

Producteisen

Behorend bij Nadere Overeenkomst 1 vallend onder de Raamovereenkomst 3B

30 september 2026

Kenmerk <NOK1 Producteisen v1.0 30-09-2026 definitief>

Versie 1.0

Definitief

bronversie Format A-302 v20260115

1	Inleiding	3
1.1	Algemene bepalingen	3
1.2	Standaard bouwdelen (typicals)	5
1.3	CCTV	5
1.4	Lokale bedienlessenaar	5
1.5	Cybersecurity en informatiebeveiliging (ICO)	6

1 Inleiding

In dit document zijn de producteisen opgenomen waar in de uitvoering van de Nadere Overeenkomst 1 vallend onder de Raamovereenkomst 3B aan dient te worden voldaan. Door het indienen van uw inschrijving voor deze opdracht verklaart u onvoorwaardelijk akkoord te gaan met ALLE eisen aan de opdracht.

De eisen zijn thematisch gegroepeerd in paragrafen. De volgorde van de paragrafen is willekeurig.

1.1 Algemene bepalingen

1.	De Technische Standaard 3B dient opgesteld te worden overeenkomstig de volgende referentiedocumenten: [Basisbeschrijving Functioneel] [Bedienfilosofie] [Uitwerking bedienfilosofie] [Ontwerp Bediencentrale - ergonomie] [OT Architectuur] Zie het overzicht van referenties in paragraaf 1.2 in het beschrijvende deel bij deze eisenspecificatie.
2.	De Technische Standaard 3B omvat minimaal uitleg, toelichting en instructie met betrekking tot de volgende zaken: - architectuurprincipes - netwerksegmentatie - naamgevingsconventies - programmeer- en ontwerprichtlijnen - HMI/SCADA-uitgangspunten - versie- en patchbeleid - logging - back-up - test- en releaseafspraken - documentatiesjablonen - cybersecurity-baseline.
3.	De Technische Standaard 3B dient dusdanig versiebeheer te hebben dat bij toepassing van de Technische Standaard 3B op een object deze eenduidig herleidbaar is naar 1 specifieke versie.
4.	Voortschrijdend inzicht en ontwikkeling van de Technische Standaard 3B dient efficiënt en gecontroleerd implementeerd te kunnen worden.
5.	De Technische Standaard 3B dient dusdanig te zijn opgesteld dat deze toekomstige ontwikkelingen kan adopteren zonder dat dit direct vergaande impact heeft op de Technische Standaard 3B als geheel.
6.	De Technische Standaard 3B dient bij te dragen aan een goed beheerbare en uniform werkende bediening.
7.	De Technische Standaard 3B dient te voldoen aan Wet- en regelgeving waaronder de Machineverordening 2023/1230.

8.	De Technische Standaard 3B dient een robuuste koppeling tussen bediencentrale en objecten te realiseren, dusdanig dat het wegvallen van de koppeling tussen bediencentrale en object: - geen impact heeft op de mogelijkheden om vanuit de bediencentrale andere objecten te bedienen - geen impact heeft op de mogelijkheden om het object lokaal te bedienen - zelfstandig kan herstellen als aan de benodigde randvoorwaarden is voldaan - niet leidt tot gevaarlijke situaties
9.	De Technische Standaard 3B dient geschikt te zijn om de processen omschreven in [Bedienfilosofie] te realiseren
10.	De Technische Standaard 3B dient te passen binnen de kaders die voor bedienplekken zijn vastgesteld in [Ontwerp Bediencentrale - ergonomie]
11.	De Technische Standaard 3B dient vast te stellen hoe en waar de instellingen en parameters van de automatisering worden vastgelegd en beheerd.
12.	De Technische Standaard 3B dient de inrichting van instellingen en parameters zo te specificeren dat deze eenduidig, beheerbaar en zo min mogelijk versnipperd is.
13.	Ten behoeve van beheer, diagnose en herstel dienen relevante instellingen, parameters en back-ups centraal inzichtelijk en beheerbaar te zijn.
14.	De Technische Standaard 3B dient te zijn voorzien van diagnosefunctionaliteit waarin de technische status van de afzonderlijke systeemcomponenten is in te zien.
15.	Diagnosefuncties dienen in de bediencentrale vanaf een aparte bedienplek (terminal) benaderbaar te zijn. Dit moet middels gecontroleerde, beveiligde toegang volgens een met Opdrachtgever overeen te komen architectuur. Vanuit cyber security oogpunt mag deze functie niet via het internet benaderbaar zijn.
16.	De processen van de Technische Standaard 3B dienen aan te sluiten bij de ontwerpprocessen conform NEN-EN-ISO 12100
17.	De netwerkarchitectuur dient opgesteld te zijn op basis van PERA (Purdue) en zones & conduits conform IEC 62443
18.	In de gerealiseerde software dient duidelijk herkenbaar te zijn welke delen conform de Technische Standaard 3B zijn en welke delen brugspecifiek zijn.
19.	De Technische Standaard 3B dient toegepast te worden op zowel de bediencentrale als de afzonderlijke bruggen.
20.	Het ontwerp van de Technische Standaard 3B dient te voldoen aan NEN-EN-IEC 62061:2021
21.	Opdrachtnemer dient in de toepassing van NEN-EN-IEC 62061:2021 per veiligheid-gerelateerde functie van het 3B systeem een gepast Safety Integrity Level (SIL) overeen te komen met Opdrachtgever. Opdrachtnemer doet daartoe bij de indiening van het "Voorlopig Ontwerp (VO) van de systeemarchitectuur van de Technische Standaard 3B" (zie voorgeschreven milietones in de projectplanning) een onderbouwd voorstel aan Opdrachtgever.
22.	De Technische Standaard 3B inclusief de daarin gespecificeerde bouwdelen (typicals) dient te voldoen aan NEN-EN-IEC 60204-1:2018 nl
23.	De Technische Standaard 3B dient te voldoen aan NEN 6787-1:2025 nl
24.	Het 3B systeem dient functioneel uitbreidbaar te zijn met nieuwe functionaliteiten die gangbaar zijn in de markt voor vergelijkbare systemen.
25.	Het 3B systeem dient uitbreidbaar te zijn zodat nieuwe objecten (bijv. een sluis) daaraan kunnen worden toegevoegd.
26.	De status- en bedieninformatie van de afzonderlijke bruggen dient beschikbaar gesteld op een netwerkcontactpunt in de controlekamer van de bediencentrale waar later een planbord op kan worden aangesloten.

1.2 Standaard bouwdelen (typicals)

27.	De nieuw te installeren bouwdelen (typicals) dienen "proven technology" te zijn. Dat wil zeggen dat deze elders in Nederland reeds worden toegepast en waar Opdrachtnemer op verzoek van Opdrachtgever minimaal 3 positieve referenties van gebruikers (bedrijven, overheden, infrabeheerders etc.) kan overleggen.
28.	Opdrachtnemer toont met bewijsstukken van haar OEM aan dat de toegepaste bouwdelen (typicals) minimaal tot 10 jaar na indienststelling zullen worden ondersteund (d.w.z. dat er een storingsdienst is die kan worden geraadpleegd en dat bouwdelen kunnen worden geleverd).
29.	Opdrachtnemer dient uitsluitend bouwdelen (typicals) toe te passen van OEM's die een vertegenwoordiging hebben die in staat is om in de Nederlandse taal technisch ondersteuning te bieden aan Opdrachtnemer en Opdrachtgever.
30.	Opdrachtnemer dient uitsluitend bouwdelen (typicals) toe te passen waarvoor in Nederland minimaal 3 (drie) System Integrators zijn die betreffende bouwdelen (typicals) van de betreffende OEM kunnen implementeren en beheren.
31.	De veiligheidsfuncties dienen gescheiden te zijn van de reguliere besturingsfuncties en te worden gevalideerd conform de vastgestelde SIL-eisen. Alle veiligheidsfuncties dienen separaat geprogrammeerd en uitgevoerd te zijn middels een nieuwe safety PLC met eigen failsafe I/O's.
32.	De aangeboden veiligheidsbesturing, waaronder de veiligheids-PLC, dient geschikt te zijn voor het realiseren van veiligheidsgelateerde functies tot ten minste SIL 2 overeenkomstig NEN-EN-IEC 62061:2021. Indien uit de risicobeoordeling voor een specifieke veiligheidsfunctie een hoger SIL volgt, dient Opdrachtnemer inzichtelijk te maken welke aanvullende maatregelen noodzakelijk zijn om dit niveau te realiseren.

1.3 CCTV

33.	Het videosysteem dient alle beelden gedurende 28 dagen te kunnen opslaan.
34.	Het videosysteem dient daartoe bevoegde gebruikers de mogelijkheid te bieden opgeslagen beelden terug te kijken en veilig te stellen.
35.	Het videosysteem dient opgeslagen beelden, met uitzondering van veiliggestelde beelden, automatisch na een configureerbare periode te wissen.
36.	Het videosysteem dient geen koppeling te hebben naar systemen buiten het OT-domein. Het moet mogelijk zijn om de opgeslagen beelden te kopiëren naar een USB stick.

1.4 Lokale bedienlessenaar

37.	De response van de brug op de bedienhandelingen vanaf de lokale bedienlessenaar (welke niet wordt vernieuwd) dient na installatie van de nieuwe 3B componenten hetzelfde te zijn als die van de huidige 3B installatie.
38.	De Technische Standaard 3B moet voorzien in voorschriften voor ontwerp, installatie, gebruik en beheer van de lokale bedienlessenaren van de 6 bruggen waarmee deze in lijn worden gebracht met de nieuwe bedienfilosofie zoals deze binnen NOK1 wordt gerealiseerd op de bediencentrale.

1.5 Cybersecurity en informatiebeveiliging (ICO)

39.	De ICT en IA van het beheerobject dient zodanig te zijn ingericht en onderhouden, dat gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.	Voorkomen van schade	VSP/VSE-eisen CSIR3.34
40.	De ICT en IA van het beheerobject dient daar waar direct of indirect verwezen wordt naar de specifieke implementatie-richtlijnen uit de [Cybersecurity Implementatierichtlijn Objecten] te voldoen aan het Cybersecurity weerstandsniveau [NTB]. Beheerobject "Bediencentrale" – cybersecurity weerstandsniveau 2 (twee) Beheerobject "Brug" - cybersecurity weerstandsniveau 1 (één)	Toepassing cybersecurity weerstandsniveau	VSP/VSE-eisen CSIR3.33
41.	De ICT en IA van het beheerobject dient zodanig te zijn gerealiseerd dat de beveiliging van de ICT en IA volgens het principe van gelaagde beveiliging is ingericht.	Gelaagde beveiliging beheerobject	VSP/VSE-eisen CSIR3.32
42.	Maximale hardening conform de maatregelen uit paragraaf 2.5.2 "Hardening" en bijlage CSR9 "Hardening" van de [Cybersecurity Implementatierichtlijn Objecten] dient aangehouden te zijn voor de (rand)apparatuur en delen van de datanetwerkinfrastructuur van waaruit remote beheer en onderhoud wordt uitgevoerd aan de ICT en IA van het beheerobject.	Hardening	VSP/VSE-eisen CSIR3.31
43.	Voor de ICT en IA van het beheerobject dienen voor de identificatie, authenticatie en autorisatie maatregelen geïmplementeerd te worden conform paragraaf 2.2 "Maatregelen logische toegang" van de [Cybersecurity Implementatierichtlijn Objecten].	Toegangsmaatregelen beheerobject	VSP/VSE-eisen CSIR3.30
44.	Voor de ICT en IA van het beheerobject dienen de eisen en functionaliteit ten aanzien van wachtwoorden conform bijlage CSR 7 "Wachtwoorden" van de [Cybersecurity Implementatierichtlijn Objecten] gevolgd te worden.	Wachtwoordeisen beheerobject	VSP/VSE-eisen CSIR3.29
45.	Voor de ICT en IA van het beheerobject dienen bij inzet van versleuteling ter bescherming van de vertrouwelijkheid, authenticiteit en/of integriteit maatregelen getroffen te worden conform paragraaf 2.4.2 "Cryptografie" van de [Cybersecurity Implementatierichtlijn Objecten].	Cryptografie beheerobject	VSP/VSE-eisen CSIR3.28
46.	Voor de ICT en IA van het beheerobject dient bij inzet van versleuteling alleen gekozen te worden voor de versleuteling, de onderliggende algoritmes en instellingen met uitsluitend de duiding "goed", zoals aangegeven in het NCSC document [Richtlijnen voor Transport Layer Security].	Sterke encryptie beheerobject	VSP/VSE-eisen CSIR3.27

47.	Voor de ICT en IA van het beheerobject dient bij inzet van versleuteling gebruik gemaakt te worden van: - PKI-Overheid certificaten voor communicatie met externe netwerken; - Organisatie eigen interne PKI certificaten voor communicatie met interne netwerken	Gebruik van Certificaten beheerobject	VSP/VSE-eisen CSIR3.26
48.	De fysieke beveiliging van het terrein en gebouwen hierbinnen behorende bij het beheerobject dienen conform paragraaf 2.1.2 "Fysieke beveiliging terrein en gebouwen" en CSR 24 "Fysieke beveiligingsmaatregelen" ingevuld te worden.	Fysieke beveiliging omgeving beheerobject	VSP/VSE-eisen CSIR3.25
49.	De fysieke toegangsbeveiliging van ICT en IA gerelateerde ruimten (waaronder Bedienruimte en Technische Ruimten) van het beheerobject dient ingericht te zijn conform paragraaf 2.1.1 "Maatregelen Fysieke toegangsbeveiliging IA-gerelateerde ruimten" van de [Cybersecurity Implementatierichtlijn Objecten].	Fysieke beveiliging gerelateerde ruimten beheerobject	VSP/VSE-eisen CSIR3.24
50.	ICT en IA van het beheerobject dient tegen schade en storing beschermd te zijn.	Bescherming ICT en IA beheerobject	VSP/VSE-eisen CSIR3.23
51.	De ICT en IA van het beheerobject dient, indien geplaatst buiten beveiligde gebouwen en ruimten, op basis van een risico analyse en afweging geplaatst te zijn in afsluitbare kasten of ruimten, die bij fysieke opening een alarmmelding genereren, die opgevolgd wordt, evenals bij ongeautoriseerde logische toegang tot het datanetwerk in de kast of ruimte.	Alternatieve maatregelen onbeveiligde ruimten	VSP/VSE-eisen CSIR3.22
52.	Voedings- en telecommunicatiekabels van het beheerobject die voor dataverkeer of ondersteunende informatiediensten zijn toegepast dienen tegen interceptie, verstoring of schade beschermd te zijn.	Beveiliging voeding en telecom beheerobject	VSP/VSE-eisen CSIR3.21
53.	De Ontwikkel-, Test-, Acceptatie-, Productie-, en Leeromgeving van het beheerobject dient gescheiden te zijn om het risico van onbevoegde toegang tot of veranderingen aan de productie omgeving te verlagen.	Segmentering omgevingen beheerobject	VSP/VSE-eisen CSIR3.20
54.	De ICT en IA van het beheerobject dient beschermd te zijn tegen malware conform de maatregelen uit paragraaf 2.5.1 "Anti-malware" en bijlage CSR 11 "Malware scanning en opschoning middels een USB" van de [Cybersecurity Implementatierichtlijn Objecten].	Malwarebescherming beheerobject	VSP/VSE-eisen CSIR3.19
55.	De ICT en IA van het beheerobject dient gehardend te zijn conform de maatregelen uit paragraaf 2.5.2 "Hardening" en bijlage CSR 9 "Hardening" van de [Cybersecurity Implementatierichtlijn Objecten].	Hardening beheerobject	VSP/VSE-eisen CSIR3.18

56.	De ICT en IA van het beheerobject dient gepatcht te zijn conform de maatregelen uit paragraaf 2.5.3 "Patching" en bijlage CSR 8 "Patch management" van de [Cybersecurity Implementatierichtlijn Objecten].	Patchmanagement beheerobject	VSP/VSE-eisen CSIR3.17
57.	De integriteit en beschikbaarheid van de ICT en IA van het beheerobject dient geborgd te zijn doormiddel van back-ups conform paragraaf 2.10 "Maatregelen back-ups" en bijlage CSR 18 "Back-up en recovery" van de [Cybersecurity Implementatierichtlijn Objecten].	Back-up en recovery beheerobject	VSP/VSE-eisen CSIR3.16
58.	De ICT en IA van het beheerobject dient de activiteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen vast te leggen in logbestanden conform paragraaf 2.6 "Maatregelen logging en monitoring" en bijlage CSR 10 "Logging" van de [Cybersecurity Implementatierichtlijn Objecten].	Logging en monitoring beheerobject	VSP/VSE-eisen CSIR3.15
59.	Voor de ICT en IA van het beheerobject dient een (centrale) syslog server ingericht te zijn die syslog events verzamelt en toegankelijk maakt voor analysedoeleinden en automatische waarschuwingen door een Security Information en Event Management (SIEM) systeem en/of een Security Operations Centre (SOC) conform paragraaf 2.6 "Maatregelen logging en monitoring" en bijlage CSR 10 "Logging" van de [Cybersecurity Implementatierichtlijn Objecten].	systeemlogging beheerobject	VSP/VSE-eisen CSIR3.14
60.	De ICT en IA van het beheerobject dient technisch te zijn voorbereid op monitoring middels detectievoorzieningen van het Security Operations Centre (SOC) van Opdrachtgever conform paragraaf 2.6 "Maatregelen logging en monitoring" van de [Cybersecurity Implementatie Richtlijn Objecten].	Detectievoorzieningen beheerobject	VSP/VSE-eisen CSIR3.13
61.	Het objectdatanetwerk van het beheerobject dient uitgevoerd te zijn met analysepoorten door poorten in het lokale objectdatanetwerk tot analyse poort te configureren.	Configuratie analysepoorten	VSP/VSE-eisen CSIR3.12
62.	De datanetwerkkoppelingen van het beheerobject dienen uitgevoerd te zijn conform paragraaf 2.4.1 "Netwerkkoppelingen" en bijlage CSR 3 "Architectuur objectnetwerk" van de [Cybersecurity Implementatierichtlijn Objecten].	Datanetwerkkoppelingen beheerobject	VSP/VSE-eisen CSIR3.11
63.	Alle datanetwerkverbindingen van het beheerobject dienen strikt en uitsluitend te verlopen via centrale beveiligde voorzieningen. Directe vaste of draadloze datanetwerkverbindingen met andere datanetwerken dan die van Opdrachtgever zijn strikt verboden.	beveiligde verbindingen beheerobject	VSP/VSE-eisen CSIR3.10

64.	Het aantal ICT en IA datanetwerkkoppelingen van het beheerobject met andere externe datanetwerken dient geminimaliseerd te zijn.	Minimalisatie verbindingen beheerobject	VSP/VSE-eisen CSIR3.9
65.	Draadloze netwerken van het beheerobject zijn ingericht conform paragraaf 2.4.2 "Cryptografie" en bijlage CSR 5 "Draadloze netwerken" van de [Cybersecurity Implementatierichtlijn Objecten].	Cryptografie draadloze netwerken beheerobject	VSP/VSE-eisen CSIR3.8
66.	Voor de ICT en IA van het beheerobject dient gebruik te zijn gemaakt van een gecompartmenteerde datanetwerk dat van de kantoorautomatisering is gescheiden. De scheiding kan fysiek of logisch zijn.	Segmentering datanetwerk beheerobject	VSP/VSE-eisen CSIR3.7
67.	Voor de ICT en IA van het beheerobject dient segmentering van dataverkeersstromen toegepast te zijn voor Ontwikkel-, Test-, Acceptatie-, Productie-, Leer- en Beheeromgeving.	Segmentering datastromen omgevingen beheerobject	VSP/VSE-eisen CSIR3.6
68.	De ICT en IA datanetwerken van het beheerobject dienen ingericht te zijn conform paragraaf 2.4.1 "Netwerkkoppelingen" en bijlage CSR 3 "Architectuur objectnetwerk" van de [Cybersecurity Implementatierichtlijn Objecten].	Inrichting datanetwerken beheerobject	VSP/VSE-eisen CSIR3.5
69.	ICT en IA van het beheerobject dient voorzien te zijn van invoer en uitvoer validatie controles om corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken.	Invoer/uitvoer controles beheerobject	VSP/VSE-eisen CSIR3.4
70.	ICT en IA van het beheerobject dient voor beheer en onderhoud ingericht te zijn conform paragraaf 2.9 "Maatregelen beheer en onderhoud" van de [Cybersecurity Implementatierichtlijn Objecten].	Inrichting beheer en onderhoud beheerobject	VSP/VSE-eisen CSIR3.3
71.	Bij inzet van (web)applicaties voor beheer of onderhoud van ICT en IA van het beheerobject dient de beveiliging van de in te zetten (web)applicaties ingericht te zijn conform de [ICT-Beveiligingsrichtlijnen Webapplicaties] van het Nationaal Cybersecurity Centrum.	Eisen aan webapplicaties voor beheer van beheerobject	VSP/VSE-eisen CSIR3.2
72.	Voor het beheerobject dient de toepassing van IoT gebaseerd te zijn op de uitkomsten van een risico en privacy assessment en voorzien te zijn van relevante mitigerende maatregelen conform bijlage CSR 6 "IoT" van de [Cybersecurity Implementatierichtlijn Objecten].	Risico-gebaseerde afweging inzet IoT bij beheerobject	VSP/VSE-eisen CSIR3.1
73.	Gevirtualiseerde ICT en IA van het beheerobject dient ingericht te zijn conform bijlage CSR 22 "Virtualisatie" van de [Cybersecurity Implementatierichtlijn Objecten].	Eisen virtualisatie ICT en i.r.t. bij beheerobject	VSP/VSE-eisen CSIR3.0
74.	De software van ICT en IA van het beheerobject dient ontwikkeld en beheerd te zijn volgens gangbare principes en de voorgeschreven maatregelen conform Secure Software	Toepassing Grip op SSD ICT en IA beheerobject	VSP/VSE-eisen CSIR3.1

	Development (SSD) van het Centrum voor Informatiebeveiliging en Privacy (CIP).		
75.	De cybersecurity eisen zijn onverkort van toepassing voor de inrichting en onderhoud van eventuele (permanente) Ontwikkel-, Test-, Acceptatie- en Leeromgevingen voor de ICT en IA van het beheerobject, inclusief de vereisten uit paragraaf 2.8 "Maatregelen gecontroleerd wijzigen" van de [Cybersecurity Implementatierichtlijn Objecten].	Toepasselijkheid cybersecurity eisen op omgevingen beheerobject	VSP/VSE-eisen CSIR3.2
76.	De ICT en IA van het beheerobject dienen als integraal onderdeel van de FAT, SAT en SIT getest te zijn op technische naleving van beveiligingseisen en het aantoonbaar maken van de werking van de security functies en maatregelen.	Test op naleving en werking cybersecurity eisen beheerobject	VSP/VSE-eisen CSIR3.3
77.	De ICT en IA van het beheerobject dient naar een vooraf gedefinieerde veilige situatie gestuurd te worden in geval van een aanval, incident of calamiteit conform paragraaf 2.3 "Maatregelen beveiligingsincidenten en incident response plan" van de [Cybersecurity Implementatierichtlijn Objecten].	Veilige modus beheerobject	VSP/VSE-eisen CSIR3.4