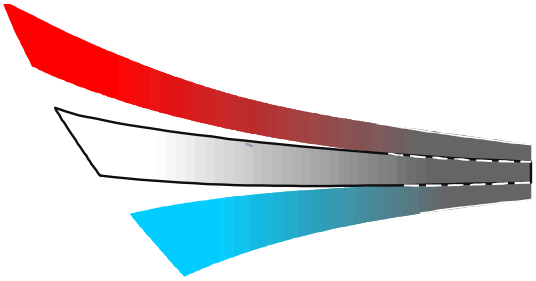


IVERA

Technische specificatie

Versie 2.10

3 november 2008

Een uitgave van
Stichting Beheer IVERA protocol
Zoetermeer, Nederland

Pub. No.: IVERA TS 2.10

Datum: 3 november 2008

Titel: IVERA Technische specificatie (versie 2.10)

Mocht u fouten of onvolledigheden ontdekken, of suggesties voor verbetering hebben, dan stellen wij het zeer op prijs, als u deze stuurt naar:

Stichting Beheer IVERA protocol
Postbus 190
2700 AD Zoetermeer

Voorwoord

Nederland kent een groot aantal geregelde kruispunten voorzien van verkeersregelinstallaties. De verkeersregelinstallaties zijn in beheer bij rijkswaterstaat, provincies en gemeentes. Voor een adequaat beheer van de verkeersregelinstallatie is uniformiteit in beheer een noodzaak, vooral voor beheerders met verkeersregelinstallaties van verschillende fabrikanten in hun park.

Het IVER en ASTRIN hebben de noodzaak tot standaardisatie onderkend en hebben de wens uitgesproken in de toekomst alle nieuwe verkeersregelinstallatie te voorzien van een gestandaardiseerde communicatie-interface voor de communicatie met een beheerscentrale.

Enkele jaren geleden leidde dit tot het verschijnen van een eerste versie -1.30- van het IVERA-protocol. Inmiddels is deze versie van het protocol in gebruik in meer dan 500 verkeersregelinstallaties.

Nu er enige tijd ervaring is opgedaan met het gebruik van dit protocol, wordt de behoefte gevoeld bij wegbeheerders en fabrikanten het protocol te verbeteren en uit te breiden op basis van die ervaring.

Dit heeft geleid tot het door de Technische Werkgroep van de Stichting Beheer IVERA-protocol opstellen van een specificatie voor versie 2.10 van het protocol.

Deze specificatie bestaat uit de volgende documenten:

- Een functionele specificatie van het IVERA-protocol (niet toepassingspecifiek).
- Een beschrijving van alle objecten en hun eigenschappen zoals die voorkomen in de toepassing van het IVERA-protocol voor de communicatie tussen een verkeersregelinstallatie en een beheerscentrale.
- Een technische specificatie

Inhoudsopgave

1. Samenvatting

Het IVERA-protocol is de bovenste laag in de communicatie structuur; de zogeheten applicatie laag. Het is alleen toepasbaar wanneer de onderste lagen de randvoorwaarden voor het gebruik van IVERA voor hun rekening nemen. Deze randvoorwaarden zijn foutvrije gegevensoverdracht en master/slave verbindingen.

Aan deze voorwaarden wordt voldaan door een op TCP/IP gebaseerde oplossing. Om een en ander te realiseren is het noodzakelijk dat een opzet voor het bijbehorende netwerk wordt gemaakt. Hierbij wordt rekening gehouden met:

- vastlegging van te gebruiken IP-adressen en
- definiëren van te gebruiken poorten

Op globaal niveau wordt per wegbeheerder een of meer (sub-)netwerkadressen uitgegeven. De wegbeheerder is zelf verantwoordelijk voor het toekennen van de adressen per netwerk node (bijvoorbeeld beheerscentrale of VRI). Wel moet hij hierbij voldoen aan de in dit document gestelde regels. Op deze wijze heeft elk element dat gebruik maakt van het IVERA-protocol een uniek adres.

Voor het opbouwen van de verbinding zijn per netwerknode één of meer poorten gedefinieerd waarop verbindingsverzoeken binnen komen. Er kunnen meerdere connecties tegelijk gemaakt worden op een poort.

2. Inleiding

Het IVERA-protocol is een initiatief van het IVER, CVN en ASTRIN. Het IVERA-protocol beoogt een fabrikant onafhankelijke communicatie tussen verkeersregelinstallaties en een beheerscentrale door middel van vastlegging van gegevensuitwisseling op applicatie niveau. Om tot daadwerkelijk fabrikant onafhankelijk gebruik van het protocol te komen, moeten aan de infrastructuur eisen worden gesteld.

Dit document beschrijft de ondersteunde infrastructuur en bijbehorende (software) lagen. Het resultaat hiervan is een overzicht van eisen die aan enerzijds de verkeersregelaar en anderzijds de beheerscentrale gesteld worden. Tevens wordt vastgelegd hoe verbindingen totstandkomen en hoe gegevens uitgewisseld moeten worden.

Bij de definities in dit document wordt rekening gehouden met ondersteuning van:
- vaste verbindingen
- telefoon(kies)lijnen
- eigen netwerken

- ISDN
- GSM
- GPRS
- WLAN

Bij het opstellen van de eisen ten aanzien van de communicatie-infrastructuur is het uitgangspunt een open, dynamische en standaard oplossing. Op dit moment biedt de techniek TCP/IP als netwerk protocol een oplossing die voldoet aan deze eisen. Dit document gaat daarom uit van een oplossing gebaseerd op TCP/IP en geeft aan hoe met eventuele uitzonderingssituaties omgegaan moet worden.

TCP/IP levert virtuele verbindingen. Dit betekent dat over eenzelfde fysieke verbinding meerdere verbindingen actief kunnen zijn. Hierdoor is het netwerk niet belemmerend om tegelijkertijd met een VRI verschillende vormen van communicatie te hebben.

2.1 Referenties

Ref	Document		datum	auteur
[1]	IVERA Functionele specificatie 2.10		TBA	Technische Werkgroep IVERA
[2]	IVERA Objectdefinitie Verkeersregelinstallatie 2.10		TBA	Technische Werkgroep IVERA
[3]	TCP/IP and related protocols	(0-07-005553-X)	1992	Uyless D. Black
[4]	TCP/IP Illustrated Volume 1	(0-201-63346-9)	1994	W. Richard Stevens

TCP/IP en de gerelateerde standaard protocollen die in dit document worden genoemd, zijn gedocumenteerd in RFC documenten. Deze worden beheerd door de IETF (www.ietf.org).

2.2 Afkortingen

ASTRIN	Association of Traffic Industries in the Netherlands
CVN	Contactgroep Verkeersregeltechnici Nederland
GSM	Global System Mobile

ISDN	Integrated Services Digital Nederland
IVER	Initiatiefgroep Verkeersregeltechnici Rijkswaterstaat en Provincies
IVERA	IVER en ASTRIN
LAN/WAN	Local Area Network / Wide Area Network
OSI	Open Systems Interface
PSTN	Public Switched Telephone Network
TCP/IP	Transmission Control Protocol / Internet Protocol
VRI	Verkeersregelinstallatie
RFC	Request for Comments.
IETF	Internet Engineering Task Force.
FTP	File Transfer Protocol.
PPP	Point to Point Protocol.

2.3 Begrippen

Beheersinstantie	Instantie belast met het beheer van een aantal VRI's.
Netwerknode	Adresseerbaar punt in het netwerk, b.v. een VRI of een Centrale.
Host	zie Netwerknode.

2.4 Doel

Dit document maakt technische afspraken waarmee een kader wordt gezet waarbinnen het IVERA-protocol is toe te passen. Enerzijds heeft dit consequenties voor de VRI's met betrekking tot de ondersteuning van bijvoorbeeld TCP/IP. Anderzijds heeft dit consequenties voor de beheerscentrale(s) met betrekking tot bijvoorbeeld de manier waarop verbindingen totstandkomen.

Het doel is te komen tot een fabrikantonafhankelijke oplossing waarbij een beheerscentrale met iedere automaat kan communiceren.

2.5 Aanpassing van dit document

2.5.1 Nieuw in versie 2.10

Versie 2.10 bevat een groot aantal wijzigingen ten opzichte van versie 1.30. Deze wijzigingen omvatten zowel kleine verbeteringen als forse uitbreidingen van de functionaliteit.

Hieronder wordt volstaan met een overzicht van de voornaamste wijzigingen/uitbreidingen:

- Aanpassingen n.a.v. Addendum op versie 1.30 verwerkt in tekst.
- Standaard methode "FTP" laden van programma's beschreven.
- Ondersteuning TCP-poort 7000 t.b.v. IBER/UBER-communicatie.
- Ondersteuning TCP-poort 7001 t.b.v. MON_IBER/MON_UBER-communicatie.

3. Protocollen

Het IVERA-protocol zoals beschreven in [1] geeft een definitie van het protocol op applicatie niveau. De eisen die in [1] aan de onderliggende (software) lagen worden gesteld, zijn:

- opzetten en instandhouden van de verbinding,
- foutloos en in dezelfde volgorde versturen van berichten,
- oplossen van routering,
- prioriteren van IVERA-berichten bij parallelle verbindingen,
- comprimeren van data,
- encryptie van data en
- melden van het totstandkomen en verbreken van verbindingen.

Naast deze eisen moet het geheel zo open, dynamisch en standaard mogelijk zijn waardoor implementatie-inspanning tot een minimum beperkt wordt.

3.1 TCP/IP

De TCP/IP protocol suite is opgebouwd rondom de kernlagen TCP en IP. Verder bestaan er inmiddels veel ondersteunende tools en protocollen die het gebruik van TCP/IP vereenvoudigen. Deze tools worden in dit document buiten beschouwing gelaten wat niet betekent dat ze ontoepasbaar zijn. De boeken vermeld onder [3] en [4] geven gedetailleerde informatie.

De eigenschappen van IP zijn:

- **connectionless**
  IP vereist geen point-to-point verbinding met de andere zijde. Berichten worden het netwerk op gestuurd naar de eerstvolgende node (bepaald door de Router). Mocht het hierdoor noodzakelijk zijn een bepaalde fysieke verbinding op te bouwen dan zal de fysieke laag dit oplossen.
- **onbetrouwbaar**
  IP verzorgt alleen het versturen van berichten. Er vindt geen controle plaats of berichten correct aankomen aan de andere zijde. Bij fouten worden de berichten eenvoudig weggegooid.

IP verzorgt dus alleen het transport over het netwerk. De te versturen berichten worden ingepakt en verzonden. De ontvangende kant kan deze berichten uitpakken en verder verwerken. Tijdens het inpakken worden onder andere de adressen van zender en ontvanger in het bericht geplaatst.

De eigenschappen van TCP zijn:

- **connection-oriented**
  TCP gaat uit van een verbinding met de andere zijde. Bij het versturen van berichten wordt eerst de verbinding opgebouwd. Pas als dit gelukt is, zal de informatie daadwerkelijk overgestuurd worden.
- **betrouwbaar**
  TCP voert controle uit op het berichtenverkeer. Op elk verstuurd bericht moet een antwoord volgen wat aangeeft of het bericht al dan niet is aangekomen. Bij fouten wordt de informatie nogmaals verstuurd.
- **concurrent connection**
  TCP ondersteunt meerdere logische verbindingen tegelijkertijd over dezelfde fysieke verbinding.

Omdat IP verantwoordelijk is voor het versturen, hoeft TCP alleen de controle op het berichtenverkeer uit te voeren. De combinatie TCP/IP vormt een betrouwbaar, connection-oriented protocol voor het versturen van berichten over een netwerk. De omvang van het netwerk maakt hierbij voor het versturen niet uit door de toepassing van Routers die netwerkpaden specificeren. Voor de tijd dat een bericht onderweg is, maakt dit route mechanisme echter wel uit. Het aantal nodes dat een bericht passeert, bepaalt de duur dat een bericht onderweg is. In het geval van een IVERA-netwerk is het voor de performance van belang dat het aantal te passeren nodes klein blijft.

De combinatie TCP/IP maakt zich niet druk over de fysieke samenstelling van het netwerk. Hierdoor kan een TCP/IP netwerk opgebouwd worden uit talloze soorten fysieke verbindingen met ieder hun eigen specifieke kenmerken.

Omdat configuratie van uitgegeven netwerk (IP) adressen en de relatie tot de fysieke laag vastgelegd wordt in de Router(s) van het netwerk maakt het voor het netwerk geen verschil via welke fysieke lagen de verschillende nodes zijn aangesloten. Wel maakt het verschil voor de performance van het geheel.

3.2 PPP

Voor het gebruik van IVERA over een seriële interface (of via een modem) wordt gebruik gemaakt van PPP. De voordelen van PPP zijn:

- ondersteuning van meerdere protocollen over een fysieke verbinding,
- controle per verstuurd (deel van een) bericht,
- compressie van de TCP/IP overhead mogelijk,
- linkprotocol voor dynamische bepalen van ondersteunde opties tijdens het opbouwen van de verbinding.

In combinatie met IVERA gelden de volgende PPP configuratie eisen:

- Het IP adres van het regeltoestel is geconfigureerd in het regeltoestel (vast IP adres).
- Server assigned IP-adressen worden niet ondersteund (dwz. als er wordt ingebeld in een regeltoestel zal het regeltoestel niet automatisch een IP adres toekennen aan de inbellende partij).
- In de PPP IPCP -fase moeten VRI en centrale een eigen IP-adres eisen. Het is echter wel toegestaan een IP-adres voor de PPP-peer voor te stellen ten behoeve van twee situaties; die waarbij een werkstation in de centrale inbelt en geen eigen IP-adres eist en die waarbij een centrale op laptop lokaal op het regeltoestel wordt aangesloten.
- De volgende gegevens kunnen in het regeltoestel dynamische worden ingesteld/gewijzigd.
    - Het IP-adres van de centrale.
    - Het telefoonnummer van de centrale.
    - Poort/socket van de centrale (default = 5001).
    - De events waarop de VRl de centrale gaat bellen.
- Op het moment dat een PPP-verbinding tot stand is gekomen wordt de PPP-verbinding automatisch de default gateway tot het moment dat de verbinding wordt verbroken.
- Indien er geen gebruikers zijn gedefinieerd (AUTHOG) is CHAP:MD5 uitgeschakeld en kan er zonder user/password worden ingebeld. Zodra er gebruikers zijn gedefinieerd, wordt CHAP:MD5 automatisch ingeschakeld. Als de gebruikers weer worden verwijderd, wordt CHAP:MD5 automatisch uitgeschakeld.

Voorts geldt dat de PPP interface aan de centrale kant niet noodzakelijkerwijs de centrale zelf hoeft te zijn. Dit zou ook een network access server kunnen zijn. Dit is de reden dat de VRI de PPP peer als default gateway moet instellen.

3.3 Netwerken

Het IVERA-netwerk kent de volgende lagen met betrekking tot de communicatie:

- **Fysieke laag**

- **Linklaag**
  De linklaag verzorgt het totstandkomen van verbindingen met de gebruikte apparatuur. Dit kan uiteenlopen van een Ethernet verbinding tot een verbinding met behulp van Radio communicatie. Voor elk type verbinding moet een implementatie van de linklaag beschikbaar zijn. In de volgende paragrafen wordt een aantal mogelijkheden behandeld.
- **Netwerklaag**
  De netwerklaag verzorgt het transport van berichten over het netwerk. Hiervoor is IP verantwoordelijk.
- **Transportlaag**
  De transportlaag verzorgt het foutloos versturen van berichten. Hiervoor is TCP verantwoordelijk.
- **Applicatielaag**
  De applicatielaag is het IVERA-protocol zelf. Doordat de combinatie van link, netwerk en transport laag aan de definities van het IVERA-protocol (***met uitzondering van prioriteren***) voldoet, kan het IVERA-protocol direct op de TCP laag geplaatst worden. Het comprimeren en encrypten van gegevens is afhankelijk van de toegepaste linklaag.

Elk van deze lagen moet opgebouwd worden tussen VRI en centrale. Om enigszins onderscheid te maken tussen de "verbindingen" op de verscheidene lagen, wordt in de IVERA-specificatiedocumenten onderscheid gemaakt tussen een verbinding maken en een connectie maken. Verbindingen worden op de fysieke laag gemaakt, bijvoorbeeld wanneer een modemverbinding tot stand is gekomen (carrier detect of "CONNECT string"), of wanneer een ethernetkaart de switch "ziet". Voor datalinkprotocollen zoals PPP wordt ook over verbinding gesproken, zei het expliciet een PPP-verbinding. Voor TCP/IP werken laag 3 en 4 samen, en wordt er over een connectie gesproken.

3.3.1 Ethernet

De meest voorkomende fysieke verbinding in combinatie met TCP/IP is Ethernet. Deze fysieke laag wordt binnen het IVERA-netwerk toegepast bij het verbinden van de Centrales en de werkstations. Ook het gebruik van fabrikantafhankelijke subnetwerken komen hiervoor eventueel in aanmerking. Het is zelfs mogelijk (een deel van) het arsenaal aan VRI's via een Ethernetverbinding aan het netwerk te koppelen.

Voor het gebruik van Ethernet zijn op nagenoeg alle platformen implementaties beschikbaar. Het is daarom niet nodig de software voor deze fysieke laag zelf te implementeren.

3.3.2 Analoge inbelverbinding

Bij het gebruik van IVERA via telefoonlijnen wordt als protocol PPP gebruikt.

- In het geval dat er geen IP communicatie meer plaatsvindt over de PPP verbinding zal het regeltoestel de PPP en modem verbinding na enige tijd verbreken.

- In het geval dat het regeltoestel de centrale belt zal het regeltoestel een beperkte tijd wachten op het totstandkomen van de modemverbinding.
- Het wachten op het totstandkomen van een PPP verbinding heeft een time-out
- Het wachten op het openen van de triggerpoort door de centrale heeft een time-out.
- Het wachten op een response van de centrale (het openen van poort 5000) heeft een time-out.
- In het geval van een fout bij het bellen naar de centrale zal het regeltoestel het een aantal keren na enige tijd opnieuw proberen.

De waardes van de verschillende time-outs en andere variabelen die de behandeling van de verbindingsopbouw bepalen, zijn vastgelegd in het object DATACOM.

Nadat het aantal maximum retries is overschreden, gaat de VRI over op een exponentieel back-off mechanisme; de retry time wordt na elke poging verdubbeld (bijv.3, 6, 12, 24 etc.). Wanneer de berekende back-off tijd groter is dan 24 uur, wordt de trigger toch gedropt.

Een modemverbinding kan op initiatief van zowel de centrale als de VRI (trigger melding) opgezet worden. Wanneer de modemverbinding eenmaal is gemaakt wordt de modemverbinding wegens de IVERA master-slave filosofie altijd op initiatief van de centrale weer verbroken. Bovengenoemde VRI time-outs blijven evenwel als fail-safe aan de VRI kant gehandhaafd.

3.3.3 GSM-verbinding

De werking bij het gebruik van een GSM verbinding is identiek aan een analoge inbelverbinding, met daarbij de volgende opmerkingen:

- In centrale wordt gebruik gemaakt van een vaste (analoge) telefoonverbinding.
- Het GSM-modem in het regeltoestel dient voorzien te zijn van een SIM-kaart met een data-abonnement. Bij een SIM-kaart met zowel voice als data dient het telefoonnummer van de dataverbinding te worden gebeld.
- Normaliter zal het regeltoestel de pincode invoeren in het GSM-modem (hiermee is een gestolen SIM onbruikbaar).

3.3.4 GPRS

Voor een verbinding op basis van GPRS zijn er in principe twee type abonnementen mogelijk. Het soort abonnement wordt bepaald door de gebruikte SIM-kaart.

- Verbinding met het internet
- Verbinding met een privé GPRS-netwerk.

Bij een internetabonnement heeft het regeltoestel rechtstreeks toegang tot het internet. Dit betekent concreet dat er "zware" beveiligingsmaatregelen noodzakelijk zijn om misbruik te voorkomen. De verbinding tussen de centrale en het regeltoestel is in dit geval gebaseerd op VPN (Virtual Private Network).
Bij een privé GPRS-netwerk wordt alle dataverkeer door de telecomprovider op een beveiligde manier door het netwerk verstuurd. Hiervoor is aan de zijde van de centrale wel een speciale server noodzakelijk.

Bij het gebruik van GPRS voor de communicatie tussen de IVERA-centrale en een regeltoestel is er sprake van drie betrokken partijen:

- De leverancier van de IVERA-centrale;
- De leverancier van het regeltoestel;
- De leverancier/beheerder van het GPRS-netwerk.

Bij de implementatie van een GPRS-netwerk zijn er diverse opties en keuzes die per netwerk dienen te worden ingesteld. Deze opties/keuzes worden in principe bepaald door de beheerder van het GPRS-netwerk.

Op dit moment is niet mogelijk om een eenduidige, fabrikant onafhankelijke, specificatie te

schrijven voor het gebruik van het IVERA-protocol over een GPRS-verbinding. Voor het gebruik van GPRS-communicatie is daarom het advies om in het regeltoestel een aparte 'GPRS-module' te plaatsen en deze via ethernet of een serielijn met PPP aan te sluiten op het regeltoestel. De beheerder van het GPRS-netwerk bepaalt welke 'GPRS- modules' compatibel zijn met het netwerk en als zodanig kunnen worden toegepast.

Het aansluiten van een GPRS-modem direct op het regeltoestel is technisch mogelijk, maar wordt bij een verbinding via het internet niet geadviseerd.

3.3.5 xDSL-verbinding

Door middel van xDSL-technologie is een breedbandige verbinding tussen centrale en regeltoestel mogelijk.

- ADSL-verbinding met het internet.
- xDSL-verbinding in een privé netwerk.

Voor het gebruik van xDSL-verbindingen geldt hetzelfde als voor GPRS-verbindingen. Het advies is een aparte 'xDSL-module' te gebruiken en deze via ethernet of een serielijn met PPP aan te sluiten op het regeltoestel. De beheerder van het netwerk bepaalt welke 'xDSL-modules' compatibel zijn met het netwerk en als zodanig kunnen worden toegepast.

Gangbare xDSL-varianten zijn: MDSL, SDSL, HDSL en SHDSL (G.SHDSL). Laatstgenoemde wordt waarschijnlijkheid de industriestandaard wegens het feit dat deze als enige internationaal ISO/ITU gestandaardiseerd is en het feit de TC-PAM lijnencoding beter is dan die van de andere varianten.

3.3.6 Vaste (leased-line)verbinding

De basis is dat er gebruik gemaakt wordt van (analoge) modems die zelfstandig zonder inbreng van de centrale of het regeltoestel een modemverbinding tot stand brengen. Zodra de modemverbinding tot stand is gekomen, kan er op initiatief van de centrale en/of het regeltoestel een PPP-verbinding worden opgebouwd. Voor de PPP-verbinding zijn er diverse variaties:

Opmerkingen over leased-lineverbindingen:

- Het modem dient met volledige modem control (DTR, DSR, CTS, RTS en DCD) te worden aangesloten op het regeltoestel.
- Het modem kan worden voorzien van een vaste configuratie (zonder verder configuratie vanuit het regeltoestel) of worden geconfigureerd vanuit het regeltoestel.
- Het gebruik van de CLIENT-CLIENTSERVER handshake is facultatief.

In leased-linemodus moet het ene modem als originating en het andere als answering modem geconfigureerd worden. Aangezien vanaf V.34 transmissiesnelheden asymmetrisch zijn en geoptimaliseerd voor download naar het originating modem, verdient het de voorkeur om de modems aan de centrale kant in originating mode te configureren

Bij het gebruik van leased-lineverbindingen zijn er twee betrokken partijen:

- De leverancier van de IVERA-centrale.
- De leverancier van het regeltoestel.

De leverancier van de IVERA-centrale bepaalt welke van de bovengenoemde instellingen worden gebruikt. Deze instellingen worden eenduidig vastgelegd en opgenomen in het bestek voor het leveren van een regeltoestel. Om compatibiliteitsproblemen te voorkomen dient de leveran-

cier van de IVERA-centrale tevens te specificeren welke modemtypes bij voorkeur dienen te worden gebruikt.

4. Apparatuur

In principe schrijft IVERA geen apparatuur voor. De wegbeheerder is verantwoordelijk voor de te gebruiken apparatuur om het netwerk te realiseren. Dit zal altijd in overleg moeten met de fabrikant(en).

- Bij het gebruik van GPRS/UMTS/xDSL-communicatie adviseert de netwerkbeheerder aan welke eisen de te gebruiken apparatuur moet voldoen en welke apparatuur bij voorkeur in het netwerk dient te worden toegepast.

- Bij gebruik van leased-lijnverbindingen stelt de leverancier van de IVERA-centrale een lijst van modems samen die compatibel zijn met de modems aan de kant van de centrale.

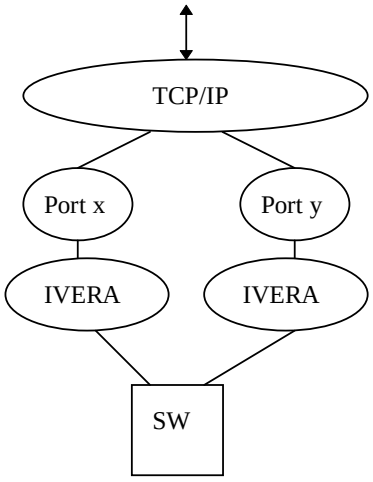
- De verkeersregeltoestellen ondersteunen ten minste IVERA over analoge telefoonlijnen met PPP en PPP over een seriële lijn. De beschikbaarheid van IVERA via ethernet met TCP/IP is optioneel.

5. Connecties

De Centrale is in een IVERA-connectie master, de VRI slave. De master is verantwoordelijk voor het opbouwen van de connectie. Dit hoofdstuk beschrijft hoe een connectie tot stand komt.

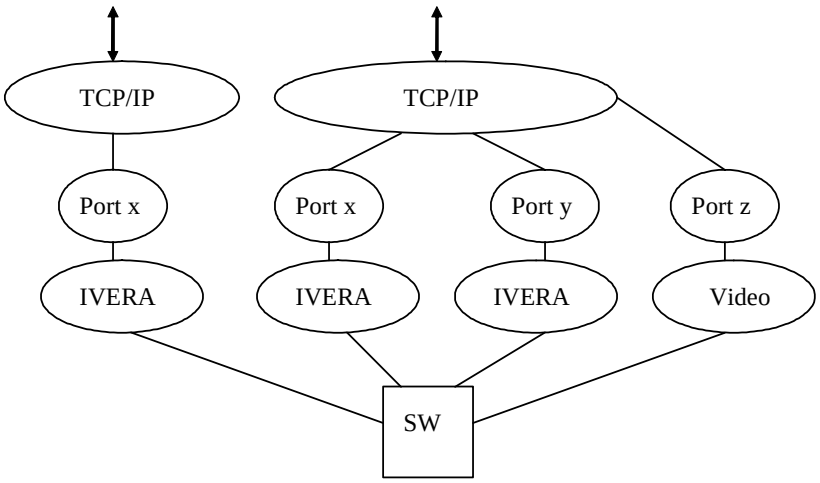
5.1 Socketconnecties

Socketconnecties zijn logische connecties via TCP/IP. Een socketconnectie definieert naast de IP-adressen van zender en ontvanger ook de poortnummers van beide partijen. Deze combinatie van vier elementen maakt de connectie uniek. Zodoende is het mogelijk meerdere logische connecties via één fysieke verbinding te behandelen.



Figuur 1 Twee logische IVERA-connecties in een VRI

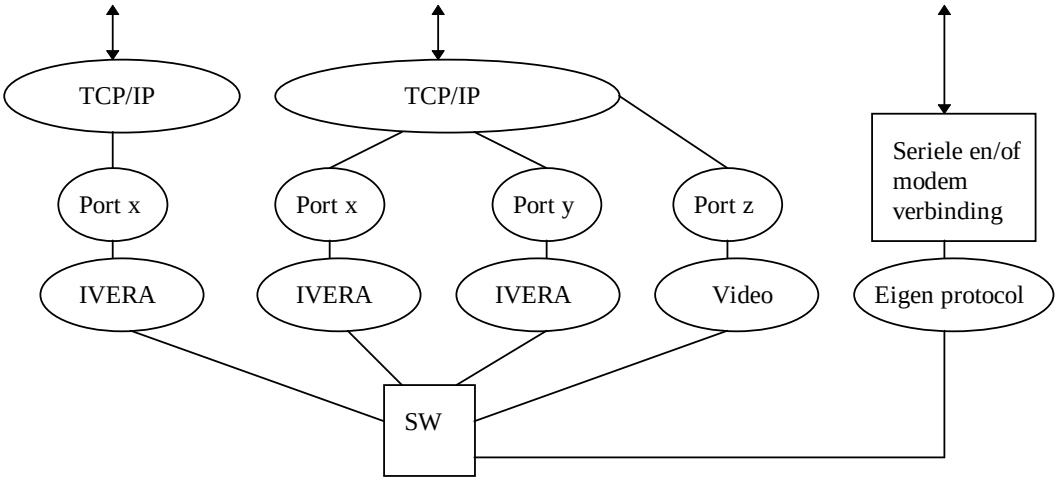
Het is ook mogelijk meerdere fysieke verbindingen in een VRI te ondersteunen. Dit betekent echter wel dat de VRI meerdere IP-adressen toegewezen krijgt. Over de TCP/IP-connecties kunnen ook andere applicatieprotocollen gebruikt worden. Onderstaand voorbeeld schetst een aan de VRI aangesloten videocamera die via een eigen socketconnectie zijn gegevens naar een centrale stuurt.



Figuur 2 Twee fysieke en vier logische connecties in een VRI

5.2 Eigen verbindingen

Bij het gebruiken van bestaande apparatuur en infrastructuur in het IVERA-netwerk kan het voorkomen dat VRI's moeten communiceren met een fabrikantafhankelijk protocol. Dit is ook van toepassing bij bijvoorbeeld onderhoud aan VRI's. Indien dit protocol geen gebruik maakt van een IP-netwerklaag, dient deze eigen verbinding fysiek naast de IVERA-netwerkverbinding te staan, zodat de IVERA-verbinding altijd tot stand kan komen.



Figuur 3 De fysieke en logische verbindingen aan een VRI

De eigen verbinding kan ook toegepast worden in het geval dat een Concentrator de TCP/IP verbinding simuleert en zelf de communicatie met de VRI's onderhoudt.

5.3 Poorttoewijzing

De toewijzing van poort nummers vindt plaats tijdens het opbouwen van de connectie. Deze paragraaf gaat alleen uit van IVERA-connecties.

De Centrale maakt een connectie met de VRI op een bepaalde poort. Hiervoor wordt poort 5000 gereserveerd. Dit betekent, dat de VRI altijd poort 5000 gereserveerd heeft voor binnenkomende connecties. Het is mogelijk meerdere connecties te realiseren. Natuurlijk kan de VRI de connectie ook afwijzen, wanneer bijvoorbeeld geen connectie meer mogelijk is.

De connectie wordt in de regel ook op initiatief van de centrale verbroken. Alleen in uitzonderlijke situaties (bijvoorbeeld afsluiten voor onderhoud) verbreekt de VRI de connectie.

Een VRI moet ten minste 4 gelijktijdige connecties kunnen toelaten.

5.4 Triggers

Naast het master-slave principe, is er binnen IVERA een mechanisme dat de VRI de mogelijkheid geeft de centrale te attenderen op een gebeurtenis; de triggermelding. Een triggermelding "triggert" de centrale om een gewone IVERA connectie te maken met de VRI in kwestie. Om triggermeldingen te ontvangen luistert de centrale standaard op poort 5001 voor inkomende triggers. Een VRI die een trigger wil melden, maakt een TCP/IP-connectie op deze poort. De centrale identificeert de VRI op basis van zijn IP-adres. Als het adres niet bekend is bij de centrale wordt het connectieverzoek geweigerd. De VRI verstuurt 1 of meer triggermeldingen over de connectie. De VRI verbreekt de connectie na het verzenden van de meldingen. Daarna kan de centrale een gewone IVERA connectie maken om detailinformatie op te vragen. Zie ook paragraaf 3.3.2 voor VRI-triggergedrag bij gebruik van kieslijnen.

6. Bijzondere vormen van communicatie met een VRI

6.1 Laden en dumpen van programma's

Om een VRI te voorzien van nieuwe (sub-)programma's dient gebruik gemaakt te worden van het standaard protocol "FTP", zoals beschreven in RFC 959. Door middel van dit protocol kunnen de programma's op een standaardmethode in de VRI geladen worden.

Opmerking: waar "programma" wordt genoemd kan ook "subprogramma" gelezen worden.

FTP-specificaties

- de FTP-server bevindt zich in de VRI; de FTP-client maakt onderdeel uit van de centrale.
- gebruik van gebruikersnaam/password/rechten is optioneel; echter, wanneer de server hier gebruik van maakt, dient de FTP-client dit te ondersteunen.
- mode waarin FTP werkt is binair
- de FTP-server dient minimaal 2 gelijktijdige verbindingen te ondersteunen (hiervan is minimaal 1 verbinding te gebruiken ten behoeve van het laden van een programma; daarnaast is er minimaal 1 andere verbinding beschikbaar ten behoeve van het overige FTP-verkeer (bijvoorbeeld het ophalen van logboeken of dumps).
- de volgende minimale set aan FTP-commando's wordt door de FTP server ondersteund:

FTP commando	Beschrijving
USER <naam>	Aanmelden gebruiker.
PASS <password>	Invoeren password, mag soms ook leeg zijn.
LIST	Ophalen lijst met bestanden volgens UNIX formaat.
NLST	Ophalen lijst met bestandsnamen.
SYST	Opvragen systeemtype (UNIX).
TYPE [<I> of <A>]	Bestandstype I (Image of binair) of A (ASCII).
PORT a1,a2,a3,a4,p1,p2	Instellen netwerk adres (a1, a2, a3, a4) en portnummer (p1, p2). Port = p1 * 256 + p2
CWD <pad>	Instellen pad.
PWD	Print de huidige directory.
RETR <bestandsnaam>	Opvragen bestand van FTP-server (lezen).
STOR <bestandsnaam>	Opsturen bestand naar FTP-server (schrijven).
DELE <bestandsnaam>	Het verwijderen van een bestand op de FTP server.
PASV	FTP server in passieve mode zetten.
QUIT	Afsluiten sessie met FTP-server.
NOOP	Pingen van FTP server (verversen sessie time-out).

Alle overige FTP commando's, welke in RFC959 zijn gespecificeerd, zijn optioneel.

- standaard FTP antwoord- en foutcodes worden gebruikt (zoals beschreven in RFC959)
- de leverancier van een regeltoestel beschrijft middels een sequence van FTP-commando's (script) op welke wijze een programma in het regeltoestel kan worden geladen.

6.2 Communicatie met poort 7000

Via TCP-poort 7000 zijn de IBER- en UBER-buffer van de CVN-interface bereikbaar. Via deze methode kunnen centrales meldingen welke de regelapplicatie in het UBER-buffer schrijft inlezen en opslaan.
Tevens is het voor de centrale mogelijk om zelf berichten in het IBER-buffer te plaatsen. Deze berichten kunnen dan bijvoorbeeld door de CCOL-parser afgehandeld worden.

Werking

- de VRI creëert bij opstarten een serversocket op TCP-poort 7000.

- wanneer een client een socketverbinding opgezet heeft, zal de procesbesturing er direct voor zorgen dat:
  - alle data die op de socket van de VRI binnenkomt in het IBER-buffer gezet wordt
  - alle data die de procesbesturing leest van het UBER-buffer naar de socket geschreven wordt
- het IBER/UBER-mechanisme in de CVN-interface heeft geen contextinformatie en is dus single-user georiënteerd. Door zowel de procesbesturing als de client het recht te geven om de socketverbinding te allen tijde te verbreken, kan de procesbesturing na het aanspreken van een fasebewaking een DUMP aanmaken, zonder dat de berichten van het UBER-buffer naar de socket geschreven worden.

Toepassingsvoorbeeld

Naast het automatisch aanmaken van een dump na aanspreken van de fasebewaking, is het ook mogelijk om handmatig het aanmaken van een dump te forceren.

Er zijn binnen CCOL diverse dumps mogelijk:
1. Dump van de regeling, commando DUMP
2. Dump van de groen standen, commando GDUMP
3. Dump van de parameterinstellingen, commando PDUMP
4. Registratie dump, commando RDUMP

De dump wordt over de C-interface aangeboden via CIFUBER. Deze informatie kan via TCP-poort 7000 door de centrale opgehaald worden.
De verschillende dumps kunnen gestart worden vanuit de centrale door het bedienen van een applicatieschakelaar. Omdat deze schakelaars gerepresenteerd worden door IVERA-schakelaars, kunnen deze vanuit de IVERA-centrale gezet worden. In de centrale behoeven dus geen extra voorzieningen getroffen te worden.
De procesbesturing zal, zodra een schakelaar opgezet wordt, de bijbehorende waarde in de CVN-interface opzetten. Hierdoor kan de CCOL-applicatie de betreffende dump middels de CCOL-variabelen (DUMP, GDUMP, …) starten.

De naam van deze schakelaars kan door de CCOL programmeur bepaald worden.

Voorbeeld:

Voor DUMP: cdump
Voor GDUMP: cgdump
Voor PDUMP: cpdump
Voor RDUMP: crdump

6.3 Communicatie via poort 7001

Via TCP-poort 7001 zijn de MON_IBER- en MON_UBER-buffer van de CVN-interface bereikbaar. Via deze weg is een on-line data-inwinmethodiek beschikbaar.

De werking van TCP-poort 7001 is identiek aan de werking van TCP-poort 7000. Uiteraard wordt de informatie in dit geval van de MON_IBER- en MON_IBER-buffer geschreven en gelezen.

7. Beveiliging

Deze paragraaf beschrijft de een aantal maatregelen voor de beveiliging van een IVERA-toestel tegen inbreuk door derden.

7.1 Aanleiding

De verbinding van het regeltoestel met de buitenwereld verloopt via TCP/IP en PPP. Daar dit standaard ‘open’ protocollen zijn, kan ‘iedereen’ met de beschikking over deze protocollen een verbinding opbouwen met het regeltoestel of de centrale waarvan het telefoonnummer bekend is. Op IVERA-applicatieniveau is een ‘beperkte’ autorisatie op basis van een pincode geïmplementeerd. De pincode bepaalt de toegang van de gebruiker tot de IVERA-objecten. Deze openheid van het systeem wordt als niet acceptabel ervaren.

Om het protocol verder te beveiligen is gezocht naar een oplossing die voldoet aan de volgende randvoorwaarden:

- Beveiliging door middel van het opgeven van gebruikersnaam en password.
- Bij foutieve invoer van gebruikersnaam en/of password wordt de verbinding automatisch verbroken.
- Mogelijkheid tot het wijzigen van de gebruikersnaam en password tijdens de levensduur van het regeltoestel.
- Mogelijkheid tot het gebruik van organisatie (of persoon) gebonden gebruikersnaam en password.
- Mogelijkheid om een externe partij “tijdelijk” toegang te geven tot het regeltoestel via een gebruikersnaam en password.

Een standaardoplossing die aan de randvoorwaarden voldoet is PPP/CHAP. In het regeltoestel is het hiermee mogelijk meerdere gebruikers te definiëren met een eigen gebruikersnaam en password. In het regeltoestel en de centrale wordt CHAP geïmplementeerd conform de standaard: RFC 1334 (PPP Authentication protocols. Algoritme: MD5). Voor gedetailleerde informatie over CHAP wordt verwezen naar RFC 1334.

7.2 Regeltoestel

Voor het gebruik van de beveiligingsfunctie is de volgende functionaliteit in het regeltoestel minimaal vereist:

Verbreken van de verbinding door het regeltoestel

Het regeltoestel is in de termen van RFC1334 een ‘authenticator’ en het regeltoestel specificeert welk ‘authentication protocol’ wordt gebruikt (CHAP:MD5). In het geval de andere kant zich niet weet te autoriseren wanneer dit door het regeltoestel wordt gevraagd verbreekt het regeltoestel automatisch de verbinding. Het regeltoestel moet ten minste eenmalig bij het opzetten van de verbinding (‘Link Establishment phase’) de inbeller autoriseren.

Melding in het logboek

In het logboek wordt minimaal gelogd:
- Het tot stand komen van een fysieke verbinding op poort 5000.
- Het verbreken van een fysieke verbinding (poort 5000).

Indien technisch mogelijk wordt gelogd:
- Een poging tot inbreuk in het systeem

7.3 Centrale

Als in de centrale CHAP wordt toegepast zal in het regeltoestel een gebruikersnaam + password moeten worden geconfigureerd voor toegang tot de centrale.

Het regeltoestel zal in de centrale inloggen met de gegevens van de 2e gebruiker. Dit voorkomt dat in het regeltoestel een extra gebruikersnaam + password moet worden opgeslagen en beheerd. Concreet betekent dit, dat, als de centrale om autorisatie vraagt aan het regeltoestel, het regeltoestel de sleutel berekent op basis van de 2e gebruikersnaam en password.

Er is gekozen voor een vast IP-adres per IVERA-node.

Het IP-adres wordt bepaald door de beheerder van het netwerk waarin de IVERA-node zich bevindt. Op deze wijze heeft iedere IVERA-node in het netwerk een uniek (en vast IP-adres).

NB. Door de toekenning van een vast IP-adres aan een IVERA-node is er een potentieel adres conflict indien wordt ingebeld in een IVERA-node vanuit een ander netwerk Een voorbeeld van zo'n conflict is het inbellen door een fabrikant terwijl de PC waarmee wordt ingebeld is opgenomen in het netwerk van de fabrikant en zich in het netwerk van de fabrikant een node bevindt met hetzelfde IP-adres als het IVERA-toestel.

Ter voorkoming van adres conflicten geniet het de voorkeur om een IVERA-toestel altijd te benaderen via de IVERA-beheercentrale door in te bellen in de IVERA-beheercentrale waarna de IVERA-beheercentrale een verbinding opbouwt met het IVERA-toestel.

De globale werkwijze voor het toekennen van IP-adressen is als volgt:
- Een opdrachtgever reserveert in overleg met zijn netwerkbeheerder een groep van IP-adressen voor IVERA-toestellen.
- Bij opdracht voor een IVERA-toestel wordt door de opdrachtgever het IP-adres van het regeltoestel, het IP-adres en het telefoonnummer van de IVERA-beheercentrale opgegeven aan de leverancier van het toestel.
- De leverancier van het IVERA-toestel configureert de gegevens in het IVERA-toestel.