	PLC onafhankelijkheid		0.1
Specificatie	Als een nautisch object uit meerdere onafhankelijke delen bestaat, bijvoorbeeld twee sluiscolken moeten de componenten hiervan niet gecombineerd worden. De PLC's van deze delen moeten onafhankelijk van elkaar kunnen werken: er kan één PLC uitgeschakeld worden, waarbij de andere PLC volledig in dienst en bedienbaar blijft. Als een nautisch object uit een brug-sluisc-combinatie bestaat, waarbij de brug nodig is voor het sluisproces, moet dit principe, naast het enkelvoudig aansturen van systeemdelen, zoveel mogelijk aangehouden worden. Daarnaast geldt voor utiliteiten en andere overkoepelende installaties dat deze onafhankelijk van brug of kolk onderhouden moeten kunnen worden. Echter als blijkt dat voor dit soort systeemdelen maar enkele signaleringen of bedieningen nodig zijn, kan in gezamenlijk overleg besloten worden deze in de PLC van brug of kolk op te nemen.		
Toelichting	De afhankelijke systeemdelen zijn dan in de praktijk meestal de scheepvaartseinen.		
V&V Fase	Methode	Criterium	
Ontwerp	Document inspectie	Uit ontwerpdocumentatie blijkt dat de (on)afhankelijkheid van systeemdelen in de ontwerpkeuzes zijn meegenomen.	
Realisatie			
Oplevering			

4.2 Referentie ontwerp

In de bijlagen B en C is het referentieontwerp van de hardware en software weergegeven gebaseerd op ontwerpbesluiten zoals deze gedefinieerd zijn op basis van de MOBZ 3/4 configuratie en de architectuurprincipes uit de LBS.

4.3 Raakvlakken

4.3.1 Deelsystemen

Het raakvlak tussen het besturingssysteem en de onderliggende dynamische systemen wordt gevormd door de interface met inkomende en uitgaande signalen op de IO-rekken en andere netwerkinterfaces. Alle signalen op deze interface worden afgestemd en beheerd vanuit het deelsysteem Bedienings- en Besturingssysteem en daarmee door de partij die dit systeem ontwerpt en realiseert.

4.4 Aandachtspunten voor het proces

Hieronder staan kort enkele relevante aandachtspunten beschreven voor het ontwerp- en realisatieproces.

Handelingen en procedures Noodbediening in handleiding

Alle handelingen en procedures benodigd voor de noodbediening moeten duidelijk beschreven zijn in de bedienhandleiding.

De Opdrachtnemer dient alle technische en procedurele randvoorwaarden voor het uitvoeren van Noodbediening in de Bedienings- en Onderhoudshandleiding vast te leggen.

Verificatievoorschriften

Bij het ontwikkelen en opleveren van technische systemen is er in meer of mindere mate sprake van 'testen'. Afhankelijk van de rol, specialisme, ervaring, projectfase of simpelweg (geen) afspraken kan er een verschil in opvattingen en verwachtingen bij het 'testen' zijn. Om de testaanpak voor een ieder helder te hebben wordt door Opdrachtnemer een testplan opgesteld.

Tenminste de volgende testsoorten worden daarbij onderscheiden;

1. Unit- en systeemtest (al dan niet geautomatiseerd)
2. FAT (acceptatietest per deelsysteem bij de Opdrachtnemer)
3. IFAT (integratie van deelsystemen)
4. SRECS (per veiligheidsfunctie)
5. iSRECS (integratie van veiligheidsfuncties)
6. IO test (interfacetest tussen dynamische systemen en besturingssysteem)
7. SAT (acceptatietest op nautisch object)
8. SIT (integratietest van techniek, operationeel en processen)

Enkele van deze testen zijn al voorgeschreven door de IEC-61508 en IEC-61131-3.

Door het geautomatiseerd testen kan er snel en veel getest worden, de testen worden consequent hetzelfde uitgevoerd en niet afhankelijk van een tester welke een protocol dient te volgen. Na een software update kan er dan direct snel een nieuwe test uitgevoerd worden.

Het geautomatiseerd testen kan bijvoorbeeld uitgevoerd worden met behulp van de Siemens TIA portal Test Suite, of vergelijkbare software van een andere leverancier.

De IFAT omgeving dient representatief te zijn aan de uiteindelijke opstelling van het Nautische Object. Deze test opstelling minimaal moeten bestaan uit de definitieve SCADA omgeving, definitieve representatieve netwerk architectuur, PLC CPU's fysiek toegepast, de Remote IO hoeft niet fysiek aanwezig te zijn en mag gesimuleerd worden. Dit bijvoorbeeld met een Siemens SIMIT UNIT-PN256 of vergelijkbare oplossing.

RAMS

Het deelsysteem moet voldoen aan de veiligheidseisen, waarbij de beschikbaarheid en onderhoudbaarheid van het nautisch object geborgd blijft. FMECA-sessies en toepassen van faaldefinities zijn hiervoor een middel om de robuustheid van het systeem te beoordelen en maatregelen hiervoor op te stellen. Aan deze FMECA-sessies wordt door verschillende stakeholders deelgenomen, dit wordt afgestemd met Opdrachtgever.

Omdat vanuit de klanteisen geen kwantitatieve getallen zijn gevraagd in het kader van RAMS worden deze dan ook niet gemaakt. Kwalitatieve analyses geven, mits goed uitgevoerd, veel meer resultaat en garantie op een robuust, onderhoudbaar en veilig systeem.

De Opdrachtnemer dient de V&V criteria bij zowel de ontwerpbeslissingen als de specificaties tijdens de DO fase in/aan te vullen. Zodat er een verificatie matrix opgeleverd kan worden gedurende het project om de aantoonbaarheid te kunnen borgen.

4.5 Kansen en risico's

4.5.1 Kansen

Onderstaande kansen werden gezien tijdens het ontwerptraject.

- Gebruik van een **OntwikkelTestAcceptatieProductie** (OTAP) omgeving
- Automatisch uitvoeren van unit testen
- Gebruik van Enterprise Architect tijdens de ontwerpfase, voor het snel en consistent opbouwen van een ontwerp document.
- Het opbouwen van een Bibliotheek voor software objecten, hierdoor ontstaat er een kans voor standaardisatie en uniformiteit in het areaal als deze ook in andere projecten toegepast worden.
- Visueel software ontwerp voor doorgronding van het programma, dit zorgt voor een beter inzicht en herbruikbaarheid bij andere Nautische Objecten.

4.5.2 Risico's

Onderstaande risico's gelden voor het project.

- Hergebruiken van bestaande MOBZ 3/4 bibliotheek of SCADA blokken en die aanpassen naar nieuwe look/and feel. Hierdoor blijf je met oude PLC functies achter en worden niet de laatste nieuwe technologieën gebruikt.

4.6 BTO-keuzes

Bouwkundige, technische en organisatorische (BTO) keuzes beschreven t.b.v. het V&G-plan zijn opgenomen in document HB 3689083.

5 Openstaande punten

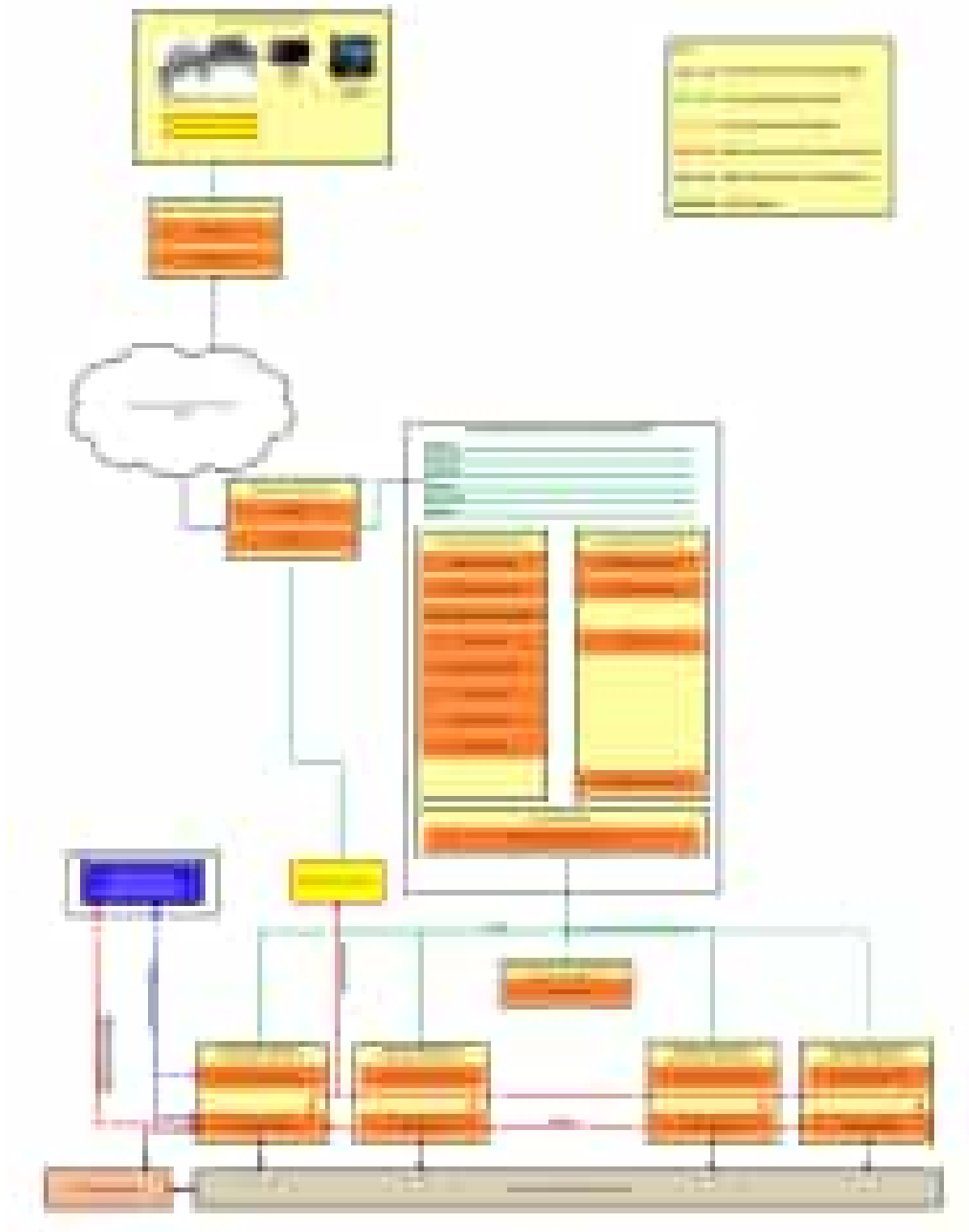
Onderstaande punten betreffende het ontwerp van dit deelsysteem staan nog open.
Dit kan als actielijst gezien worden.

A Systemen versus bedieningen

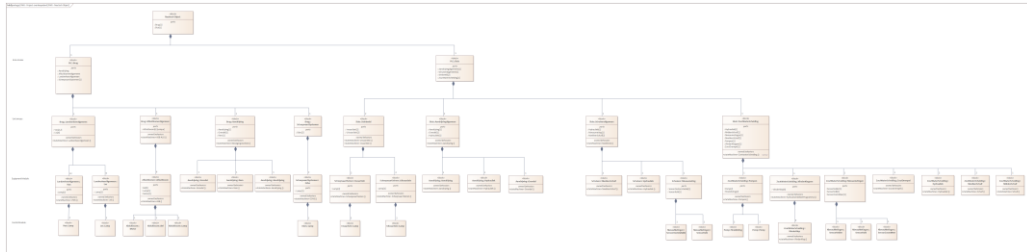
Zie bijgevoegde Excel "Systemen versus bedienvormen.xlsx".

B Referentie ontwerp hardware Bediening en Besturing

[afbeelding vervaagd omwille van beveiligingsredenen; wordt op verzoek gedeeld na trechtering]



C Referentie ontwerp software Bediening en Besturing



Deze figuur is ook in het model en als separate uitdraai uit het model beschikbaar.

PPO ZD B Sluizen

Versie 1.0 - 22 april 2021

Beschouwde varianten: Bergse Diepsluis, Zandkreeksluis, Roompotsluis, Grevelingensluis, Sluis Hansweert

Aandrijvingen:

Hoofdaandrijving: aandrijving welke via de reguliere besturing kan gebruikt worden om het bewegingswerk aan te drijven.

Primaire vermogensleverancier: deze wordt standaard gebruikt; voor onderhoud kan deze soms in tragere snelheid gebruikt worden.

Reserve vermogensleverancier: deze wordt gebruikt als de primaire faalt of om onderhoud uit te voeren; vaak heeft deze licht functieverlies (trager)

Noodaandrijving machinaal: aandrijving welke buiten de reguliere besturing kan gebruikt worden om het bewegingswerk in veilige toestand te brengen.

Niet elke aandrijving is op elk bewegingswerk aanwezig. Als dit er niet is en niet gevraagd is vanuit de scope/klanteisen, zal die er ook niet komen.

N	Nee, niet nodig/aanwezig
J	Ja, nodig/aanwezig
✓	Verplicht vanuit LBS/klanteisen/uniformiteit met MOBZ 3/4
?	Onbekend/ontwerpvrijheid/afhankelijk van onderzoek machineveiligheid
NN	Nee, hier wijken we af van de LBS/MOBZ 3/4

[volgende 3 pagina's weggelaten omwille van beveiligingsredenen; wordt op verzoek gedeeld na trechtering]

