

De (I)VRI in het IT landschap.



Auteurs:

XXXX

	Systeemdocumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

Management samenvatting

Dit document beschrijft het IT landschap waarin (intelligente) Verkeer Regel Installaties zijn opgenomen. In het kader van deze aanbesteding worden er 3 categorieën Verkeer Regel Installaties onderscheiden:

1. VRI - Traditionele Verkeer Regel Installatie
Dit is een traditionele VRI gebaseerd op CCOL regelingen die geen communicatie onderhoudt met UDAP en/of de weggebruiker.
2. iVRI - Intelligente Verkeer Regel Installatie
Dit is een volwaardige iVRI inclusief slimme regelingen en communicatie met UDAP. De iVRI kan uitgerust zijn met een WiFi-P modem voor communicatie met de weggebruiker. De iVRI beschikt over betere specificaties ten aanzien van Informatiebeveiliging.
3. iVRI-Ready - Voorbereide Intelligente Verkeer Regel Installatie
Dit is een iVRI die draait op traditionele CCOL regelingen en nog niet is voorzien van een slimme regeling. De installatie is maximaal voorbereid en kan eenvoudig opgewaardeerd worden tot een volwaardige iVRI. De iVRI-Ready beschikt over betere specificaties ten aanzien van Informatiebeveiliging.

In dit document zal

“VRI” gebruikt worden voor een traditionele VRI.

“iVRI” gebruikt worden voor een Intelligente VRI of voor een iVRI-Ready.

Vanuit het perspectief van Informatie Technologie (IT) is een (i)VRI een apparaat dat zich in de openbare ruimte bevindt in een afgesloten straatkast en dat een netwerkverbinding met het datacenter onderhoudt. De dataverbinding wordt gebruikt voor het besturen van de installatie, de mogelijkheid van onderhoud aan software van de IT-producten en het overdragen van sensor en logging data. Moderne intelligente (i)VRI's worden via de netwerkverbinding verbonden met het landelijke overnamepunt Urban Data Access Platform (UDAP) waarmee communicatie met voertuigen en beïnvloeding van de regeling door landelijke aansturing mogelijk wordt.

In enkele gevallen wordt de data die omgaat in de (i)VRI geclassificeerd als privacy gevoelig. De (i)VRI wordt gezien als een volledig networked device. De data classificatie voor deze applicatieketen en de aansluiting op het netwerk dwingt eisen te stellen aan de Informatiebeveiliging en de omgang met de data in het kader van privacy. Voor Informatiebeveiliging moet het normenkader zoals beschreven in de Baseline Informatiebeveiliging Overheid (BIO) aangehouden worden en ten aanzien van privacy dient de applicatieketen te voldoen aan de AVG-wetgeving.

Dit document beschrijft de opbouw van de applicatieketen en de daarbij aanwezige koppelvlakken. De koppelvlakken vormen de grenzen van beheer en de verantwoordelijkheid voor zowel opdrachtgever als opdrachtnemer.

Op hoofdlijnen ziet de applicatieketen er als volgt uit: De applicatiesuite “Verkeer Beheer Systeem (VBS)” wordt gehost in het VOR-IN datacenter en wordt gebruikt voor besturing en beheer van de (i)VRI's. De

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

suite is geplaatst in een beveiligd en afgeschermd netwerksegment en er vindt communicatie plaats met de (i)VRI in de openbare ruimte en met het landelijke overnamepunt UDAP in het geval het gaat om een (i)VRI. De hosting omgeving, de telewerkvoorziening die toegang geeft voor de opdrachtnemer, en de netwerkverbindingen zijn in beheer bij de opdrachtgever. De (i)VRI en eventuele (i)VRI specifieke management software wordt beheerd door de opdrachtnemer. Het koppelvlak is de aansluiting op het netwerk van de opdrachtgever en de netwerkaansluiting van de (i)VRI.

Er moet veel waarde worden gehecht aan Informatiebeveiliging en privacy aspecten en dit resulteert in een aantal eisen en randvoorwaarden aan de (i)VRI:

- Er zal gedurende de looptijd van de opdracht periodiek getoetst worden op Informatiebeveiliging aspecten.
- Er zullen periodiek updates en upgrades moeten plaatsvinden om het systeem veilig te houden.
- De “end of life” status van een product moet bewaakt worden en eventueel tijdige vervanging moet plaatsvinden om zo te kunnen blijven voldoen aan de informatie beveiliging.
- Het systeem zal moeten voldoen aan het kader dat is vastgelegd in de BIO voor de Nederlandse overheid.
- Het systeem communiceert efficiënt (niet onnodig) met beveiligde protocollen over het netwerk. (“attack surface” minimaliseren, “hardening”)
- Er zijn aanvullende fysieke en logische beschermingsmaatregelen om de integriteit van de installatie en de applicatieketen te borgen.

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

Versie historie

Historie

Versie	Status	Wijzigingen	Auteur	Datum
0.1	Initiële versie	Initieel document	X	13 augustus 2020
0.2	concept	Tekst aanpassingen	X	10 maart 2021
0.3	concept	Samenvoegingen en herstructureren.	X	14 maart 2021
1.0	Vrijgave	Opschonen document	X	1 april 2021

Distributie

Naam	Organisatie	Rol
X	Verkeer en Openbare Ruimte	X
X	Verkeer en Openbare Ruimte	X
X	Verkeer en Openbare Ruimte	X
X	Verkeer en Openbare Ruimte	X

Personen en relaties

Relatie	Doel / Rol	Stakeholder	e-mail
Gemeente Amsterdam	X	X	X
Gemeente Amsterdam	X	X	X
Gemeente Amsterdam	X	X	X
Gemeente Amsterdam	X	X	X
Gemeente Amsterdam	X	X	X

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

Inhoudsopgave

De (I)VRI in het IT landschap.	1
Management samenvatting	2
Versie historie.....	4
Personen en relaties.....	4
Inhoudsopgave	5
Inleiding en context.....	6
De (i)VRI applicatieketen	8
Toelichting op de gebruikte netwerkverbindingen.....	11
Toelichting op de categorieën Verkeer Regel Installaties	13
Toelichting op de hosting omgeving	14
Informatiebeveiliging en privacy	17
Informatiebeveiliging	17
Privacy	18
Aansluitvoorwaarden	19
Bijlage 1 Verkeer Regel Installatie applicatieketen	21
Bijlage 2 Situatietekening1 (i)VRI	22
Bijlage 3 Situatietekening2 (i)VRI	23

	Systeemdocumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

Inleiding en context

De gemeente Amsterdam, onderdeel Verkeer en Openbare Ruimte, heeft ongeveer 400 Verkeer Regel Installaties ((i)VRI) in beheer. Deze (i)VRI's zijn, behoudens tijdelijke uitzonderingen ten gevolge van bijvoorbeeld werkzaamheden, aangesloten op het industriële netwerk. De naam van dit netwerk en de bijbehorende hosting faciliteiten is Verkeer en Openbare Ruimte Intelligent Netwerk (VOR-IN). Deze netwerkomgeving is gebaseerd op 3 pijlers:

- Besturing
- Beveiliging en monitoring
- Data

De primaire taak van de netwerkomgeving is het besturen van de assets die in beheer zijn. De assets die bestuurd worden zijn naast de (i)VRI's ook verkeer informatie systemen zoals zicht- en kenteken camera's, verzinkbare palen, Crowd Monitoring sensoren e.d. en ook een deel van de openbare verlichting van Amsterdam.

Deze verschillende assets kennen verschillen gebruikersgroepen, beheerders en applicaties en zijn daarom van elkaar gescheiden. De data die omgaat binnen deze assets is ook verschillend van aard. Vanuit een beveiligingsperspectief mag geen ongecontroleerde vermenging ontstaan. De tweede pijler is daarom beveiliging en monitoring. Het netwerk, de daarop aangesloten serversystemen, en bedienposten moeten goed beveiligd worden tegen onrechtmatig gebruik. De beschikbaarheid van de systemen wordt met geautomatiseerde middelen bewaakt.

De derde pijler betreft data. De assets die in beheer zijn genereren data die voor onderhoud, besturing en analyse relevant zijn. Het inwinnen van data is niet langer een bijvangst vanuit beheer, maar is een structurele taak die doelbewust wordt ingeregeld in het kader van Dynamisch Verkeer Management (DVM).

(i)VRI's zijn niet langer standalone apparaten waarvoor het handig is over een netwerkverbinding wat programma's te schakelen en onderhoud te plegen. De (i)VRI's maken deel uit van het Dynamisch Verkeer Management platform en zijn naast signaalgevers tegelijkertijd ook sensoren. Een (i)VRI maakt deel uit van het (logische) verkeersnetwerk waarin ook andere signaalgevers en sensoren zijn geplaatst.

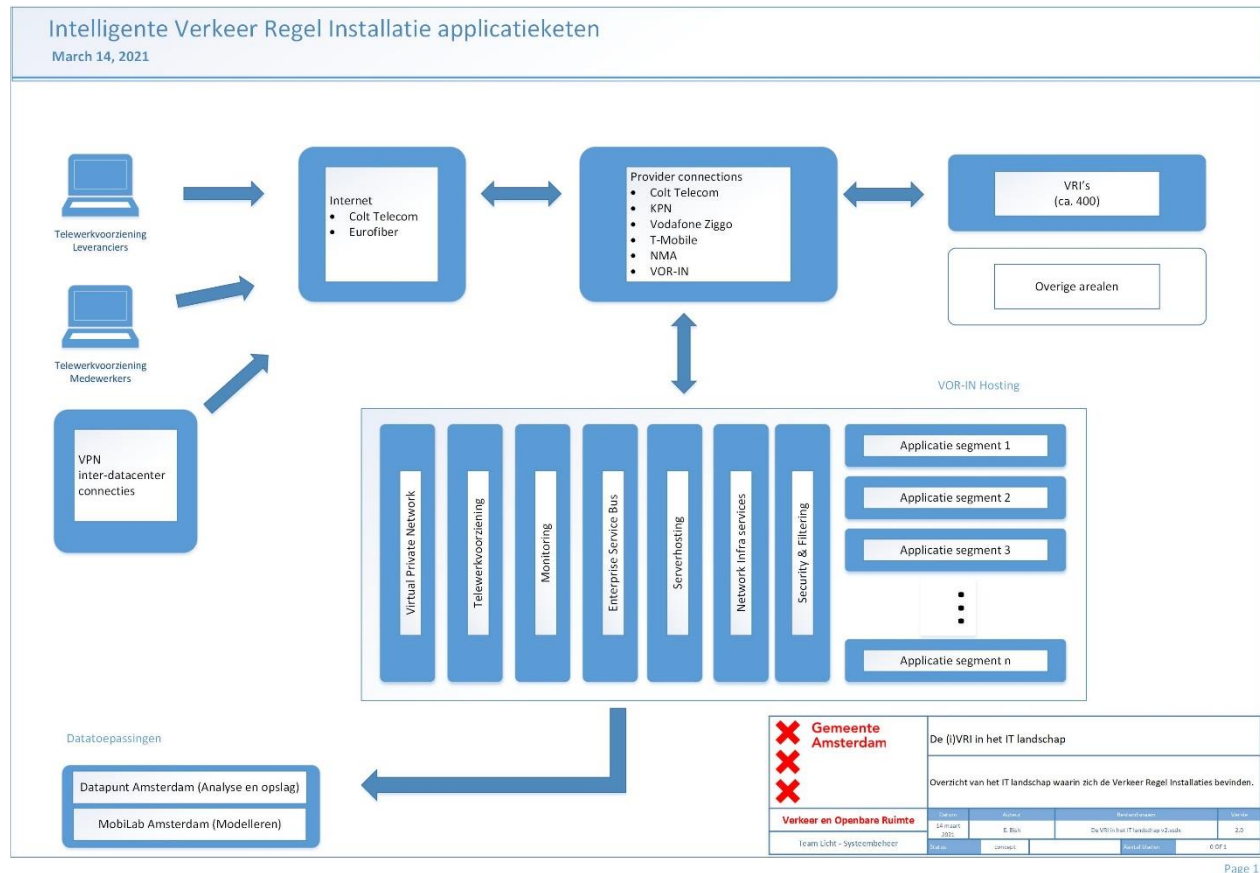
In het geval van een (i)VRI wordt de VLOG-datastroom ingewonnen en wordt bijvoorbeeld gebruikt voor het analyseren van de doorstroming van het verkeer. Het VOR-IN netwerk vormt een data hub voor alle assets in beheer. Verkeer en Openbare Ruimte gebruikt data zelf voor operationele toepassingen zoals het begeleiden van evenementen, maar zet de data ook door naar Datapunt. Dit is een ander onderdeel

	Systeemdocumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

van de gemeente die alle datasets van de gemeente verzameld voor analyse doeleinden en deze voor zover dat toegestaan is weer beschikbaar stelt als open data¹.

¹ Zie eventueel <https://data.amsterdam.nl/>.

De (i)VRI applicatieketen



De tekening hierboven geeft schematisch en vereenvoudigd weer hoe het IT landschap waarin Verkeer Regel Installaties ((i)VRI) zijn opgenomen er uit ziet. Vanuit het perspectief van IT is een (i)VRI een apparaat dat zich in de openbare ruimte bevindt in een afgesloten straatkast en dat een netwerkverbinding met het datacenter onderhoudt. De dataverbinding wordt gebruikt voor het besturen van de installatie, de mogelijkheid van onderhoud aan software van de IT-producten en het overdragen van sensor en logging data. Moderne intelligente VRI's worden via de netwerkverbinding en een proxy component verbonden met het landelijke overnamepunt Urban Data Access platform (UDAP)² waarmee communicatie met voertuigen en beïnvloeding van de regeling door landelijke aansturing mogelijk wordt.

De Points-of-Presence van het industriële netwerk in de openbare ruimte zijn ondergebracht bij de assets. Zo is in de (i)VRI-kast ook de datacommunicatie apparatuur geplaatst om de (i)VRI te kunnen laten communiceren met de applicaties die worden gehost in het datacenter. Er wordt gebruik gemaakt

² Zie voor uitleg: <https://www.talking-traffic.com/nl/urban-data-access-platform>

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

van een grote diversiteit aan typen netwerkverbindingen. Voor de opdrachtnemer is alleen van belang te weten dat de benodigde communicatie parameters worden verstrekt door de beheerders van de gemeente en dat de medewerking van de opdrachtnemer is vereist voor het plaatsen en onderhouden van de datacommunicatie apparatuur in de straatkasten. Het aanleggen van hoogwaardige dataverbindingen in de openbare ruimte is geen eenvoudige zaak en vaak erg kostbaar. Er wordt daarom gestreefd naar meervoudig gebruik van datalijnen waarbij de vereiste netwerksegmentatie behouden moet blijven. Het komt bijvoorbeeld met enige regelmaat voor dat een nabijgelegen toezichtcamera wordt aangesloten op de datacommunicatie apparatuur in de (i)VRI kast. Andersom, kan een (i)VRI ook zijn aangesloten op een nabijgelegen aansluitpunt van een camera.

Het dataverkeer van- en naar de (i)VRI dient geauthentiseerd en versleuteld te zijn. Dit staat los van het feit dat er ook gebruik gemaakt wordt van VPN-verbindingen. Niet alle verbindingen zijn vanuit een beveiligingsperspectief even sterk en daarom dient alle aangesloten apparatuur efficiënt (geen onnodig verkeer) en encrypted te communiceren.

Via de netwerkverbinding is de (i)VRI aangesloten op het datacenter. Het netwerk is gesegmenteerd en alle toepassingen voor de verschillende soorten assets zijn standaard van elkaar geïsoleerd. De besturingsapplicatie en de managementapplicaties van de (i)VRI's zijn in een eigen applicatiesegment geplaatst. Het verkeer tussen (i)VRI en applicatie doorloopt een security & filtering laag. Alleen vooraf gedefinieerde protocollen en netwerksegmenten zullen kunnen communiceren. Communicatie tussen de (i)VRI-systemen onderling op TCP/IP niveau is niet of slechts beperkt mogelijk (micro segmentering) en hangt af van de wijze waarop de lokale netwerkverbinding is gerealiseerd. Vanuit het applicatiesegment kunnen netwerk infrastructuur services zoals DNS, DHCP, NTP, PKI e.d. op aanvraag en in overleg gebruikt worden.

De hosting omgeving wordt gevormd door meerdere hyperconverged Hyper-V cluster³ opstellingen op basis van Microsoft Windows Server 2016 of nieuwer. Op dit virtualisatie platform draaien zowel Virtuele machines op basis van Windows Server 2016 of nieuwer als Redhat Enterprise Linux (RHEL). Het standaard database platform is MS SQL. Er wordt gewerkt aan een bredere ondersteuning en andere aanvullende hosting faciliteiten, maar op het moment van schrijven van dit stuk kan daar nog geen definitieve toezegging over gedaan worden.

De standaard applicatie suite voor de gemeente Amsterdam voor het besturen van de (i)VRI's is het Verkeer Beheer Systeem (VBS). Deze maatwerk applicatie suite bevat alle componenten voor het effectief besturen, onderhouden en beheren van de installaties en kan niet vervangen worden door een applicatie (suite) van de opdrachtnemer. Het is wel mogelijk aanvullende management applicaties noodzakelijk voor effectief onderhoud van de (i)VRI's in de hosting omgeving te laten draaien. Het is niet toegestaan dat ingewonnen data van de (i)VRI's wordt doorgezet buiten het VOR-IN netwerk.

³ Zie eventueel <https://docs.microsoft.com/en-us/windows-server/hyperconverged/>

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

De opdrachtnemer krijgt via de Telewerkvoorziening die gebaseerd is op een Remote Desktop Protocol (RDP) sessie naar een managementserver in het applicatiesegment toegang tot de omgeving waarvoor de opdrachtnemer verantwoordelijk is. Vanuit deze managementserver kan de opdrachtnemer communiceren met de (i)VRI's voor het uitvoeren van onderhoud en wijzigingen. Het is van buiten de VOR-IN omgeving niet mogelijk rechtstreeks met de Graphical User Interface (GUI) van de (i)VRI te communiceren. Dat is alleen mogelijk binnen de VOR-IN omgeving.

De toegang tot de telewerkvoorziening is door middel van een gepersonaliseerde two-factor authenticatie beveiligd. Het is niet mogelijk of toegestaan met groepsaccounts te werken. Activiteiten zullen worden gelogd. De lijst met geautoriseerde personen wordt minimaal jaarlijks herzien. De managementserver wordt in overleg met de systeembeheerders ingericht met de noodzakelijke software voor het beheer van de (i)VRI's en vervolgens ter beschikking gesteld. Het is niet toegestaan om remote access tools zoals bijvoorbeeld TeamViewer of (web) VPN-verbindingen te gebruiken. Dit ondermijnt de beveiliging van de omgeving en vergroot de kans op een datalek⁴.

In het kader van Dynamisch Verkeer Management wordt op structurele basis logging data uit alle assets in beheer opgehaald. Het gaat daarbij om VLOG data en in het geval van een (i)VRI ook over de datastroom tussen (i)VRI en UDAP in de vorm van ETSI berichten⁵ SPaT, MAP, CAM, SRM, SSM, DENM⁶. Zowel de VLOG als de ETSI berichten worden als streaming data uitgewisseld. De logging data wordt ingewonnen door een Enterprise Service Bus (ESB) applicatie. Deze ESB beschikt over connectors voor VLOG en de berichtenstroom met UDAP. Communicatie over het netwerk is encrypted op basis van TLS. De uitvoer van de ESB-applicatie wordt voor operationele doeleinden zoals evenementen begeleiding door Verkeer en Openbare Ruimte zelf gebruikt. Voor analyse, onderzoek en lange termijn opslag wordt de data doorgezet naar Datapunt en MobiLab. Dit zijn twee andere onderdelen van de gemeente Amsterdam die datasets verzamelen en beschikbaar stellen voor onderzoek en analyse. Indien mogelijk wordt data ook weer als Open Data beschikbaar gesteld. Voor de opdrachtnemer betekent dit het volgende:

1. VLOG 2 (of nieuwer), IVERA 4 (of nieuwer), TLS 1.2 (of nieuwer), NTP tijdsynchronisatie, DNS moet ingeregeld zijn op de (i)VRI conform de standaarden van de gemeente Amsterdam.
2. Doelsystemen die data van de (i)VRI ontvangen moeten zonder belemmering door de opdrachtnemer configureerbaar zijn op de (i)VRI. Zo dient bijvoorbeeld het gebruik van een proxy component voor de datastroom van een (i)VRI eenvoudig instelbaar te zijn en kunnen/mogen de doelservers van UDAP niet hard-coded zijn.
3. Het gebruik van TLS vereist de installatie van PKI Certificaten. Deze certificaten zijn (i)VRI specifiek en zullen door de opdrachtgever ter beschikking worden gesteld in de vorm van een back-up bestand. Het gebruik van certificaten ten aanzien van minimale encryptie niveaus en

⁴ Zie eventueel <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken>

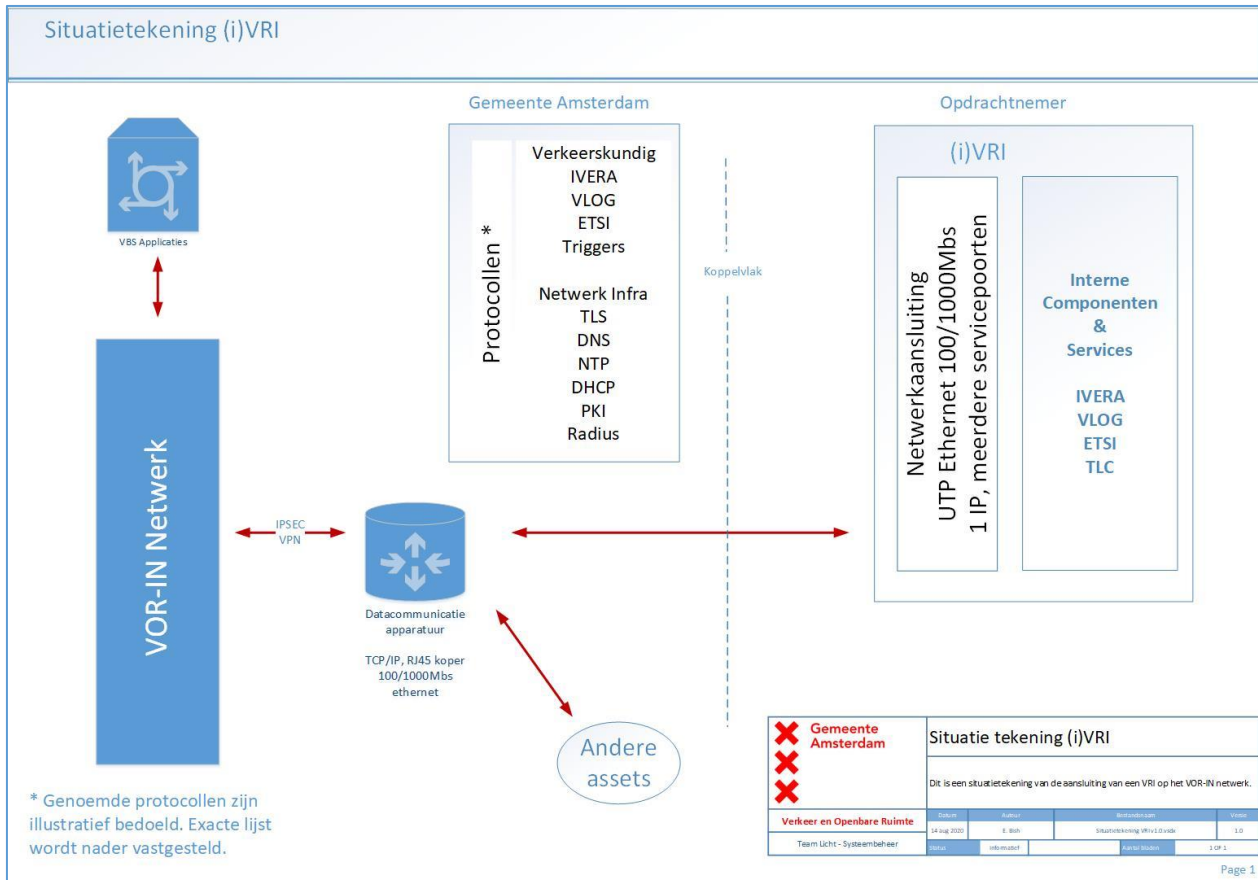
⁵ Zie voor uitleg: <https://en.wikipedia.org/wiki/ETSI>. Website van ETSI: <https://www.etsi.org/>

⁶ Specificatie van de berichten in standaard: ETSI TS 102 894-1

	Systeemdocumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

sleutellengtes volgt uit de BIO standaard en zal naar verwachting gedurende de levensduur van de (i)VRI één of enkele malen aangescherpt worden.

Toelichting op de gebruikte netwerkverbindingen



Het aanleggen van dataverbindingen van het datacenter naar objecten in de openbare ruimte is een lastige en kostbare zaak. Er wordt gebruik gemaakt van lokaal beschikbare mogelijkheden en indien mogelijk wordt meervoudig gebruik van een verbinding toegepast. Hierdoor bestaat er een grote variatie in de wijze waarop een (i)VRI is aangesloten op het datacenter:

	Systeemdocumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

Koppeling met DC	Techniek	Frequentie
Niet	n.v.t.	Zelden en uitsluitend tijdelijk.
Stand-alone 4G	IPSEC VPN over 4G Mobiele data	Regelmatig.
Layer-2 streng	IPSEC VPN over 4G Mobiele data gedeeld met maximaal 6 (i)VRI's.	Meest voorkomend.
Layer-3 streng	Twee of meer glasvezel verbindingen worden gedeeld gebruikt met meerdere (i)VRI's en andere assets. Redundantie.	Beperkt, alleen voor hoogwaardige toepassingen.

Voor het realiseren van Mobiele dataverbindingen wordt de provider gebruikt die voortkomt uit de periodieke gemeentelijke publieke aanbesteding en is op dit moment T-Mobile.

De verbindingen tussen de (i)VRI straatkasten waardoor sprake is van een streng zijn in eigendom van de gemeente Amsterdam en zijn uitgevoerd op basis van ethernet extenders over een vrij aderpaar van de koppelkabels die tussen de (i)VRI straatkasten liggen of zijn in het geval van nieuwbouw situaties uitgevoerd met single mode glasvezel bekabeling. In het geval van glasvezel bekabeling tussen de (i)VRI's kunnen koppelsignalen over het netwerk serieel getransporteerd worden.

De beschikbare bandbreedte en de netwerk latency (=vertraging in milliseconden van het dataverkeer) zijn afhankelijk van enerzijds de kwaliteit van de gedeelde koppeling met het datacenter en anderzijds van de lokale bekabeling tussen de (i)VRI's.

Type verbinding	Bandbreedte (indicatief)	Latency (indicatief)
Koper koppel kabel	max. 11 Mb/s	Ca. 20 ms
Glasvezel Koppel kabel	1 Gbit/s	< 1ms
Koppelvlak switch	100Mb/s	< 3 ms
VPN over 4G	Ca. 25 Mb/s	80 – 300 ms

In het geval van een layer-2 streng die een 4G verbinding deelt met maximaal 6 onderling verbonden (i)VRI's over koperen koppelkabels zal de specifieke combinatie van verbindingstypes dus uiteindelijk de beschikbare prestaties gaan bepalen. In het slechtste geval zal een bandbreedte van ca. 10 Mbit/s resulteren en/of een variabele latency tot wel 300ms + 20ms per hop. In het geval van 4G moet ook rekening worden gehouden met periodieke resets van de verbinding door de provider. Dit vindt minimaal op dagelijkse basis plaats en zal de VPN verstoren. Dit geeft aanleiding tot periodieke onderbrekingen van de verbinding tot enkele minuten per keer.

De gemeente Amsterdam vervangt regelmatig bestaande layer-2 of standalone verbindingen door hoogwaardige glasvezel koppelingen om de kwaliteit en stabiliteit van de besturing en datalevering te verbeteren. Voor de goede werking van een iVRI is dit zelfs een randvoorwaarde.

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

De benodigde gegevens voor het aansluiten van een (i)VRI op het industriële netwerk worden door de systeembeheerders verstrekt. De opdrachtnemer krijgt duidelijke tekeningen en instructies over de wijze waarop de (i)VRI op de juiste poort van het datacommunicatie apparaat (router of switch) moet worden aangesloten. Het is de opdrachtnemer niet toegestaan achter deze poort zelf een switch, router of andere netwerkcomponent te plaatsen zonder daarvoor eerst in overleg te treden met de systeembeheerders van de gemeente. Indien een extra aansluiting noodzakelijk is, dan zal eerst worden gekeken of die door de gemeente beschikbaar kan worden gemaakt op de bestaande apparatuur of dat de switch kan worden vervangen door een ander type met meer aansluitingen. In het kader van Informatiebeveiliging zullen niet gebruikte poorten uitgeschakeld of onbruikbaar gemaakt worden. De datacommunicatie apparatuur is voorzien van logging en registreert wijzigingen in aansluiting of gebruik.

Toelichting op de categorieën Verkeer Regel Installaties

In het kader van deze aanbesteding worden er 3 categorieën Verkeer Regel Installaties onderscheiden:

1. Traditionele Verkeer Regel Installatie
Aanduiding: VRI
Dit is een traditionele VRI gebaseerd op CCOL regelingen die geen communicatie onderhoudt met UDAP en/of de weggebruiker.
2. Intelligente Verkeer Regel Installatie
Aanduiding: iVRI
Dit is een volwaardige iVRI inclusief slimme regelingen en communicatie met UDAP. De iVRI kan uitgerust zijn met een WiFi-P modem voor communicatie met de weggebruiker. De iVRI beschikt over betere specificaties ten aanzien van Informatiebeveiliging.
3. Voorbereide Intelligente Verkeer Regel Installatie
Aanduiding: iVRI-Ready
Dit is een iVRI die draait op traditionele CCOL regelingen en nog niet is voorzien van een slimme regeling. De installatie is maximaal voorbereid en kan eenvoudig opgewaardeerd worden tot een volwaardige iVRI. De iVRI-Ready beschikt over betere specificaties ten aanzien van Informatiebeveiliging.

Elke nieuw te plaatsen Verkeer Regel Installatie moet voldoen aan moderne eisen ten aanzien van Informatiebeveiliging. De iVRI's zijn een aanzienlijke stap vooruit op dit vlak maar de eisen die worden gesteld aan de kwaliteit van de netwerkverbinding maakt het onmogelijk op elke willekeurige locatie een iVRI te plaatsen. Er wordt ook niet automatisch gekozen voor het gebruik van intelligente regelingen.

De iVRI-Ready

In het kader van deze aanbesteding worden daarom Verkeer Regel Installaties uitgevraagd die voorzien zijn van de verbeterde specificaties ten aanzien van Informatiebeveiliging, maar die standaard zullen draaien op basis van traditionele CCOL regelingen. Het opwaarderen van een iVRI-Ready naar een volwaardige iVRI moet eenvoudig mogelijk zijn.

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

Toelichting op de hosting omgeving

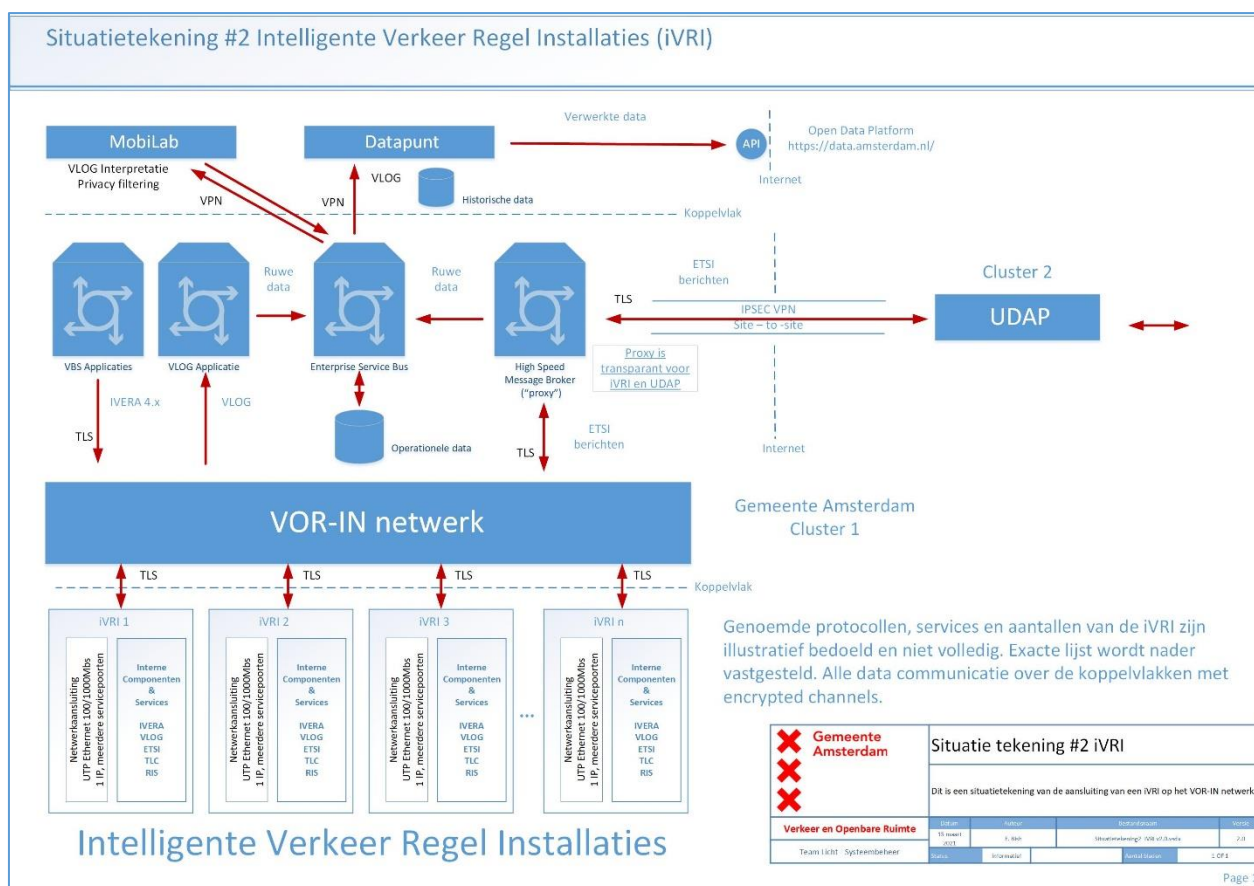
De hosting omgeving van Verkeer en Openbare Ruimte bestaat uit netwerkvoorzieningen zoals toegelicht in de vorige hoofdstukken en uit de mogelijkheid applicatie servers te laten draaien. Het besturen van de (i)VRI's gebeurt door de applicatie suite "Verkeer Beheer Systeem" (VBS). Deze suite bestaat uit verschillende client-server applicaties die op de servers en bedienposten draaien.

Het is mogelijk om aanvullende of ondersteunende applicaties voor het beheren van de (i)VRI's in de hosting omgeving onder te brengen. Hiervoor moet een aanvraag gedaan worden door de opdrachtnemer en het ingediende plan zal worden beoordeeld op technische haalbaarheid, kosten, beheer en cybersecurity aspecten.

De hosting omgeving wordt gevormd door meerdere Hyper-V hyperconverged cluster opstellingen op basis van Microsoft Windows Server 2016 of nieuwer. Op dit virtualisatie platform draaien zowel Virtuele machines op basis van Windows Server 2016 of nieuwer als ook Redhat Enterprise Linux (RHEL). Het standaard database platform is MS SQL. Er wordt gewerkt aan een bredere ondersteuning en andere aanvullende hosting faciliteiten, maar op het moment van schrijven van dit stuk kan daar nog geen definitieve toezegging over gedaan worden.

Het datacenter is voorzien van een hoogwaardige redundante Internetkoppelingen. Het is mogelijk IPSEC site-to-site VPN verbindingen met datacenters van andere leveranciers of ketenpartners te leggen. Indien noodzakelijk, dan zijn hier aansluitvoorwaarden op van toepassing. Het is niet mogelijk cliënt-to-site VPN inbelverbindingen op te zetten. Toegang op afstand wordt alleen op basis van de Telewerkvoorziening gegeven en voorziet niet in always-on verbindingen met het netwerk.

Hieronder staat een situatie tekening voor de positie van de iVRI en bijbehorende data stromen in het VOR-IN netwerk:



Ten aanzien van iVRI beheer wordt vermeld dat er in de hosting omgeving een Enterprise Service Bus voor data toepassingen aanwezig is. VLOG-data van alle (i)VRI's wordt structureel en op eenduidige wijze ingewonnen. Privacy gevoelige elementen in de VLOG datastroom worden verwijderd en verkeerskundige parameters bepaald door de uitwisseling met Mobilab. Voor de iVRI's is een dataproxy (high-speed messagebroker) aanwezig om alle communicatie tussen de iVRI's en het landelijke overnamepunt UDAP via één beveiligd kanaal te laten verlopen en tegelijkertijd de ETSI berichten voor verkeersanalyses op de ESB te kunnen plaatsen.

Voorzieningen in het datacenter zijn zoveel als mogelijk redundant uitgevoerd. Er wordt ook gewerkt aan een 2^e datacenter. In dat licht gezien kunnen geen fysieke systemen van leveranciers of ketenpartners geplaatst worden omdat daarvoor geen fail-over functionaliteit mogelijk is. Ondersteunende applicaties voor (i)VRI beheer kunnen alleen in de vorm van virtuele servers beschikbaar gesteld worden.

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

Het datacenter van Verkeer en Openbare Ruimte is gevestigd in een moeilijk toegankelijke locatie. De mogelijkheid om koppelvlakken van telecomproviders te realiseren is daarom zeer beperkt. Op dit moment beschikt het datacenter over koppelvlakken van Colt Telecom, KPN, Ziggo, en Netwerk Metro Amsterdam (NMA).

Er wordt op grote schaal gebruik gemaakt van VPN-verbindingen over mobiele dataverbindingen voor het aansluiten van de objecten in de openbare ruimte op de hosting omgeving. Helaas zijn deze verbindingen minder van kwaliteit dan vaste verbindingen. In het bijzonder wordt opgemerkt dat mobiele dataverbindingen periodiek gereset worden door de provider en dat de communicatie met de (i)VRI daarmee wordt onderbroken voor enkele minuten per keer. De onderliggende VPN-verbinding en de verbinding met de applicatie moet automatisch opnieuw worden opgebouwd.

Voor de (i)VRI betekent dit:

- Data moet lokaal in de (i)VRI gebufferd worden en na terugkomst van de verbinding alsnog verstuurd worden.
- De buffering moet voldoende groot zijn om onderbrekingen van minimaal enkele uren te kunnen overbruggen. (Bijvoorbeeld ten gevolge van stroomstoringen elders in de keten.)
- De (i)VRI moet tolerant zijn ten aanzien van wegvallende sessies met de applicatieservers. De lokale netwerkverbinding tussen (i)VRI en het data communicatie apparaat kan wel als stabiel beschouwd worden.
- Het is toegestaan vanuit de (i)VRI's op een lage frequentie (enkele keren per minuut) een PING commando te versturen naar een systeem in het datacenter om daarmee beschikbaarheid van de netwerkverbinding voor de (i)VRI automatisch te kunnen bepalen.

NB. Vereisten ten aanzien van functioneel fail-safe gedrag van de (i)VRI maakt geen onderdeel uit van dit document.

	Systeemdocumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
---	---

Informatiebeveiliging en privacy

De afgelopen jaren wordt door de Nederlandse overheid gewerkt om de digitale weerbaarheid van systemen sterk te verbeteren. Het algehele veiligheidsbewustzijn en de kwaliteit van de systemen moet sterk verbeterd worden. Het doel is betrouwbare en stabiele werking van cruciale digitale infrastructuur van de overheid.

De gemeente Amsterdam moet als onderdeel van de Nederlandse overheid voldoen aan de richtlijnen en kaders zoals die bestaan ten aanzien van Informatiebeveiliging en Privacy wetgeving.

Onder specifieke omstandigheden wordt de data die omgaat in de (i)VRI geclassificeerd als privacy gevoelig en bepaalt daarmee dat aan het gehele (i)VRI applicatieketen zwaardere eisen worden gesteld ten aanzien van informatiebeveiliging. De (i)VRI wordt gezien als een volledig networked device. Digitale kwetsbaarheden kunnen direct of indirect nadelige gevolgen hebben voor de verkeersveiligheid en moeten daarom altijd voorkomen worden en bij constatering direct opgelost worden. “Security & Privacy by design” is het belangrijke principe van waaruit gewerkt wordt.

Informatiebeveiliging

Voor Informatiebeveiliging moet het normenkader zoals beschreven in de Baseline Informatiebeveiliging Overheid (BIO) aangehouden worden.

Op hoofdlijnen komt het erop neer dat de (i)VRI's onderdeel van een applicatieketen zijn. Deze keten moet met technische, logische, fysieke en procedurele maatregelen beschermd worden tegen misbruik. De maatregelen zijn gebaseerd op een risico analyse en worden periodiek herzien.

- Apparatuur moet degelijk zijn uitgevoerd waardoor het niet eenvoudig mogelijk is misbruik te maken.
- Pogingen tot misbruik of niet correct functioneren van apparatuur moet gedetecteerd worden.
- De apparatuur moet pro-actief onderhouden en bij-de-tijd gehouden worden.
- Activiteiten moeten in een logboek worden opgenomen.
- Digitale identiteiten zijn uniek en niet deelbaar.
- Data wordt uitgewisseld via beveiligde kanalen.
- Data wordt niet doelloos ingewonnen en niet langer (lokaal) opgeslagen dan noodzakelijk.
- De kwaliteit van de keten wordt periodiek getoetst en maatregelen herzien of aangescherpt.
- De maatregelen en controls zijn zowel technisch als procedureel van aard.

Er is een interpretatie van de BIO voor Verkeer Regel Installaties alsmede een bijpassende leeswijzer opgesteld. Deze documenten maken deel uit van de aanbestedingsstukken.

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

Privacy

Sinds 25 mei 2018 geldt in de hele EU dezelfde privacywetgeving: de Algemene Verordening Gegevensbescherming (AVG).

Op de website van de autoriteit persoonsgegevens is alle relevante informatie te vinden.

<https://autoriteitpersoonsgegevens.nl/nl>

In het algemeen is er in de (i)VRI applicatieketen geen sprake van het verwerken van persoonsgegevens. De gegevens van detectielussen of andere signalen zijn niet rechtstreeks te relateren aan een specifiek persoon. Er zijn echter specifieke situaties waarbij wel sprake is van data die als persoonsgegevens aangemerkt kunnen worden.

Voorbeelden:

- KAR berichten (KAR = Korte Afstand Radio) zijn te relateren aan een specifieke bestuurder van een voertuig dat het bericht uitzond.
- Sommige van de ETSI berichten⁷ in de (i)VRI keten zijn aangemerkt als persoonsgegevens. In het bijzonder gaat het om de “Co-operative Awareness Messages” (CAM) die herleidbaar zijn naar specifieke weggebruikers of voertuigen.
- Uit VLOG-data kan opgemaakt worden wanneer begeleidingen voor VIP’s zijn ingezet.

Dit impliceert dat de gehele applicatieketen aan hogere informatiebeveiligingseisen moet voldoen om de correcte verwerking van de privacy gevoelige data te kunnen garanderen. Er moet bekend zijn welke privacy gevoelige data elementen door het systeem verwerkt worden. Deze data-elementen moeten passen bij de doelbinding van het systeem. De verwerking van data in de keten moet beschreven zijn en vastgesteld door juristen.

⁷ Zie voor een definitie van de berichten <https://www.etsi.org/technologies/automotive-intelligent-transport>.

	Systeemdocumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
---	---

Aansluitvoorwaarden

Het industriële netwerk van de Gemeente Amsterdam is het digitale hart van een aantal applicatieketens. Deze ketens bestaan uit apparatuur zoals sensoren en besturingen geplaatst in de openbare ruimte, applicaties in het Datacenter, bedienposten op kantoorlocaties en datakoppelingen met ketenpartners en leveranciers.

Het netwerk heeft een aanzienlijke omvang en dient aan moderne beveiligingseisen te voldoen. Hierdoor is het niet mogelijk elke willekeurige applicatie of verbinding te realiseren. Uitsluitend door te werken met standaard bouwstenen kan de kwaliteit en stabiliteit geborgd worden.

De applicatieketens moeten ook ondersteund kunnen worden door de eigen Servicedesk, maar evengoed verbonden zijn met Servicedesks van leveranciers en ketenpartners.

Dit resulteert in de volgende lijst met voorwaarden om een succesvolle implementatie te kunnen doen:

1. Principe's

- Security & Privacy by design. Werken volgens kaders en wetgeving.
- Areaal scheiding op netwerkniveau. Geen ongecontroleerde vermenging van toepassingen.
- Reductie van koppelvlakken: 1 koppelvlak per ketenpartner of leverancier.
- De koppelvlakken zijn de heldere en duidelijke grenzen van beheer en verantwoordelijkheid.
- Koppelingen op Datacenter niveau, niet op applicatieniveau.
- Koppelingen over Internet op basis van IPSEC site-to-site VPN.
- Standaard Telewerk voorziening, geen "back doors".
- Data uitwisselingen over de grenzen van het VOR-IN netwerk zijn altijd encrypted.
- Primaire functionaliteit draait altijd "on-premise".

2. Documentatie en ondersteuning

Elke applicatieketen moet volledig gedocumenteerd zijn waarbij het niveau en detaillering geschikt is voor ondersteuning door de Servicedesk. Van elke component in de keten moet duidelijk zijn wie er verantwoordelijk voor is en hoe eventuele storingen gemeld en geëscaleerd kunnen worden. Wijzigingen en storingen worden gemeld aan de Servicedesk:

e-mail : servicedesk@vorin-amsterdam.nl

Telefoon : 020 254 5294

Bereikbaar op werkdagen van 07:00 – 19:00 uur.

Meldingen, aanvragen of andere activiteiten zullen door de Servicedesk worden geaccepteerd op basis van meldingen van vooraf aangemelde vaste contactpersonen.

3. Enterprise Service Bus

Applicaties die data verwerken in de vorm van berichten, VLOG en C-ITS ETSI berichten zijn daarvoorbeelden van, worden met een applicatie specifieke connector op de Enterprise Service Bus aangesloten. De uitvoer van de ESB is gestandaardiseerd in JSON-formaat. Directe koppeling op

	Systeemdokumentatie Titel : De (i)VRI in het IT-landschap. Auteur : XX Datum : 1 april 2021 Versie : 1.0
--	---

de ESB is ook mogelijk als aan een gestandaardiseerd JSON-format voldaan kan worden. Er is een apart document opvraagbaar voor details van koppelingen met de Enterprise Service Bus.

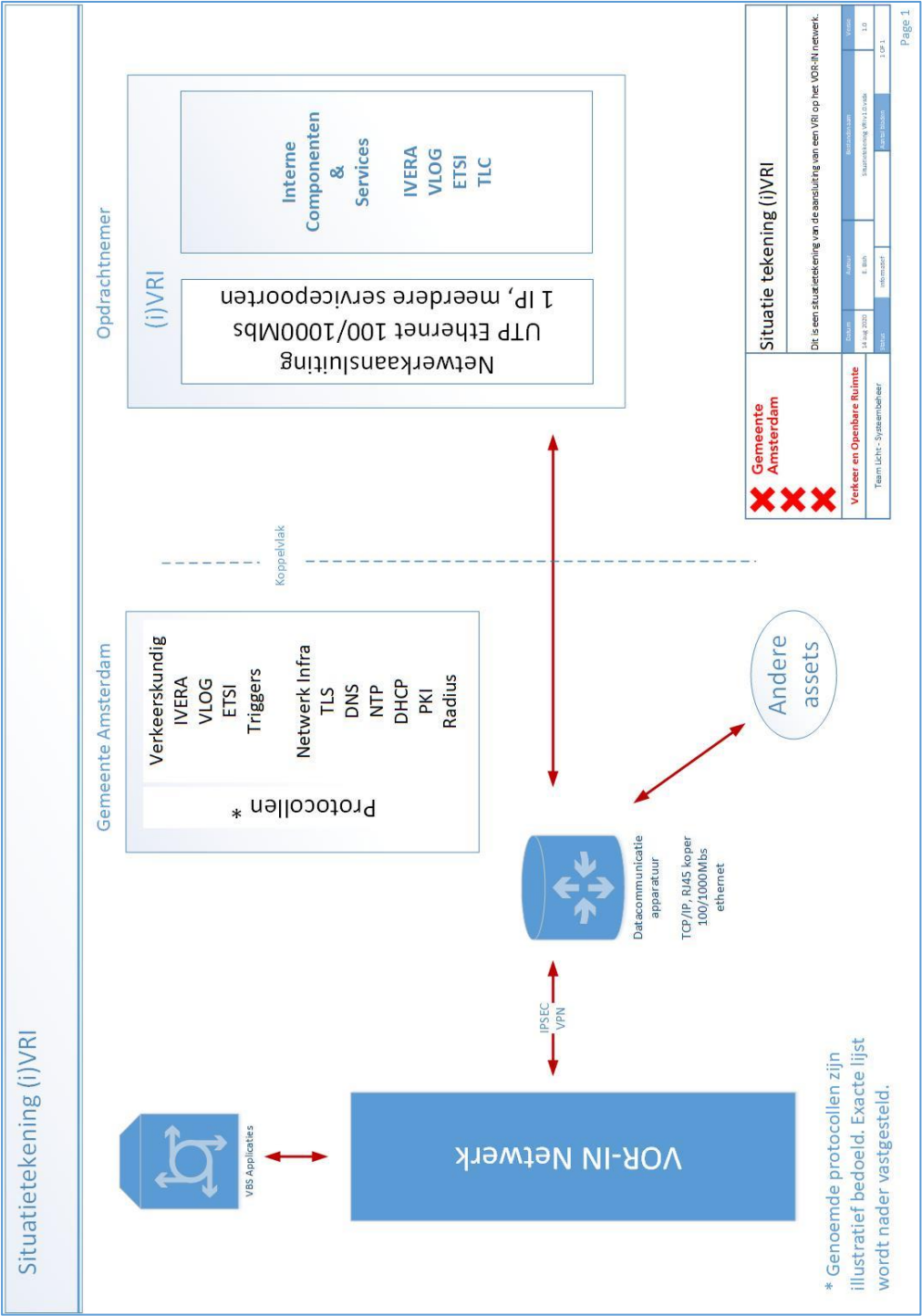
4. **Virtualisatieplatform en ondersteunde besturingssystemen.**

De VOR-IN hosting omgeving is gebaseerd op Microsoft Hyperconverged Hyper-V clusters. Op deze clusters draaien Windows Server 2016 (of nieuwer) en Redhat Enterprise Linux (RHEL) virtuele servers. Het standaard database platform is MS SQL.

5. **Stepping stone principe voor beheer op afstand.**

Leveranciers en ketenpartners krijgen via een managementserver geplaatst in het juiste applicatie segment toegang voor beheer. De toegang is gepersonaliseerd en beveiligd met een Azure 2-Factor autorisatie op basis van een App op de Smartphone van de support engineer. Het aantal personen dat toegang krijgt wordt geminimaliseerd en nut & noodzaak wordt periodiek herzien. Op de managementserver wordt door de VOR-IN systeembeheerders de noodzakelijke applicaties geïnstalleerd die nodig zijn voor het beheer van het areaal.

Bijlage 2 Situatietekening1 (i)VRI



Bijlage 3 Situatietekening2 (i)VRI

