NZL Bestek Noodzakelijke Aanpassingen SCL

NB-Radiocommunicatie

Vertrouwelijkheidsniveau: **vertrouwelijk**

Colofon

Uw contact: NB-Radiocommunicatie

Versie beheer

Versie	Wijziging	Auteur
221122	versie 1.0	GVB

Voor U ligt een document dat als vertrouwelijk is geclassificeerd. Voor u als lezer/ gebruiker houdt dat het volgende in:

1. U bent voor dit gebruik expliciet geautoriseerd door de informatie-eigenaar.
2. Als gebruiker van deze informatie (als medewerker, als inhuurkracht of als Leverancier) hebt u een geheimhoudingsverklaring getekend.
3. Het is niet toegestaan deze informatie met niet expliciet daartoe geautoriseerde personen te delen.
4. Deze informatie in papieren vorm moet na gebruik uit het zicht worden opgeborgen.
5. Als u (delen van) deze informatie elektronisch wilt uitwisselen met anderen via een openbaar netwerk dan moet deze informatie versleuteld zijn.

Inhoudsopgave

1 Inleiding

1.1 Beschrijving Noord-Zuidlijn

De Noord-Zuidlijn (NZL) loopt ondergronds vanaf de tunnelmond na station Noorderpark (NDP) via de stations Centraal Station (CSN), Rokin (RKN), Vijzelgracht (VZG), De Pijp (DPP) en Europaplein (EPP) tot de tunnelmond richting Zuid. Elke ondergronds station heeft twee technische ruimtes aan de noord- en zuidzijde waar apparatuur voor de SCL staat. Daarnaast worden de tunnelmonden gevoed van NDP aan de noordzijde en het SET-gebouw aan de zuidzijde.

Er zijn twee donorinkoppelingen voor C2000 vanaf DBS'n De Mirandalaan en Sixhaven. MOBNEXT wordt met glas ingekoppeld vanaf twee BS'n WBS en CSI-SCL. De SCL heeft twee mastersites: SET en CSN zd. Per systeem wordt daar een donor ingekoppeld en vervolgens verdeeld naar alle slave locaties. Elke slave locatie wordt vanaf beide masters gevoed. Zie bijgevoegde schema's.

1.2 Nadere details NZL

De SCL in de Noord-Zuidlijn (NZL) is geleverd door SEE Telecom. De actieve apparatuur is eigen fabrikaat en de coaxkabel is van Eupen.

In tegenstelling tot de Oostlijn zijn de ruimtes, noodstroomvoorziening, etc, geen onderdeel van de scope.

Alle voeding voor de actieve componenten is op basis van 24 VDC. Binnen de SCL zijn geen accu's of UPS'n toegepast. Elke kast heeft een dubbele 230 VAC voeding; één achter een UPS en één die niet per sé achter een UPS zit.

De infrastructuur voor glas en IP zitten buiten het domein van de SCL.

Het systeem heeft de volgende eigenschappen

- Kabelbewaking op de coax gaat op basis van SWR. Alle coax is in lussen aangebracht. Er zijn enkel uitlopers naar de 2 handoverantennes aan de tunnelmonden.
- De glasvezelomzetters regelen zichzelf, binnen grenzen, naar het ingesteld niveau.
- In de downlink wordt gewerkt met glassplitters. Eenmaal ingesteld werkt het prima, maar voor storingsonderzoek moet rekening gehouden worden met de cascade.
- Overspaningsbeveiliging op de coax is niet toegepast. Er zijn wel DC-blocks toegepast maar die zitten niet op afstand in een kunststof behuizing.

Een aandachtspunt is het managementsysteem. Dat is nu een verouderd systeem va SEE Telecom. Elke site heeft beheerunits die uitgelezen kunnen worden. Per tray is er een IP-adres. Alle harde contacten zijn afgewerkt op een verzamelunit met een apart IP-adres

1.3 Doel en scope document

Dit document beschrijft de functionele en technische eisen voor de noodzakelijke aanpassingen van de SCL in de NZL.

2 Technische en functionele eisen

Alle noodzakelijke wijzigingen aan de NZL moeten voldoen aan alle eisen zoals geformuleerd in dit bestek én de volgende documenten:

- Bijlage 1: GVB Beheer Codering SysteemOnderdelen
- Bijlage 2: GVB Beheer Definities en Begrippenlijst
- Bijlage 3: GVB Beheer Documentatieplan
- Bijlage 4: GVB Beheer Eisen en Normen Infrastructuur
- Bijlage 5: GVB Beheer Tekenvoorschriften
- Bijlage 6: GVB Beheer NMS Architectuur

In de volgende paragrafen wordt per item beschreven wat er moet worden aangepast.

Zie voor de huidige as built Bijlage 7 SEE NZL As-built Blokschema Rev16.4 210317.

Veldsterktemetingen moeten worden uitgevoerd conform de Lee sampling criteria. Zie daarvoor bijlage 9.

2.1 Aanpassingen Master-kasten.

De masterkasten in SET en CSN zdhebben een dubbele functie:

1. Masterfunctie met distributie van C2000- en MOBNEXT-signalen naar alle RAU-kasten aan de Slave Stations via glasvezel.
2. RAU-functie om zijn gebeid te dekken met RF-signalen door stralende kabel te voeden.

Ze zijn ontworpen in een dubbel verbonden kasten met een mix van de Master-functie en RAU functie. In deze twee stations worden de RF-signalen direct met een coaxkabel op de RAU aangesloten. Alle andere RAU's op de Slave Stations zijn verbonden via glasvezel. Om deze reden zullen de RAU’s in Masters niet 100% zijn zoals die op de slave-stations is geïnstalleerd.

De aannemer dienst beide kasten te scheiden waarbij elke kast z’n eigen functie krijgt Master of RAU). Hiervoor moeten de volgende werkzaamheden worden uitgevoerd:

- Scheiding van de 2 kasten en het toevoegen van scheidingswanden.
- Het verplaatsen van de rijgklemmen voor de inkomende voeding van de bodem van de kast naar een 19” rail.
- Installatie van 8-voudige servicecontactdozen
- Installatie van DC-zekeringen of stroomonderbrekers voor alle individuele apparatuur op DC (Eacsys, PA)
- Verplaats apparatuur van RAU naar kast 2 (LNA, ALC, OTx, RTx,…)
- In RAU-kast (2) installatie van limiter ALC op een 19'' plank, toevoeging en integratie van de ALC alarmen op het alarm-subrack.
- Routering van alle kabels tussen de kasten via de kelder en kabels in één stuk maken.

- Plaatsen en afwerken van de huidige patchkabels die vanaf een derde kast komen op een patchpaneel in de masterkast. Vervolgens extra patchkabels leveren vanaf het patchpaneel alle patches maken
- Kast op één punt met aarde verbinden

Alle bovenstaande punten moeten worden ontworpen en aangepast aan de best mogelijke oplossingen.

2.2 Aanpassingen RAU-kasten.

Ook de RAU-kasten op de slave locaties moeten worden aangepast. Het gaat om de volgende punten:

- Het verplaatsen van de rijgklemmen voor de inkomende voeding van de bodem van de kast naar een 19” rail.
- Installatie van DC-zekeringen of stroomonderbrekers voor alle individuele apparatuur op DC (Eacsys, PA)
- In RAU-kast (2) installatie van limiter ALC op een 19'' plank, toevoeging en integratie van de ALC alarmen op het alarm-subrack.
- Kast op één punt met aarde verbinden
- Verwijderen en in de spare toevoegen van ongebruikt materiaal.

2.3 DC-blocks en overspanningsbeveiligingen

De huidige DC-blocks zijn direct op de coaxkabel aangebracht onder de vereiste jumper. Tevens liggen ze los in de goot zonder de vereiste afstand. Overspanningsbeveiligingen ontbreken in het geheel. De coax is achter de DC-block geaarde waardoor de DC-block functie enkel functioneert voor de binnengeleider. Dit geheel is een onwenselijke situatie en alle punten moeten worden hersteld.

Het herstel houdt dit de volgende werkzaamheden in:

- Plaatsen van kunststof behuizingen conform de Oostlijn
- Plaatsen van de bestaande DC-blocks en nieuwe overspanningsbeveiligingen in deze kasten
- Het juist aarden van dit geheel
- De huidige aardklemmen van de coaxkabel verwijderen. De kabel inkorten om de mantel tot aan de connector te laten lopen.
- Jumpers plaatsen indien de aangesloten coax groter is dan ½”

E.e.a. conform de eisen zoals gesteld in Bijlage 4: GVB Doc Beheer Eisen en Normen Infrastructuur.

2.4 Labelling

In de huidge kasten is de apparatuur niet of eenvorming gelabeld. In de gehele SCL komen dezelfde codes meermaals terug. Per kast zijn codes wel uniek.

Aannemer dient alle apparatuur opnieuw te labellen conform de eisen gesteld in Bijlage 1: GVB Doc Beheer Codering SysteemOnderdelen.

2.5 As built documentatie

Voor alle wijzigingen moet ook de as built documentatie conform de eisen in de bijlagen worden aangepast.

2.6 Beheersysteem updaten

Het huidige beheersysteem is out of date en moet vervangen worden door het huidige systeem van SEE Telecom. Tevens moet het beheersysteem verplaatst worden van SET naar CSN nd.

Het nieuwe beheersysteem moet gekoppeld worden met Nagios van GVB waardoor alle alarmen en vereiste functionaliteit vanuit de NZL bij Nagios binnen komt.

2.7 Cybersecurity

Cybersecurity zorgt voor de weerbaarheid van het betrokken systeem tegen cyberaanvallen en cyberbesmettingen. Het doel van cybersecuritymanagement is om de operationele veiligheid en beschikbaarheid van alle stakeholders van de OV-operatie te borgen door de invloed van risico's van cyberaanvallen en cyberbesmettingen op de systemen te mitigeren. Cybersecuritymanagement is (naast aspecten als risicomanagement, configuratiemanagement, financieel management, etc) een natuurlijk onderdeel van projectbeheersing.

In het kort betekent cybersecuritymanagement voor een project en voor Opdrachtnemer (ON) het volgende:

- Het aanstellen van een projectcybersecurity-officer door en van ON
- Het samenwerken met projectcybersecurity-officer van Opdrachtgever (OG)
- Opstellen van cybersecuritymanagementplan (inclusief de V&V voor cybersecurity) voor alle projectfasen én tot en met de beheerfase na het project.
- Uitvoeren van cyberrisico-analyses, indien wordt afgeweken van de standaard eisenset en maatregelen
- Ontwerpen, realiseren en implementeren van technische en organisatorische cybersecuritymaatregelen.

Bindende/vigerende bijlagen
De bijlagen (zie Bijlage 9) die vigerend zijn voor dit project en een onderdeel vormen van de cybersecurity-eisen per 28 september 2022, zijn de volgende:

CS-1 Cybersecurity-voorschrift OT Versie 1.7 Bedrijfsvertrouwelijk
CS-2 Cybersecurity-eisen-maatregelen voor OT Versie 1.3 Bedrijfsvertrouwelijk
CS-3 Vraagspecificaties Cybersecurity voor OT, Versie 1.1 Bedrijfsvertrouwelijk
CS-4 Cybersecuritydossiersjabloon OT, 28 juni 2022 Bedrijfsvertrouwelijk

CS-5 Vertrouwelijkheid OT Versie 2.1 Bedrijfsvertrouwelijk
CS-6 Cyberincidentprocedure OT Versie 1.3 Bedrijfsvertrouwelijk
CS-7 Wachtwoordenbeleid OT Versie 2.11 Bedrijfsvertrouwelijk
CS-8 Hardeningvoorschrift OT Versie 0.2 Bedrijfsvertrouwelijk
CS-9 Aansluitvoorwaarden NMA-netwerk Versie 1.0 Vertrouwelijk *)
CS-10 Cyberrisicomanagement OT, Versie 1.2 Bedrijfsvertrouwelijk
CS-10.1 Cyberdreigingsbeeld OT, 28 juni 2022 Vertrouwelijk *)
CS-11 Cybersecurity beleid buitenlandse devices, 28mrt22,Bedrijfsvertrouwelijk
CS-12 RT2000 Pre-project Cyberrisk Assessment Result Summary.pdf *)
CS-13 RT2000 Pre-project Cyberrisk Assessment Result.xlsx *)

*) wachtwoord wordt separaat onder geheimhouding verstrekt door OG

Eis-CS-1 Cybersecurity
Het betrokken systeem dient beveiligd te zijn tegen cyberaanvallen en cyberbesmettingen. Voor het betrokken systeem dienen minstens de maatregelen te zijn getroffen zoals beschreven in het document Cybersecurity-eisen-maatregelen voor OT (CS-2).

> Eis-CS-1.1 Verificatiemethode: Aan de hand van het door ON opgestelde en door OG goedgekeurde Projectcybersecuritymanagementplan (inclusief de verificatie en validatie).
> Eis-CS-1.2 Validatiemethode: Door OG zal vooraf aan de acceptatie van het project een pen-test laten uitvoeren, ter validatie van de ingerichte en geïmplementeerde maatregelen. Eventuele herstelwerkzaamheden naar aanleiding van de pen-test zijn een verantwoordelijkheid van ON en dienen vooraf aan de acceptatie van het project te zijn uitgevoerd.
> Eis-CS-1.3 Voorschrift/Normen: Cybersecurity-eisen-maatregelen voor OT (CS-2) aangevuld met Cybersecurity-voorschrift OT (CS-1).

Eis-CS-2: Aanstellen van een projectcybersecurity-officer
Opdrachtnemer dient een projectcybersecurity-officer aan te stellen om de projectcybersecurity- aspecten te behartigen, om de gestelde cybersecurity-eisen in te vullen en om als primair contactpersoon te fungeren voor (in het bijzonder) de projectcybersecurity-officer van OG.

Eis-CS-3: Opstellen van cybersecuritymanagementplan
De Opdrachtnemer dient een projectcybersecuritymanagementplan op te stellen op basis van hetgeen gesteld in het Cybersecurity-voorschrift OT (CS-1) en de Cybersecurity-eisen-maatregelen voor OT (CS-2) en laat dit plan goedkeuren door Opdrachtgever alvorens aan de ontwerpfase mag worden begonnen. Het projectcybersecuritymanagementplan dient ook de verificatie en validatie (V&V-plan) te beschrijven voor de cybersecurity gedurende alle fase van de Werkzaamheden en bevat alle formele momenten van goedkeuring door de Opdrachtgever.

Eis-CS-4: Ontwerpen, realiseren en implementeren
Opdrachtgever dient alle cybersecuritymaatregelen te ontwerpen, realiseren en implementeren zoals gegeven in Cybersecurity-eisen-maatregelen voor OT (CS-2) én de

aanbevelingen zoals gegeven in de resultaten van de Pre-project Cyberrisk Assessment (CS-12 en CS-13). De maatregelen zijn gericht op de borging van de door Opdrachtgever gestelde/geëiste operationele doelstellingen voor Beschikbaarheid.

Eis-CS-5: Comply-or-explain
Er mag worden afgeweken van de Cybersecurity-eisen-maatregelen voor OT (CS-2) op basis van een schriftelijke door de Opdrachtgever goedgekeurde cyberrisico-analyse en een goedgekeurd voorstel voor alternatieve maatregelen. ON kan gebruik maken van de Cyberrisicomanagementaanpak (CS-10) van Opdrachtgever. De cyberrisicoanalyses en alternatieve maatregelen dienen expliciet door Opdrachtgever te worden goedgekeurd alvorens een volgende projectfase mag worden gestart. Het Cyberdreigingsbeeld OT (CS-10.1) dient mede te worden gebruikt als input voor de risico-analyses en wordt door de OG ter beschikking gesteld na gunning van de opdracht (i.v.m. de vertrouwelijkheid ervan).

3 Fasering

De leverancier is verantwoordelijk om een definitief ontwerp tot in detail uit te werken. Hij zal in zijn definitieve ontwerp en bouwbeschrijvingen moeten aangeven hoe hij aan de genoemde functionele en technische eisen denkt te kunnen voldoen. De leverancier is ervoor verantwoordelijk dat het geheel conform alle gestelde eisen functioneert. Tijdens de afname moeten worden aangetoond dat aan de eisen is voldaan.

Na opdrachtverlening dienen de volgende processtappen doorlopen te worden:

- Definitief ontwerp
- Realisatie
- Oplevering

Er moet worden gewerkt aan een installatie die volledig in bedrijf is. Er worden delen van de aanpassingen al gebruikt terwijl het geheel nog niet voor oplevering gereed is. Een deel van de wijzigingen kan enkel in gebruik worden genomen indien dat deel aan alle functionele, technische en beheerseisen voldoet. Voorafgaand aan een dergelijke situatie moet het betreffende deel geaccepteerd worden door GVB met de volledige documentatie. Na acceptatie kan de aannemer het deel in dienst stellen en gebruikt worden. De aannemer is verantwoordelijk voor de instandhouding binnen de kaders van de vereiste beschikbaarheid.

De volgende deelrealisaties en –oplevering zijn voorzien:

1. Master SET
2. Master CSN zd
3. RAU NDP
4. RAU CSN nd
5. Station RKN
6. Station VZG
7. Station DPP
8. RAU’s Churchilllaan
9. Station EPP

4 Bijlagen

4.1 GVB Doc Beheer Codering SysteemOnderdelen

4.2 GVB Doc Beheer Definities en Begrippenlijst

4.3 GVB Doc Beheer Documentatieplan

4.4 GVB Doc Beheer Eisen en Normen Infrastructuur

4.5 GVB Doc Beheer Tekenvoorschriften

4.6 GVB Doc Beheer NMS Architectuur

4.7 SEE NZL As-built Blokschema Rev16.4 210317

4.8 Lee sampling criteria

4.9 Bijlagen cybersecurity

CS-1 Cybersecurity-voorschrift OT Versie 1.7 Bedrijfsvertrouwelijk
CS-2 Cybersecurity-eisen-maatregelen voor OT Versie 1.3 Bedrijfsvertrouwelijk
CS-3 Vraagspecificaties Cybersecurity voor OT, Versie 1.1 Bedrijfsvertrouwelijk
CS-4 Cybersecuritydossiersjabloon OT, 28 juni 2022 Bedrijfsvertrouwelijk
CS-5 Vertrouwelijkheid OT Versie 2.1 Bedrijfsvertrouwelijk
CS-6 Cyberincidentprocedure OT Versie 1.3 Bedrijfsvertrouwelijk
CS-7 Wachtwoordenbeleid OT Versie 2.11 Bedrijfsvertrouwelijk
CS-8 Hardeningvoorschrift OT Versie 0.2 Bedrijfsvertrouwelijk
CS-9 Aansluitvoorwaarden NMA-netwerk Versie 1.0 Vertrouwelijk *)
CS-10 Cyberrisicomanagement OT, Versie 1.2 Bedrijfsvertrouwelijk
CS-10.1 Cyberdreigingsbeeld OT, 28 juni 2022 Vertrouwelijk *)
CS-11 Cybersecurity beleid buitenlandse devices, 28mrt22,Bedrijfsvertrouwelijk
CS-12 RT2000 Pre-project Cyberrisk Assessment Result Summary.pdf *)
CS-13 RT2000 Pre-project Cyberrisk Assessment Result.xlsx *)