



BRCONTROLS

Datacommunicatie Algemeen



Disclaimer

Alle rechten voorbehouden.

Het verspreiden van dit document is alleen toegestaan indien het document volledig en ongewijzigd wordt gelaten. Het is niet toegestaan specifieke gedeeltes uit dit document te verspreiden in welke vorm dan ook anders dan door de uitgever en/of auteur schriftelijk goedgekeurde gedeeltes.

Producten die worden genoemd in dit document kunnen handelsmerken en/of geregistreerde handelsmerken zijn van de eigenaars. De uitgever en de auteur maken geen aanspraak op deze handelsmerken anders dan de aan BRControls gelieerde handelsmerken.

Hoewel bij de samenstelling van dit document de grootste zorgvuldigheid in acht is genomen, is de uitgever en/of de auteur niet aansprakelijk voor fouten, of voor schade die voortvloeit uit het gebruik van de informatie gegeven in dit document, of uit het gebruik van de interne en/of externe programmatuur die eventueel aangegeven zijn. In geen geval zal de uitgever en/of de auteur aansprakelijke kunnen worden gesteld voor enig verlies van winst of iedere andere vorm van schade veroorzaakt, of indirect veroorzaakt, door gebruik van dit document.

© 2021 BRControls



BRControls wil het milieu graag ontzien door o.a. de papierstroom te beperken. Daarom hebben wij er voor gekozen zoveel mogelijk digitaal met u te communiceren en u te vragen, indien dit niet strikt noodzakelijk is, van dit document geen afdrukken te maken.

Wanneer u dit document toch dient te printen, recycle het dan a.u.b. na gebruik. Recycled papier is een waardevolle grondstof voor nieuwe producten.

Inhoudsopgave

1. Inleiding	5
1.1 Changelog	6
1.2 Scope	6
1.3 Behandelde datacom	6
2. Dataverkeer	7
2.1 Serieel vs Parallel	8
2.2 Baudrate / Bitrate	8
2.3 Opbouw van frame	9
2.4 Pakket	10
2.5 Bekabeling	10
2.6 RS-232	14
2.6.1 Aansluiting	14
2.6.2 Bustopologie	14
2.6.3 Signaalniveau's	14
2.6.4 Opbouw van frame	15
2.7 RS-485	16
2.7.1 Aansluiting	16
2.7.2 Bustopologie	16
2.7.3 Afsluitweerstand	18
2.7.4 Signaalniveau's	18
2.7.5 Opbouw van frame	19
3. Netwerkbegrippen	20
3.1 MAC adressen	22
3.2 IP adressen	24
3.3 ARP tabel	25
3.4 DHCP	26
3.5 Subnet / Netmasker	28
3.6 TCP	30
3.6.1 Poorten	30
3.6.2 Verbinden	31
3.6.3 Fouten	31
3.7 UDP	32
4. Talstelsels	33
4.1 Binair talstelsel	34
4.1.1 Boleaanse operatoren	37
4.2 Hexadecimaal talstelsel	39

Inhoudsopgave

4.3	Datatypes	41
4.3.1	Endianness	42



Hoofdstuk 1

Inleiding

1 - Inleiding

1 Inleiding

1.1 Changelog

De ontwikkeling van en aan hardware en software staat bij BRControls nooit stil. Om die redenen wordt van dit document ook met regelmaat een nieuwe versie gepubliceerd.

Om te voorkomen dat bij iedere nieuwe versie steeds het gehele document moet worden doorgenomen en moet worden gezocht waar welke aanpassingen zijn verwerkt, is hieronder een korte omschrijving gegeven van de verschillende versies en een compact overzicht van de belangrijkste wijzigingen binnen die versie.

Versie	Datum	Omschrijving
P002.2111-A	2021-11	Document volledig herzien en up-to-date gemaakt
V2.1.0	2013-07	Eerste externe release
ONTWERP.V1.1	2013-06	Intern definitief
CONCEPT.V1.0	2013-06	Intern concept

1.2 Scope

In dit document wordt de technische achtergrond van datacommunicatie in het algemeen en diverse communicatietechniek beschreven

Dit document is geschreven om engineers en inbedrijfstellers van producten van BRControls meer achtergrondinformatie te bieden over de gebruikte communicatiemiddelen, en zodoende een betere zelfredzaamheid te bewerkstelligen. Storingen en problemen kunnen hierdoor sneller worden ondervangen en opgelost.

1.3 Behandelde datacom

Binnen BRControls zijn er hoofdzakelijk drie vormen van datacommunicatie te onderscheiden. Dat zijn de seriële communicatie over RS232, RS485 en IP.

Omdat deze vormen van datacommunicatie het meest voorkomen, en daarom ook het vaakst voor problemen zorgen, worden deze drie vormen van communicatie in dit document beschreven.

Daarnaast is er een uitleg over het binaire stelsel inclusief een binaire vergelijkingsmethode. Tevens wordt kort enkele andere talstelsels behandeld. Indien men niet bekend is met deze talstelsels, is het raadzaam dit hoofdstuk als eerste door te nemen.



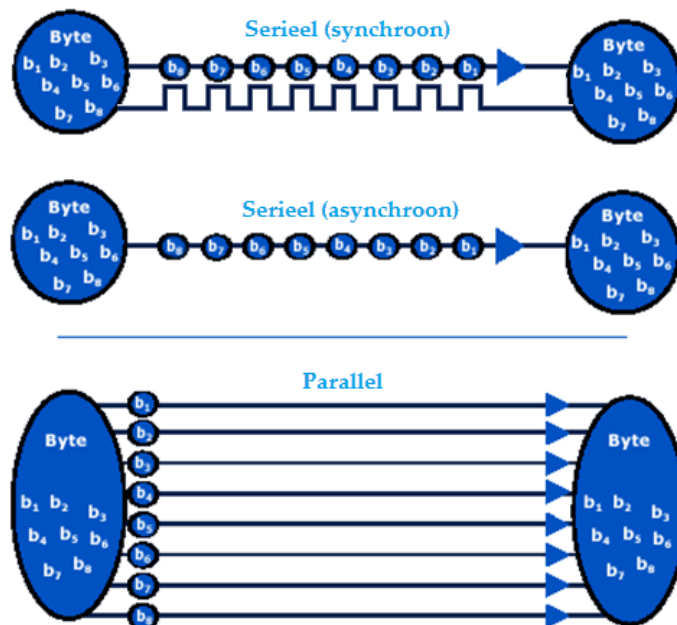
Hoofdstuk 2

Dataverkeer

2 - Dataverkeer

2 Dataverkeer

2.1 Serieel vs Parallel



Afb. 1

Het verzenden van data van punt A naar punt B kan op twee manieren. Serieel en parallel. Parallel is nog bekend van de oude LPT poort, die voornamelijk door scanners en printers werd gebruikt, evenals de IDE kabels waarmee harde schijven in PC werden gebouwd. Het is echter een uitstervend ras. Parallele dataoverdracht veroorzaakt erg veel storingen, en kan qua snelheid niet concurreren met seriële dataoverdracht. In de regeltechniek wordt het niet meer gebruikt. Met de parallelle overdracht worden de bits van een byte gelijktijdig door alle aders gestuurd (meestal 8).

Bij seriële dataoverdracht worden de bits van een byte achter elkaar verzonden. Bij een asynchrone seriële verbinding wordt de data in vaste tijdsintervallen op de lijn gezet. De ontvangende partij weet deze snelheid (baudrate), ontvangt een start en afsluitend een stopbit en kan zo de data goed ontvangen.

Bij een synchrone seriële verbinding wordt de datalijn vergezeld met een klok puls. Dit heeft o.a. als voordeel dat de ontvangende partij niet hoeft te weten wat de snelheid is van de verbinding, maar alleen het bit hoeft uit te lezen op de stijgende c.q. vallende flank van de klok puls. Op de datalijn is op dat moment al het bit geplaatst.

BRControls maakt geen gebruik van synchrone seriële verbindingen.

Het RS232 en RS485 protocol, zijn beide een asynchroon serieel protocol. De start van een bericht wordt dan aangegeven door middel van een start bit (de ontvanger reageert dan op de stijgende c.q. dalende flank).

2.2 Baudrate / Bitrate

Baud is een eenheid die het aantal signaalwisselingen ofwel symbolen per seconde op een datatransmissiekanaal, of meer algemeen, op een informatieverbinding aangeeft. De eenheid ontleent zijn naam aan Émile Baudot, de uitvinder van de baudotcode voor telegrafie.

Baud wordt vaak onterecht als synoniem gezien van bits per seconde. De uitspraak dat men een modem van 56k baud heeft is daarom niet correct: 56k is de bitrate die wordt bereikt door een 7 bits-symbool met 8000 symbolen per seconde te verzenden ($7 \times 8000 = 56000 = 56k$).

2 - Dataverkeer

Het maximaal aantal signaalwisselingen dat een kanaal kan overdragen, is afhankelijk van de bandbreedte van het kanaal. Een normale telefoonlijn heeft een kunstmatig begrensde bandbreedte van ongeveer 3000 hertz. Er is een fundamentele grens voor dit kanaal die in 1924 door Harry Nyquist werd bepaald. Nyquist leidde af dat voor een kanaal van 3000 Hz de maximale snelheid van signaalwisselingen $6000\times$ bedroeg. Voor binaire signalen bedraagt zodoende de maximale snelheid over het kanaal 6000 bit/s en is de lijnsnelheid dus ook 6000 baud.

Wel kan men, door de signaalwisselingen uit meer dan twee niveaus te laten bestaan, meer dan binaire informatie overbrengen. Door bijvoorbeeld 8 signaalniveaus te definiëren, wordt per signaalwisseling drie bits informatie overgebracht (2^3), zodat de snelheid nu 18 000 bits per seconde bedraagt (bij nog steeds 6000 baud).

De maximale datasnelheid van een kanaal wordt gegeven door de wet van Shannon-Hartley. Voor een telefoonlijn behoort de signaal-ruisverhouding minimaal 30 dB te zijn. Dat wil zeggen: de ruis is minstens een factor 1000 ($= 10^{(30/10)}$) zwakker dan het signaal. Bij 3000 Hz en 30 dB resulteert dit in een kanaalcapaciteit van circa 30 000 bits per seconde.

Als gevolg daarvan dacht men tot het eind van 20e eeuw dat de maximale snelheid over een telefoonlijn op ongeveer 30 000 bits per seconde zou liggen. De nieuwste coderingstechnieken hebben er echter toe geleid dat de snelheden nog verder opgeschroefd konden worden, waarbij in 2001 de grens van ongeveer 57000 bit/s is gehaald en in de jaren erna door bleef stijgen tot enkele tientallen megabits per seconde (ADSL en opvolgers). Bij die technieken wordt gebruikgemaakt van adaptieve detectoren.

Voorbeeld: een modem van 9600 bit/s communiceert, door gebruik te maken van symbolen die vier bits informatie overdragen, met een snelheid van 2400 baud.

Het is dus van belang om te weten of er in de documentatie van het desbetreffende apparaat wordt gesproken over baud of bits per seconde aangezien alle partijen op een communicatiebus worden verondersteld dezelfde communicatiesnelheid te gebruiken.

De apparatuur van BRControls ondersteunt een hele range aan baudrates.

2.3 Opbouw van frame

De start van een datatransmissieframe van een seriële verbinding begint met een startbit. Dit is een logische 0. Dit is niet configureerbaar aangezien het voor elke seriële verbinding hetzelfde is.

Na deze start bit komen de data bits. In veel gevallen zijn dit 8 bits, doch er zijn ook protocollen aanwezig die minder bits gebruiken. De apparatuur van BRControls ondersteunt het aantal data bits van 5 – 8.

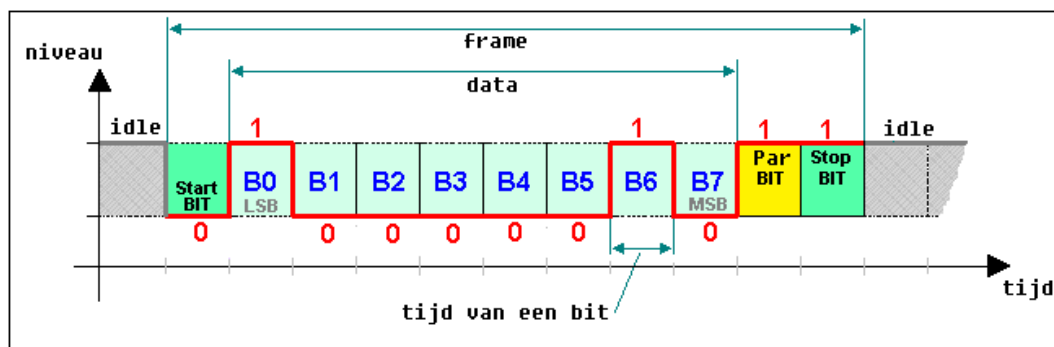
Na het aantal data bits *kan* er een pariteit bit worden verstuurd. Een pariteit bit is een controle van de juistheid van de data bits. Deze kan op verschillende manieren opgebouwd worden, de behandeling hiervan valt buiten de scope van deze documentatie. Het is het belangrijkste *als* deze gebruikt wordt, deze bij de verzender en ontvanger idem is geconfigureerd. In de regel van BRControls kan gekozen worden voor odd, even, mark en space. Er kan ook voor gekozen worden om *geen* pariteit bit te gebruiken.

Het frame moet worden afgesloten met een of twee stop bits. Hierdoor weet de ontvangende partij dat het frame wordt afgesloten en kan deze de data verder verwerken.

De totale lengte van een frame is dus *maximaal* 1 start bit + 8 data bits + 1 pariteit bit + 2 stop bits = 12 bits.

De minimum lengte van een frame is dan 1 start bit + 5 data bits + 1 stop bit = 7 bits.

2 - Dataverkeer



Afb. 2

2.4 Pakket

Een reeks frames maakt samen een pakket dat verwerkt wordt door de regelaar.

Dit pakket bevat ook een foutcontrole. Hoe deze foutcontrole precies in zijn werk gaat, is per protocol verschillend, maar voor elk protocol geldt dat er een foutcontrole is. Deze controle wordt de Cyclic Redundancy Check (CRC) genoemd. Dit is een controlesom waarmee de het hele pakket gecontroleerd kan worden op transmissie fouten.

De CRC som wordt berekend over het hele pakket. Indien de CRC niet overeenkomt met de CRC die de regelaar zelf berekend over het ontvangen pakket, wordt het hele pakket genegeerd, en indien nodig opnieuw aangevraagd bij de verzendende partij.



Afb. 3

2.5 Bekabeling

Welk type bedrading gebruikt moet worden voor de seriële verbinding is sterk afhankelijk van de lengte van de verbinding, blootstelling aan elektrische stoorsignalen en het protocol. Voor beide protocollen is niet echt een type bedrading afgesproken dat gebruikt zou moeten worden.

Volgens een richtlijn is bedradingsdiameter van 0,25mm² voldoende. Dit is erg dun en niet praktisch gebleken. Een aderdiameter van 0,75mm² / 1mm² is sterker en praktischer. Tevens dient een kabel met getwiste aderparen te worden gebruikt, zie hierna waarom.

Een veel gebruikt en goed verkrijgbaar kabeltype voor RS-485 communicatie is de **BELDEN 3106A** (www.belden.com)



Afb. 4

Voorkom storingen: gebruik kabels met getwiste aders!

Het twisten van de aders is een eenvoudig detail in de kabelconstructie. Maar verrassend genoeg begrijpen veel engineers en installateurs niet echt de voordelen ervan. De meesten hebben wel het idee dat het twisten van kabels goed is voor elektromagnetische interferentie (EMI), maar als men hen ernaar vraagt, weten ze niet goed te verklaren waarom.

2 - Dataverkeer

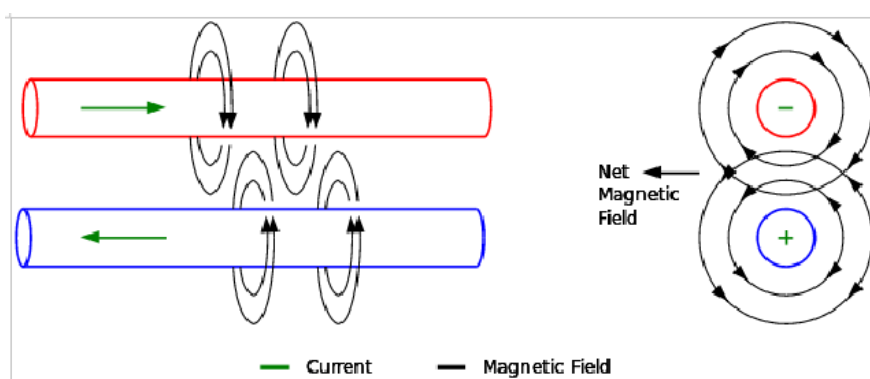
Vier voordelen

Het twisten van aderpennen in een kabel heeft vier grote voordelen. Twee daarvan liggen voor de hand. Twee zijn vrij subtiel.

Twisten verbetert de prestaties wanneer twee aangrenzende draden signaal en retoursignaal in tegengestelde richtingen geleiden. Hetzelfde geldt voor stroom en retourstroom.

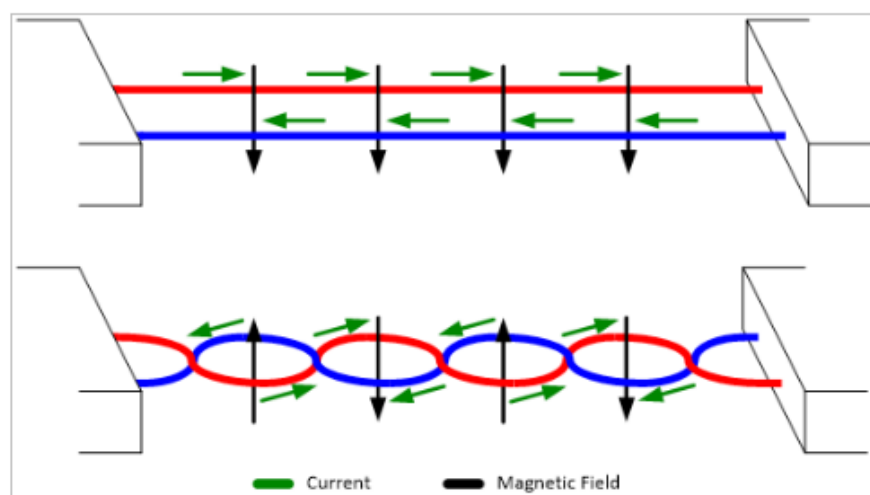
1. Onderdrukking van magnetische velden

In de ruimte tussen twee parallelle draden die stroom in tegengestelde richtingen geleiden, is het magnetisch veld additief. Als de draden niet getwist zijn, is het magnetisch veld in de nabijheid van de draden niet nul. Een grotere stroomsterkte en een grotere afstand tussen de draden veroorzaakt een groter magnetisch veld. Een circuitlus die door dat magnetische veld wordt doorsneden, zoals een ander niet-getwist aderpaar in dezelfde bundel, zal een geïnduceerde spanning ondervinden.



Afb. 5

Wanneer de draden in elkaar zijn gedraaid, zijn de magnetische velden in aangrenzende halve windingen in tegengestelde richting en hebben ze de neiging elkaar op te heffen. Meer windingen geven een betere veldannulering. Over hun lengte is het netto magnetisch veld dat door de draden wordt uitgezonden bijna nul, zodat een aangrenzende circuitlus een geïnduceerde spanning van bijna nul ondervindt.



Afb. 6

Gevoeligheid voor magnetische velden

Zoals hierboven vermeld, vormen niet-getwiste aderpennen een stroomkring die bij blootstelling aan een magnetisch veld een geïnduceerde spanning zal ondervinden. Door het aderpaar niet te twisten, zullen de apparaten aan de uiteinden van de kabel meer geïnduceerde ruis ondervinden en dus gevoeliger zijn. Het in elkaar draaien van de

2 - Dataverkeer

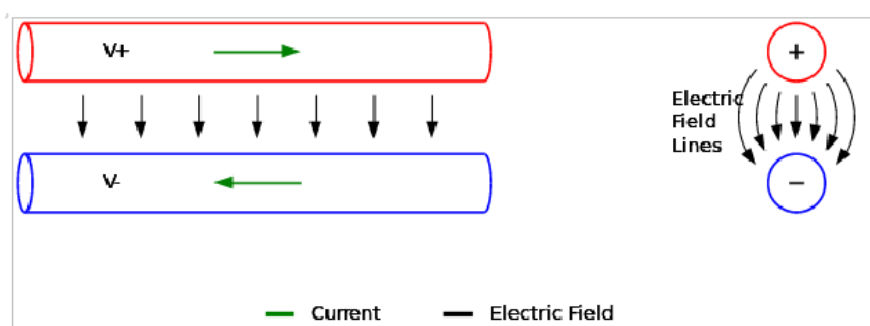
draden veroorzaakt invallende magnetische velden die spanning met tegengestelde polariteit in aangrenzende halve windingen induceren. Het netto-effect is een lagere geïnduceerde spanning en een betere ruis-immuniteit.

2. Vermindert elektrische veldemissies en instraling

Elektrische veldemissies

Meestal is er een potentiaalverschil tussen draadparen van een schakeling. Voedings- en retoursignalen kunnen onderling wisselspanning of gelijkspanning hebben, differentiële signaalparen dragen spanningen die herhaaldelijk van polariteit verwisselen, en single-ended signalen wisselen af tussen een laag potentiaalverschil (logica 0) en een hoog potentiaalverschil (logica 1).

Het elektrische veld ontstaat op de geleider met het hoogste potentiaal en eindigt op de geleider met het laagste potentiaal. Hoger spanningsverschil veroorzaakt sterkere elektrische velden. Een grotere afstand tussen de draden geeft een bredere fringing. Als het elektrisch veld eindigt op een nabijgelegen geleider, wordt stroom geïnduceerd.



Afb. 7

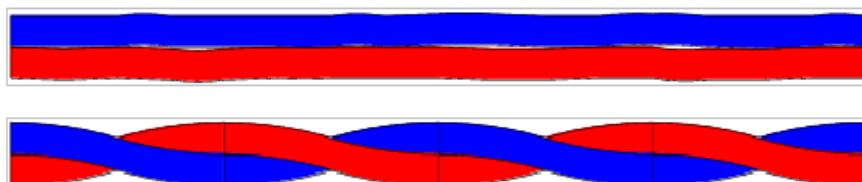
Wanneer het draadpaar dat de spanning draagt in elkaar gedraaid is, zijn de elektrische veldlijnen van aangrenzende halve windingen in tegengestelde richtingen en hebben de neiging elkaar op te heffen. Meer windingen verbeteren de veldannulering. Over hun gehele lengte is het netto elektrische veld dat door de draden wordt uitgezonden bijna nul, zodat aangrenzende schakelingen minder worden beïnvloed.

Gevoeligheid voor elektrisch veldinstraling

Net zoals emissies worden verminderd door twisten, wordt immuniteit voor elektrische veldinstraling verbeterd door twisten. Draadparen die worden blootgesteld aan een elektrisch veld dat niet evenwijdig is aan de draden, zullen stroom induceren op de draden. Als de draden in elkaar worden gedraaid, is de geïnduceerde stroom in elke aangrenzende halve winding in tegengestelde richting, zodat het netto-effect bijna nul geïnduceerde stroom is en de immuniteit voor circuitruis wordt verbeterd.

3. Houdt de draden dicht bij elkaar

Twisten heeft als bijkomend voordeel dat de draden automatisch strak tegen elkaar worden getrokken. En houdt hun scheiding op een uniforme afstand, tweemaal de dikte van de draadisolatie.



Afb. 8

De karakteristieke impedantie van een aderpaar houdt rechtstreeks verband met de afstand tussen de draden. Door de draden over hun gehele lengte op gelijke afstand van elkaar te houden, is de karakteristieke impedantie constant, een eigenschap die zeer belangrijk is voor de signaalintegriteit.

2 - Dataverkeer

Elektrische en magnetische velden afkomstig van en gekoppeld aan een aderpaar houden rechtstreeks verband met de afstand tussen de draden. Een zo klein mogelijke afstand tussen de draden minimaliseert de emissie en de overdracht.

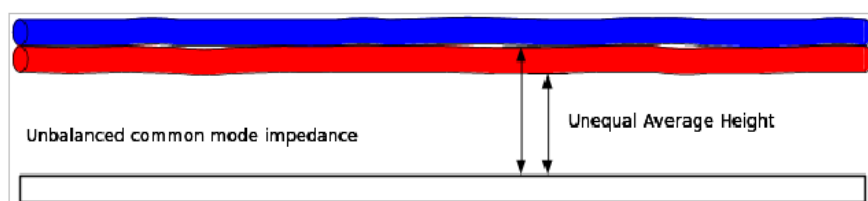
4. Evenwicht in de gemeenschappelijke impedantie

Vaak worden aderparen in de buurt van een geleidend oppervlak, een massaplaat, gelegd. Dit is het geval bij kabelbomen in auto's, vliegtuigen, apparatuurrekken, kabelgoten en elke installatie in een metalen behuizing.

Als de ene draad zich dichterbij de massaplaat bevindt dan de andere, zal de radiofrequentie-impedantie van de twee draden ten opzichte van de aarde verschillend zijn. Hun gemeenschappelijke impedantie zal ongebalanceerd zijn.

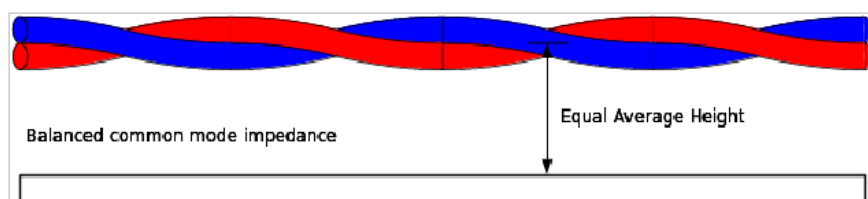
Zelfs als de twee draden op gelijke afstand van elkaar liggen en hun eindcircuits optimaal zijn ontworpen en gebalanceerd, zal de stroomkring als geheel uit balans zijn.

In een stroomkring met onbalans van de gemeenschappelijke impedantie zal een deel van het differentiële signaal, het signaal tussen de twee draden, verschijnen als gemeenschappelijke ruis, ruis tussen de signaalgeleiders en de massaplaat. Dit leidt niet alleen tot een verslechtering van de signaalintegriteit, maar ook tot hogere stralingsemissies van de draden en een grotere gevoeligheid van de eindcircuits voor ruis.



Afb. 9

Anderzijds, als de draden getwist zijn, zullen ze gemiddeld over hun lengte op dezelfde afstand van de massaplaat liggen. Hun impedantie voor de gemeenschappelijke modus zal in evenwicht zijn en de kring zal lagere uitgestraalde emissies vertonen en een grotere immuniteit voor het oppikken van ruis.



Afb. 10

Waarom zijn niet alle draden getwist?

Niet getwiste draden nemen minder ruimte in beslag en zijn korter dan getwiste draden. Niet getwiste draden zijn goedkoper. In elektromagnetische omgevingen waar de voordelen van getwiste draden niet nodig zijn, kunnen niet-getwiste draden een geschikte keuze zijn, denk hierbij aan 230VAC voedingskabels voor apparatuur of wandcontactdozen. Maar in de meeste datagerelateerde toepassingen biedt getwiste draad aanzienlijke voordelen tegen minimale kosten.



Afb. 11

2 - Dataverkeer

2.6 RS-232

RS-232 is een bekend protocol voor het overbruggen van korte afstanden (<15m). Binnen BRControls wordt dit voornamelijk gebruikt om externe converters/gateways uit te lezen en/of aan te sturen.

2.6.1 Aansluiting

Voor het aansluiten van een RS-232 verbinding zijn er drie aders nodig, de aarde (GND) de transmit(TX) en de receive (RX). Voor een RS-232 verbinding is de GND nodig, omdat RS-232 werkt met spanningen die gemeten worden ten opzichte van de GND.

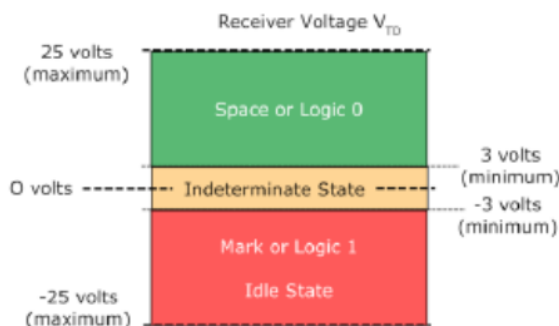
Het verkeerd aansluiten van de TX en de RX heeft als gevolg dat de verstuurd pakketten niet worden beantwoord. De TX teller in BRConfig blijft dan op 0 staan.

2.6.2 Bustopologie

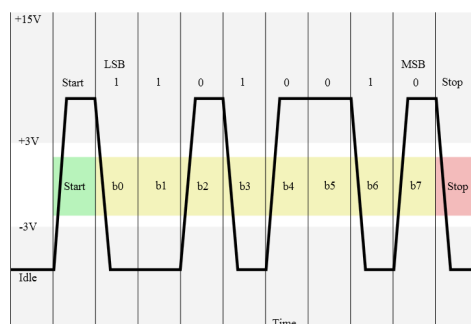
Een RS-232 verbinding wordt niet toegepast in een bus-netwerk. RS-232 is een point-to-point (1-op-1) verbinding. Het is dus een rechtstreekse verbinding van het ene apparaat naar de andere. Een positief gevolg van dit aansluitprincipe is dat apparatuur niet geadresseerd hoeft te worden; er is altijd verbinding met maar één vaste partner.

2.6.3 Signaalniveau's

RS-232 werkt met signaalniveau's van minimaal $\pm 3V$ en maximaal $\pm 25V$. Een logische 0 is een spanning t.o.v. de GND die groter is dan +3V. Een logische 1 is een spanning die kleiner is dan -3V. Voor beide geldt een maximum van $\pm 25V$.



Afb. 12



Afb. 13

Indien er geen activiteit op de RS-232 verbinding aanwezig is, zal de verbinding een negatieve spanning hebben (exacte spanning is afhankelijk van de gebruikte chip, maar in ieder geval kleiner dan -3V).

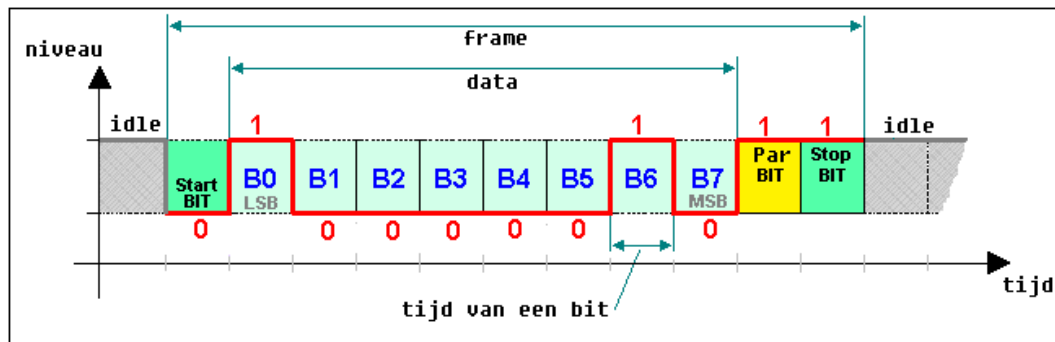
2 - Dataverkeer

2.6.4 Opbouw van frame

De opbouw van een RS-232 frame kan verschillend zijn. De exacte parameters staan in de documentatie van het aan te sluiten apparaat. Een frame zal altijd beginnen met een start bit, gevolgd door 5 – 8 data bits en afgesloten worden met 1 of 2 stopbits.

Meestal gebruikt de RS-232 verbinding ook een pariteit bit, maar dit is niet altijd het geval.

De stop bit kan 1 of 2 bits bedragen.



Afb. 14

2 - Dataverkeer

2.7 RS-485

Als er over RS-485 geschreven wordt, wordt vaak de indruk gewekt dat dit hetzelfde is als Modbus. Dit is echter onjuist. ModBUS is een protocol dat kan communiceren over een RS-485 verbinding. Dit is echter niet noodzakelijk, Modbus werkt namelijk ook prima op bijvoorbeeld een TCP/IP verbinding.

De officiële naam voor RS-485 is ANSI/TIA/EIA-485-A-98.

2.7.1 Aansluiting

RS-485 heeft een minimum van twee aders nodig. Fabrikanten kunnen deze aders anders benoemen. Enkele veelvoorkomende adercoderingen zijn:

- - / +
- A- / B+
- U- / U+
- X / Z
- DATA A - / DATA B +

Voor een RS-485 is het niet noodzakelijk om de GND aan te sluiten. RS-485 werkt met een differentiaal vergelijking (een vergelijking van de spanning op de A- ader met de spanning op de B+ ader), waardoor de GND niet nodig is om een logische 1 of 0 te onderscheiden.

Als de GND wél wordt aangesloten dient er rekening met een eventuele aardlus te worden gehouden en derhalve de aardleiding dus maar op één punt met aarde verbonden mag worden. Aardlussen zijn uiterst onwenselijk en kunnen de betrouwbaarheid van de datacommunicatie sterk reduceren.

Het wordt derhalve ook **niet aanbevolen** om de GND aan te sluiten op een RS-485 verbinding.

Het kan voorkomen dat op een apparaat de labels van A- / B+ omgedraaid zijn, waardoor het apparaat niet gevonden kan worden. Als men er zeker van is dat de andere parameters goed ingevoerd zijn, kan het de moeite lonen om de aders om te wisselen.

2.7.2 Bustopologie

Een RS-485 verbinding is een multipoint verbinding. Dit houdt in dat er meerdere deelnemers op dezelfde bus aangesloten kunnen worden.

Elke deelnemer op de bus heeft een verbruik, de zogenaamde Unit Load (UL). Deze UL is standaard 12kΩ. De UL wordt bepaald door de ingangsweerstand van de RS-485 chip binnen een apparaat.

Indien elke deelnemer deze standaard unit load gebruikt, is het maximum aantal deelnemers op de bus 32. Een deelnemer kan echter een hogere weerstand (lagere UL) hebben, zoals ¼ UL.

Unit Load	Maximum deelnemers	Minimale ingangsweerstand
1	32	12 kΩ
½	64	24 kΩ
¼	128	48 kΩ
⅛	256	96 kΩ

Indien alle deelnemers een UL van 1 hebben, zal er een repeater moeten worden gebruikt om het aantal deelnemers hoger dan 32 te laten bedragen. Achter deze repeater geldt eveneens een maximum van 32 gebruikers, tenzij anders aangegeven in de documentatie van de repeater. Dit kan in theorie uitgebreid worden tot wel enkele duizenden deelnemers maar aangezien dit enorme vertragingen op de buslijn zal veroorzaken geldt de vuistregel: maximaal 3 repeaters.

De totale lengte van een RS-485 netwerk bedraagt maximaal -in theorie- 1200 meter bij 9600 baud / 100kbps. Bij lagere baudrates kan echter een langere afstand overbrugt worden.

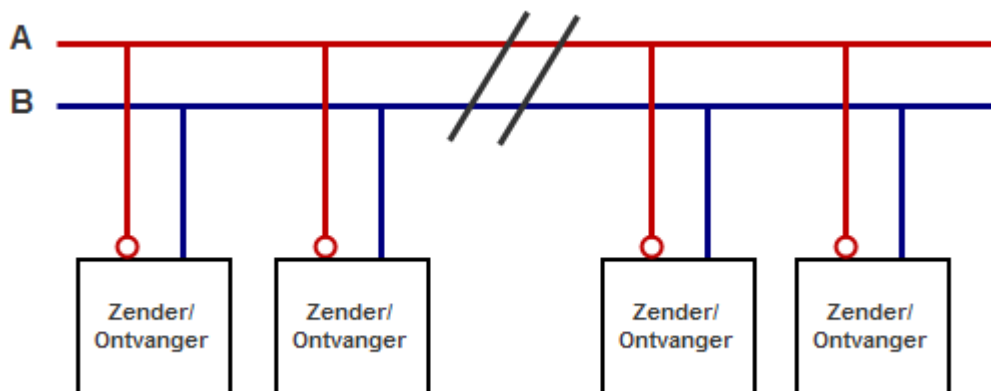
2 - Dataverkeer

Indien er verschillende types UL gebruikt worden op de bus, kan er berekend worden of het aantal deelnemers het maximum niet overschrijdt. De totale weerstand van de deelnemers mag niet onder de 375Ω liggen.

Indien de RS-485 verbinding 2-draads is uitgevoerd, is de verbinding half-duplex (zenden en ontvangen over dezelfde signaallijnen maar nooit gelijktijdig).

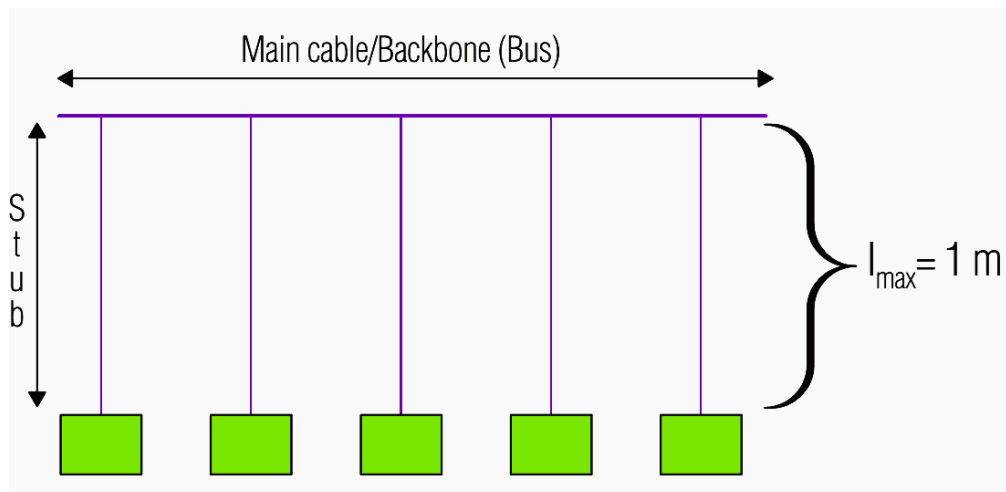
4-draads RS485 is een full-duplex verbinding maar komt in de praktijk bijna nooit voor. Hierbij wordt het ene aderpaar gebruikt voor het zenden en het andere aderpaar voor het ontvangen. Het zenden en ontvangen kan en mag dan dus wel gelijktijdig plaatsvinden

Een RS-485 netwerk moet ontworpen worden als een lijn- of bustopologie, niet als stertopologie. Een stertopologie kan ervoor zorgen dat de signaalkwaliteit drastisch naar beneden gaat. Het RS-485 netwerk heeft een afsluitweerstand nodig om ongewenste reflecties tegen te gaan indien de hoofdkabel langer is dan 50 meter.



Afb. 15

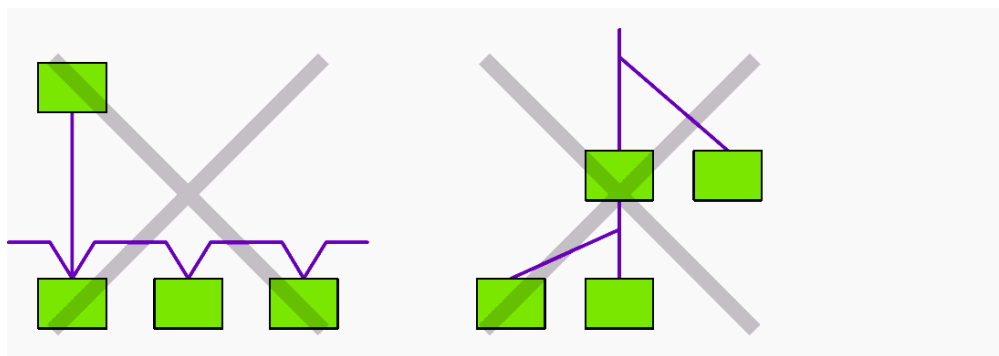
De aftakkingen vanuit de buslijn naar de apparaten mag maximaal 1 meter bedragen. Beter is het om de bus op het apparaat zelf door te lussen.



Afb. 16

Onderstaande afbeelding geeft enkele **foute aansluitvoorbeelden**;

2 - Dataverkeer



Afb. 17

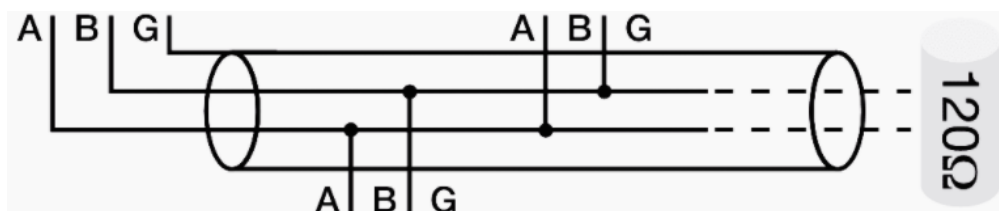
2.7.3 Afsluitweerstand

In een RS-485 netwerk wordt het sterk aangeraden om een afsluitweerstand te gebruiken indien de kabellengte meer dan 50 meter is. Dit om reflecties tegen te gaan. Reflecties ontstaan als de tijd die nodig is om van een logische 1 naar een logische 0 (of vice versa) te gaan te lang duurt. Dit wordt veroorzaakt door een te hoge weerstand van het netwerk c.q. ontvanger, waardoor de spanning niet snel genoeg kan zakken.

Hierdoor kan het voorkomen dat het volgende bit verkeerd wordt gelezen. Ontvangstfouten zijn hiervan het gevolg. Door een afsluitweerstand in het netwerk op te nemen wordt de daaltijd van de ene logische fase naar de andere drastisch verkort, en zodoende de ontvangstfouten geëlimineerd.

Het verschijnsel reflecties is vooral van toepassing op hoge snelheden. Indien er geen afsluitweerstand voorhanden is, kan het sterk verlagen van de snelheid op alle aangesloten apparaten ook een (tijdelijke) oplossing zijn.

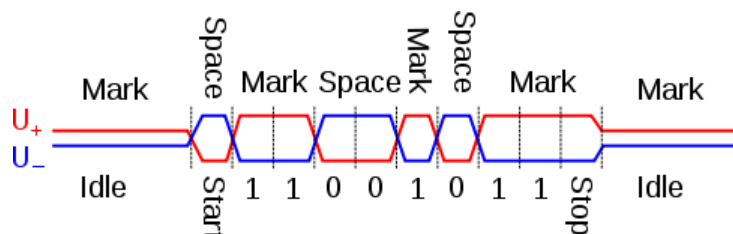
De afsluitweerstand is in de regel 120Ω en dient op het fysieke eind van de kabel geplaatst te worden tussen de twee datavoerende aders. Op diverse BRControls apparatuur kan deze eindweerstand door middel van een dipswitch worden in- of uitgeschakeld, zie hiervoor de technische documentatie van de desbetreffende apparatuur.



Afb. 18

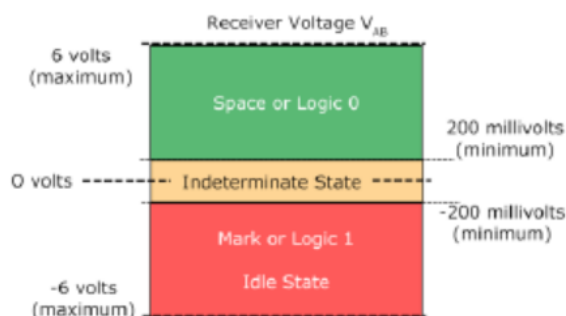
2.7.4 Signaalniveau's

Bij RS-485 wordt een logische 0 of 1 aangeduid met het spanningsverschil tussen de twee aders.



Afb. 19

2 - Dataverkeer



Afb. 20

Indien de spanning op U+ en U- tussen de +0,2V en +6V is, wordt het gezien als een logische 0. Indien het tussen U+ en U- tussen de -0,2V en -6V is, wordt deze gezien als een logische 1.

Indien er geen activiteit op de RS-485 verbinding is, zal de spanning tussen de twee aders afhankelijk zijn van het netwerk. De spanning op B+ zal echter ten opzichte van A- positief zijn.

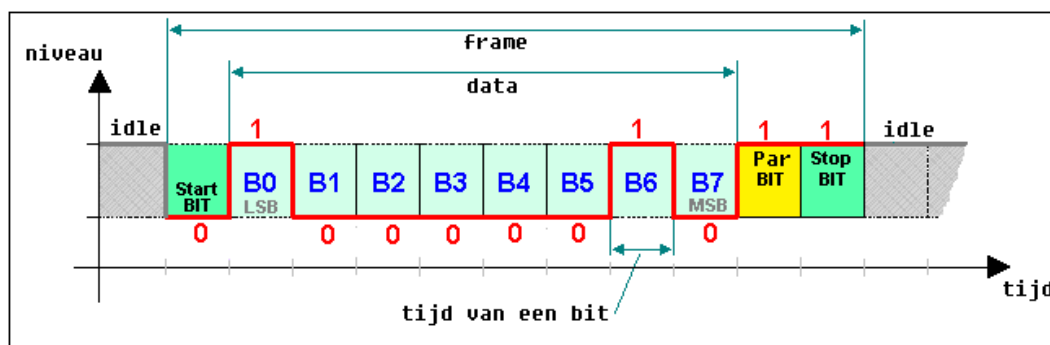
Hieruit blijkt dat het aansluiten van een RS-485 goed moet gebeuren. Indien de aders verwisseld worden, zal de data die wordt verstuurd, geïnverteerd worden. Dit veroorzaakt in een onjuist bericht, dat de ontvangers niet kunnen verwerken.

Als er meerdere ontvangers op de bus aangesloten zijn en één daarvan is er verkeerd om aangesloten, zal *alleen* deze onjuist reageren. Het verkeerd om aansluiten van een deelnemer van de bus heeft *geen* invloed op het functioneren van de andere deelnemers.

Als er slechts één deelnemer op de bus zit en de aders zijn verkeerd om aangesloten, zal er geen binnenkomend verkeer zijn. De TX teller zal op 0 blijven staan.

2.7.5 Opbouw van frame

De opbouw van een RS-485 kan verschillend zijn. Het aantal data bits dat er verstuurd wordt zal 7 of 8 bedragen. Het aantal stop bits kan 1 of 2 zijn. Een pariteit bit wordt *meestal* niet verstuurd, maar het kan zeker wel voorkomen. Lees de documentatie van het aan te sluiten product goed door, zodat deze instellingen goed staan.



Afb. 21



Hoofdstuk 3

Netwerkbegrippen

3 - Netwerkbegrippen

3 Netwerkbegrippen

Het benaderen van een BRControls regelaar vindt plaats door middel van een netwerk. Dit dient juist geconfigureerd en geïmplementeerd te worden om een correcte werking van de regelaar en een soepele toegang te waarborgen.

Een computernetwerk is een systeem voor communicatie tussen twee of meer computers. De communicatie verloopt via netwerkkabels of via een draadloos netwerk en is altijd gebaseerd op adressering.

In de netwerktopologie worden fysieke en logische topologieën onderscheiden. Men spreekt van een LAN in het geval van lokale plaatsgebonden bekabeling waarop computers binnen één gebouw of een campus aangesloten worden en een WAN wanneer er sprake is van verbindingen over grotere afstanden.

In dit hoofdstuk zullen enkele basisbegrippen en principes van netwerken worden behandeld.

3 - Netwerkbegrippen

3.1 MAC adressen

De onderste laag van de netwerkadressering werkt met Media Access Control (MAC) adressering. (uiteindelijk is de onderste laag uiteraard de fysieke of draadloze verbinding tussen twee computers maar voor de adressering is deze niet van belang).

Het MAC adres is een wereldwijd uniek adres dat bij de productie van netwerkapparatuur (= NIC = Network Interface Card) wordt ingesteld in het desbetreffende netwerkapparaat. Het MAC adres wordt standaard weergegeven in hexadecimale getallen, gescheiden door een dubbele punt. (Indien men niet bekend is met hexadecimale getallen, lees eerst het hoofdstuk 'Talstelsels' aan het eind van dit document).

Het MAC adres bestaat uit 48 bits (= 6 bytes), die gegroepeerd zijn per 8 bit (= 1 byte) en in hexadecimale notatie worden weergegeven. Het aantal adressen dat kan worden toegekend ligt dan grofweg op 281 biljoen (2^{48}). De eerste 24 bits van het MAC adres zijn gereserveerd voor de unieke Organizational Unique Identifier (OUI). Elke fabrikant heeft zijn eigen OUI.

- BRControls heeft een OUI van **00:17:14**.

Alle MAC-adressen van BRControls beginnen dus met deze OUI 00:17:14. De netwerkgerelateerde producten van BRControls hebben een uniek MAC-adres. De laatste 24 bits ($2^{24} = 16.777.215$ adressen) kunnen door BRControls dus vrij gebruikt worden voor het adresseren van de netwerkapparatuur.

Het MAC adres wordt door de routers binnen een netwerk gebruikt om de pakketten op de juiste locatie af te kunnen leveren. Pakketten worden zo niet over het hele netwerk heen gestuurd, maar alleen over het gedeelte waar het pakket echt langs moet.

Op de volgende pagina vindt u een overzicht van de door BRControls gebruikte MAC adressen.

3 - Netwerkbegrippen

MAC Adres start	MAC Adres stop	Device
00:17:14:01:00:00	00:17:14:01:FF:FF	BHPS45
00:17:14:02:00:00	00:17:14:02:FF:FF	BHPS23
00:17:14:03:00:00	00:17:14:03:FF:FF	BHPS150
00:17:14:04:00:00	00:17:14:04:FF:FF	SIO4
00:17:14:05:00:00	00:17:14:06:FF:FF	-SPARE- (RESERVED BHPS46 LAN)
00:17:14:07:00:00	00:17:14:08:FF:FF	-SPARE- (RESERVED BHPS46 WAN)
00:17:14:09:00:00	00:17:14:09:FF:FF	-SPARE-
00:17:14:0A:00:00	00:17:14:0B:FF:FF	BHPS46 LAN
00:17:14:0C:00:00	00:17:14:0D:FF:FF	BHPS46 WAN
00:17:14:0E:00:00	00:17:14:0F:FF:FF	BRN15
00:17:14:10:00:00	00:17:14:10:FF:FF	BRINTDSP WIFI
00:17:14:11:00:00	00:17:14:12:FF:FF	RIO-MU22
00:17:14:13:00:00	00:17:14:13:FF:FF	-SPARE-
00:17:14:14:00:00	00:17:14:14:FF:FF	BHPS47 LAN
00:17:14:15:00:00	00:17:14:15:FF:FF	BHPS47 WAN
00:17:14:16:00:00	00:17:14:16:FF:FF	BHPS47 WIFI
00:17:14:17:00:00	00:17:14:1A:FF:FF	-SPARE-
00:17:14:1B:00:00	00:17:14:1B:FF:FF	BRINTDSP LAN
00:17:14:1C:00:00	00:17:14:1C:FF:FF	BRINTDSP WAN
00:17:14:1D:00:00	00:17:14:1F:FF:FF	-SPARE-
00:17:14:20:00:00	00:17:14:21:FF:FF	BNFC
00:17:14:22:00:00	00:17:14:23:FF:FF	BNFC BLE BLUETOOTH DEVICES
00:17:14:24:00:00	00:17:14:37:FF:FF	-SPARE-
00:17:14:38:00:00	00:17:14:39:FF:FF	BRN20 BNZC ETH0
00:17:14:3A:00:00	00:17:14:3B:FF:FF	BRN20 BNZC ETH1
00:17:14:3C:00:00	00:17:14:49:FF:FF	-SPARE-
00:17:14:50:00:00	00:17:14:5F:FF:FF	BRT24 BLE BLUETOOTH DEVICES
00:17:14:60:00:00	00:17:14:7F:FF:FF	BRT35 BLE BLUETOOTH DEVICES
00:17:14:80:00:00	00:17:14:81:FF:FF	BRT35 BRN 15 DEVICES
00:17:14:82:00:00	00:17:14:8F:FF:FF	-SPARE-
00:17:14:90:00:00	00:17:14:9F:FF:FF	BRT35 BHPS46 BLE BLUETOOTH DEVICES
00:17:14:A0:00:00	00:17:14:AF:FF:FF	BNFC BLE BLUETOOTH DEVICES
00:17:14:B0:00:00	00:17:14:FE:FF:FE	-SPARE-
00:17:14:FE:FF:FF		BHPS USB RNDIS

3 - Netwerkbegrippen

3.2 IP adressen

Om apparatuur aangesloten op een netwerk te kunnen benoemen en identificeren, heeft ieder apparaat zijn eigen dynamische adres, het IP-adres, nodig.

Het IP-adres bestaat uit een getal van 32 bits. Voor een eenvoudigere notatie wordt dit getal weergegeven in 4 x 8 bit decimale waardes, die de waarde 0 – 255 kunnen hebben, bijvoorbeeld 192.168.5.120.

Een 32 bits getal kan 2^{32} waardes bevatten (4.294.967.296). Er zijn echter reeksen gereserveerd voor speciaal gebruik, waardoor de ruim. 4 miljard toe te kennen waardes niet gehaald worden.

Voor het gebruik op een intern netwerk of intern op een server/pc zijn er IP-adresreeksen gereserveerd (de Private Address Space) die dienen te worden gebruikt. Dit zijn de reeksen uit de onderstaande tabel. Het IP-adres van de BRControls regelaar zal dus ook binnen een van deze reeksen moeten vallen en dan specifiek binnen een **Klasse A**, **Klasse B** of **Klasse C** netwerk.

Adresbereik	Beschrijving	RFC
0.0.0.0/8	Current network (alleen geldig als bronadres)	RFC 5735
10.0.0.0/8	Private network (Klasse A)	RFC 1918
100.64.0.0/10	Shared Address Space	RFC 6598
127.0.0.0/8	Loopback	RFC 5735
169.254.0.0/16	Link-local (b.v. indien geen IP adres ontvangen van server)	RFC 3927
172.16.0.0/12	Private network (Klasse B)	RFC 1918
192.0.0.0/24	IETF Protocol Assignments	RFC 5735
192.0.2.0/24	TEST-NET-1, documentatie en voorbeelden	RFC 5735
192.88.99.0/24	IPv6 to IPv4 relay	RFC 3068
192.168.0.0/16	Private network (Klasse C)	RFC 1918
198.18.0.0/15	Network benchmark tests	RFC 2544
198.51.100.0/24	TEST-NET-2, documentatie en voorbeelden	RFC 5737
203.0.113.0/24	TEST-NET-3, documentatie en voorbeelden	RFC 5737
224.0.0.0/4	IP multicast (voormalig klasse D-netwerk)	RFC 5771
240.0.0.0/4	Gereserveerd (voormalig klasse E-netwerk)	RFC 1700
255.255.255.255	Broadcast	RFC 919

Er moet opgemerkt worden dat het adres x.x.x.0 gebruikt wordt om het netwerkadres aan te geven en het adres x.x.x.255 gebruikt wordt voor een broadcast bericht (bericht naar elke deelnemer). Deze twee adressen kunnen dus niet gebruikt worden binnen een netwerk.

Ook de speciale reeks 127.0.0.1 - 127.0.0.255 is een gereserveerde reeks IP-adressen. Dit wordt ook aangeduid met **localhost**. Deze reeks wordt gebruikt voor het testen van de eigen netwerkinterface van het device maar ook voor bijvoorbeeld een webserver die vanaf het eigen device draait. Deze adressen kunnen niet gebruikt worden binnen een netwerk.

BRControls naregelingen hebben standaard IP adressen die zijn gebaseerd op hun serienummer/MAC adres. De USB aansluiting op de BRC46 heeft tevens een vooraf bepaald IP adres.

IP Adressen	Productserie
172.20.xx.xx	BRN20
172.40.xx.xx	BRN15
172.50.xx.xx	BNFC
192.168.4.101	BRC46-USB poort

3 - Netwerkbegrippen

3.3 ARP tabel

Zoals in het voorgaande is te lezen, heeft een netwerkkapparaat een statisch hardware adres, het MAC-adres. Ook heeft het apparaat om zich te identificeren op het netwerk een dynamisch IP-adres. Dit IP-adres is naar wens in te stellen, het MAC-adres staat vast.

Om deze twee adressen aan elkaar te koppelen, zodat het netwerkkapparaat weet hoe hij het complete pakket moet samenstellen (inclusief MAC-adres), is het Address Resolution Protocol (ARP) ontwikkeld. Het valt buiten de scope van dit document om dit diepgaand te behandelen, maar het is wel van belangrijk om te weten dat er op elk netwerkkapparaat een tabel wordt bijgehouden (de zogeheten ARP-tabel), die de kruisverwijzing van MAC-adres – IP-adres bijhoudt.

De ARP-tabel uit de eigen PC valt uit te lezen door in de opdrachtprompt (Start > Uitvoeren > cmd) de functie **arp -a** aan te roepen. Soortgelijke afbeelding als onderstaande zal worden weergegeven.

```
PS C:\Users\[gebruiker]> arp -a

Interface: 192.168.30.1 --- 0x9
Internet Address      Physical Address      Type
192.168.30.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22            01-00-5e-00-00-16    static
224.0.0.251           01-00-5e-00-00-fb    static
224.0.0.252           01-00-5e-00-00-fc    static
239.255.255.250       01-00-5e-7f-ff-fa    static

Interface: 172.16.252.36 --- 0x13
Internet Address      Physical Address      Type
172.16.252.1          00-0c-29-b3-93-f4    dynamic
172.16.252.2          00-0c-29-c9-ea-7c    dynamic
172.16.252.5          00-0c-29-c9-ea-7c    dynamic
172.16.252.10         00-0c-29-93-95-6a    dynamic
172.16.252.15         00-11-32-4a-74-81    dynamic
172.16.252.26         74-83-c2-ec-ef-5d    dynamic
172.16.252.30         fc-ec-da-e5-45-95    dynamic
172.16.252.38         00-0c-29-c9-ea-7c    dynamic
172.16.252.44         1c-d6-be-6f-64-fd    dynamic
```

Afb. 22

Met de functie **arp -d** leegt u de ARP-tabel (het is mogelijk dat deze functie als Administrator moet worden uitgevoerd). De tabel wordt automatisch weer aangemaakt en bijgewerkt als er IP-adressen worden opgevraagd.

Bij een reboot van het netwerkkapparaat wordt deze tabel automatisch leeggemaakt.

3 - Netwerkbegrippen

3.4 DHCP

DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) is het principe dat toestellen in een IP-netwerk geen vast geconfigureerd IP-adres hebben, maar hun IP-adres dynamisch verkrijgen van een centraal beheerde DHCP voorziening, meestal een router, DHCP server of domeincontroller.

De server, die zelf een vast IP-adres heeft, beheert hiertoe een "pool" van beschikbare IP-adressen, veelal in de Private Address Space volgens RFC 1918, zie hoofdstuk 'IP adressen'. Na opstarten van de DHCP-server zijn die adressen vrij en kunnen ze aangevraagd worden door de toestellen op het netwerk. Door de aanvragen worden de IP-adressen toebedeeld, uiteraard in aantal beperkt tot de grootte van de pool.

Toestellen die op het netwerk komen, kunnen via een aanvraagsequentie een IP-adres verkrijgen dat beperkt geldig is, voor de ingestelde geldigheidsduur, de "lease time". Toestellen die het netwerk verlaten, dienen hun adres vrij te geven. Dit gebeurt uiteraard niet in alle gevallen. Het adres komt echter uiteindelijk toch weer vrij door het verlopen van de geldigheidsduur.

DHCP-servers kunnen voor bepaalde toestellen een vast uit te reiken IP-adres geconfigureerd hebben. Zo kan het bv. zijn dat binnen een bedrijf alle netwerkprinters een vast IP-adres krijgen, dit terwijl andere toestellen een willekeurig adres uit de pool toebedeeld krijgen.

De producten van BRControls ondersteunen geen DHCP.

Deze keuze is bewust gemaakt, aangezien het hebben van een dynamisch IP-adres voor een regelaar niet handig is. Indien er een verbinding gemaakt moet worden met de regelaar, en het IP-adres is dynamisch, moet er telkens gezocht worden naar de regelaar.

Een toestel dat een IP-adres wenst te verkrijgen, dient daartoe een sequentie van aanvraag te starten. Bij een correcte configuratie van het netwerk zal ten minste één DHCP-server op de aanvraag moeten reageren. Het aanvragende toestel kan vervolgens de finale aanvraag doen, waarop de aanbiedende server normaal bevestigend zal antwoorden. Vanaf dat moment maakt het aanvragende toestel deel uit van het netwerk ook op de internetlaag en kan het op IP-pakketten gebaseerde communicatie uitvoeren. Het is mogelijk dat er zich meer dan één DHCP-server op het netwerk bevindt, voor verschillende subnetten.

Hoe gaat het in z'n werk?

Het volledige proces ter verkrijging van de netwerkinstellingen bestaat uit een sequentie van vier aanvragen en reacties. Dit proces staat bekend onder de afkorting **DORA**. **D**iscover **O**ffer **R**quest **A**cknowledge.

Op de volgende pagina het verloop van een succesvolle DHCP-aanvraag, met vermelding van de naam van de boodschap binnen het DHCP-protocol tussen haakjes:

3 - Netwerkbegrippen

- **DHCP discovery (DHCPDISCOVER)**

Het aanvragende toestel, de client, stuurt een netwerkpakket gericht aan alle computers binnen het eigen Ethernet-segment door het gebruik van broadcast. Hiervoor gebruikt de aanvrager ofwel het globale broadcastadres 255.255.255.255, dan wel het broadcastadres van het netwerksegment waarop het zich bevindt. Alle toestellen in het betreffende netwerksegment ontvangen dit DHCPDISCOVER-pakket.

- **DHCP offer (DHCPOFFER)**

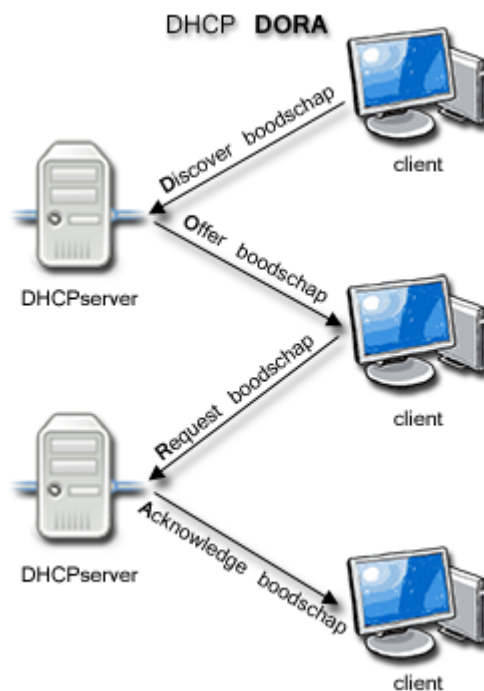
Uitsluitend de DHCP-server of eventueel DHCP-servers in het netwerk behoort/behoort te reageren op het DHCPDISCOVER-pakket. Elke DHCP-server die wenst te antwoorden reserveert een nog vrij IP-adres en stuurt een DHCPOFFER pakket terug naar het MAC-adres van de aanvrager, met vermelding van het aangeboden IP-adres.

- **DHCP request (DHCPREQUEST)**

Het aanvragende toestel weet nu van welke server of servers deze het IP-adres kan verkrijgen. Het toestel gebruikt DHCPREQUEST om daadwerkelijk de aanvraag te doen bij de eerst reagerende DHCP-server en mogelijke overige DHCP-servers te laten weten dat het een IP-adres heeft verkregen via een andere DHCP-server. Dit gebeurt dientengevolge net als bij DHCPDISCOVER met een broadcast-pakket, dat door alle DHCP-servers wordt ontvangen.

- **DHCP acknowledgement (DHCPACK)**

De DHCP-server bevestigt hiermee de aanvraag. Het verzonden DHCPACK-pakket bevat nog eens alle informatie met de netwerkinstellingen. Het toestel dat het nieuwe IP-adres heeft ontvangen, zou op dit punt een test moeten uitvoeren om zeker te stellen dat er toch geen andere toestellen hetzelfde IP-adres in bezit hebben. De client gebruikt dus de gegevens van de eerste DHCP-server waarvan hij antwoord krijgt en gebruikt deze gegevens om zijn netwerkverbinding in te stellen. De betreffende computer heeft nu een uniek IP-adres en kan derhalve vervolgens communiceren met andere toestellen.



Afb. 23

Uiteraard is het ook mogelijk dat de aanvraag niet slaagt, door een fout of een reeds bestaande allocatie. Hiertoe dienen de volgende DHCP-berichten:

- **DHCP negative acknowledgement (DHCPNAK)**

Bij een fout zal de DHCP-server antwoorden met een DHCP-NAK-pakket.

- **DHCP decline (DHCPDECLINE)**

Het clienttoestel rapporteert terug naar de DHCP-server dat het netwerkadres reeds in gebruik is.

Een clienttoestel kan het in gebruik zijnde IP-adres ook weer vrijgeven:

- **DHCP release (DHCPRELEASE)**

het clienttoestel rapporteert terug naar de DHCP-server dat het netwerkadres vrijgegeven mag worden en annuleert hierdoor de huidige leasetime.

Gegevens die onder meer (kunnen) worden doorgestuurd zijn:

- Een uniek netwerknnummer (IP-adres);
- Welk(e) adres(sen) in het netwerk een gateway is/zijn, waarmee er verbinding is met een ander netwerk, zoals het internet (niet noodzakelijk);
- Wat de naamserver(s) (DNS-servers) is/zijn (niet noodzakelijk);
- Hoe groot het netwerk is, dus onder welke omstandigheden de doelcomputer binnen het netwerk ligt of via de gateway benaderd moet worden. Dit wordt de netmask genoemd, zie volgende hoofdstuk.
- De geldigheidsduur (leasetime of looptijd)

3 - Netwerkbegrippen

3.5 Subnet / Netmasker

Een netwerk kan opgedeeld worden in verschillende losse subnetwerken door middel van een subnetmasker. Het opdelen van een netwerk in meerdere subnetten wordt veelvuldig gedaan om het netwerk beter te beveiligen, en/of de bandbreedte voor een gedeelte van een netwerk optimaal te kunnen benutten.

LET OP: een veelgemaakte denkfout is dat een subnet gelijk staat aan een VLAN. Dit is niet correct. Wél wordt een subnetmasker binnen een VLAN gebruikt om het bereik (de grootte, het subnet) van het VLAN te bepalen. Het principe van VLANs valt buiten de scope van dit document en zal verder niet worden behandeld.

Een subnetmasker is niets meer dan een rij enen, aangevuld met nullen totdat de 32 bits breedte is bereikt. Deze worden genoteerd als groepen van 8 bits (octet), waardoor deze een decimale waarde kunnen hebben van 0 – 255. (zelfde principe als bij het IP adres).

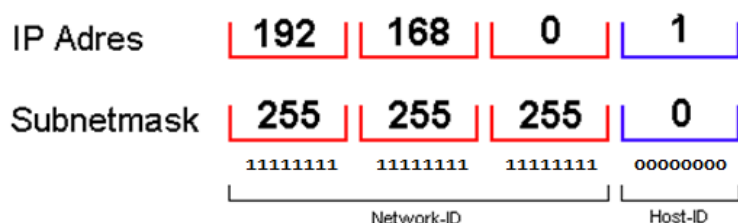
Indien een netwerk is opgedeeld in meerdere subnetten, en de BRControls regelaar is onjuist geconfigureerd, kan het zijn dat de regelaar niet bereikbaar is. Om dit te voorkomen dient de regelaar juist te worden ingesteld. De regelaar en het eigen IP-adres moeten op hetzelfde subnet actief zijn.

Als de regelaar op afstand helemaal niet bereikbaar is omdat het subnetmasker verkeerd is ingesteld, zal er lokaal ingeplugd moeten worden om het subnetmasker te herstellen. Het op afstand veranderen van het subnetmasker dient dus met grote voorzichtigheid te gebeuren.

Host / Netwerk

Een IP-adres heeft altijd een hostdeel en een netwerk deel. Deze twee worden bepaald door het subnetmasker. Op de plek waar het subnetmasker een 1 bevat, is het netwerk ID. Het gedeelte van de subnetmasker wat een 0 bevat is het host-ID.

In onderstaand voorbeeld eindigen de 1'n in het subnetmasker op het hele octet, maar dat kan natuurlijk ook halverwege zijn.



Afb. 24

LET OP: de 1'n zijn **altijd een aaneengesloten reeks**, met andere woorden: er kunnen geen nullen tussen staan. Hetzelfde geldt voor de reeks 0'n.

3 - Netwerkbegrippen

Voorbeeld

Naam	IP-adres
BRControls regelaar	192.168.1.191
Eigen IP (ook via VPN)	192.168.26.5
Gateway (router)	192.168.1.1
Subnetmasker	255.255.255.0

Nu is de gebruiker ingelogd (bijvoorbeeld via een VPN), en heeft het IP-adres 192.168.26.5 toegewezen gekregen. Is de regelaar bereikbaar?

Allereerst wordt het subnet van de regelaar berekend. Dit gebeurt door het IP-adres met behulp van een logische AND functie te vergelijken met het subnetmasker. (zie ook het hoofdstuk 'Talstelsels').

IP-adres regelaar	192.168.1.191	11000000.10101000.00000001.10111111
Subnetmasker	255.255.255.0	11111111.11111111.11111111.00000000 <AND>
Subnet	192.168.1.0	11000000.10101000.00000001.00000000

Hierna wordt het subnet van het eigen IP-adres berekend. Dit verloopt op dezelfde wijze.

IP-adres eigen	192.168.26.5	11000000.10101000.00011010.00000101
Subnetmasker	255.255.255.0	11111111.11111111.11111111.00000000 <AND>
Subnet	192.168.26.0	11000000.10101000.00011010.00000000

Hieruit blijkt dat het subnet van de regelaar anders is dan het subnet van het eigen IP-adres. De regelaar is dus niet bereikbaar. Het subnetmasker zal dan gewijzigd moeten worden, om met de regelaar te kunnen communiceren.

Om de regelaar te kunnen bereiken vanaf een aangesloten laptop/pc, moet men in het zelfde subnet zitten. In dit geval moet het subnet dus minimaal bestaan uit de range 192.168.1.0 – 192.168.26.255. Het huidige subnetmasker eindigt op een 0 (eigenlijk 000), dus de laatste acht bitjes in het subnetmasker staan al op 0. Om het subnet echter uit te breiden moeten er nog meer bits op 0 worden gezet. Hoeveel dat er zijn, is eenvoudig uit te rekenen.

De breedte van de range is 1 t/m 26, dat zijn 26 ranges. 26 is binair genoteerd (zie 'Talstelsels') 11010. De ruimte hiervoor is dus 5 bits. De rij enen in het subnetmasker moet dus ingekort worden met 5 bits. Deze worden op 0 gezet. Dit gebeurt als volgt:

Subnetmasker (oud)	255.255.255.0	11111111.11111111.11111111.00000000
Subnetmasker (nieuw)	255.255.224.0	11111111.11111111.11100000.00000000

Het nieuwe subnetmasker is dus 255.255.224.0. Als we het subnet van beide IP-adressen wederom berekenen, komen we op het volgende subnet uit:

IP-adres regelaar	192.168.1.191	11000000.10101000.00000001.10111111
Subnetmasker	255.255.224.0	11111111.11111111.11100000.00000000 <AND>
Subnet	192.168.0.0	11000000.10101000.00000000.00000000

IP-adres eigen	192.168.26.5	11000000.10101000.00011010.00000101
Subnetmasker	255.255.224.0	11111111.11111111.11100000.00000000 <AND>
Subnet	192.168.0.0	11000000.10101000.00000000.00000000

Hieruit blijkt dat beide subnetten nu gelijk zijn. Dit regelaar kan nu gevonden worden.

Dit hoofdstuk is vooral bedoeld om de techniek van het bitsgewijs berekenen van subnetten uit te leggen. Op internet zijn diverse gratis tools beschikbaar om subnetten te berekenen. Zoek op 'IP Subnet calculator'

3 - Netwerkbegrippen

3.6 TCP

Het Transmission Control Protocol (TCP) is een connectie georiënteerd protocol dat garandeert dat de verstuurd pakketten geen fouten bevat. Een groot gedeelte van het internet communiceert door middel van het TCP protocol, mede om zijn betrouwbaarheid.

3.6.1 Poorten

Binnen het TCP protocol zijn er 65535 poorten beschikbaar. Hetzelfde aantal poorten is beschikbaar binnen het UDP protocol.

De analogie

Als de fysieke bekabeling wordt gezien als een wegennet, dan kan TCP (of UDP) worden gezien als een snelweg binnen dit wegennet, en de poorten de rijstroken op die snelweg. Ook hier gelden verkeersregels (protocollen): het wisselen van rijbaan (poort) tijdens de rit is verboden en gelijktijdig verkeer in twee richtingen op dezelfde rijbaan is onmogelijk. Wisselen van rijbaan is alleen toegestaan aan het eind van de rit. Tevens zijn er verschillende snelheden mogelijk waarmee het verkeer (de bits) zich kan voortbewegen.

De praktijk

Een programma 'luistert' naar of 'praat' over een specifieke poort; Als er via een webbrowser een webpagina wordt benaderd op een webserver zal de browser de initiële aanvraag naar de server doen over poort TCP 80 (HTTP) of TCP 443 (HTTPS). De webserver luistert op beide poorten, ziet de aanvraag en zal daarna aan de webbrowser de gevraagde pagina tonen via weer diezelfde poort als waarover de aanvraag heeft plaatsgevonden. Dit is een heel simplistische voorstelling van zaken maar in de basis is dit de correcte gang van zaken.

De BRControls regelapparatuur communiceert ook over een aantal van deze TCP en UDP poorten met bijvoorbeeld BRWebservice, softwarepakketten zoals BRScheduler, BRCollect en BRTrending maar ook internetdiensten zoals de weersvoorspellingsmodule, tijdserver, mailserver en dergelijke. waarbij de diverse functies weer een andere poort zullen gebruiken.

LET OP: Bepaalde netwerkkapparatuur zoals firewalls, virusscanners e.d. dienen dusdanig geconfigureerd te worden dat deze poorten en de daarop aanwezige data, onbeperkt worden toe- en doorgelaten.

Hierna een overzicht van de door BRControls gebruikte TCP en UDP poorten.

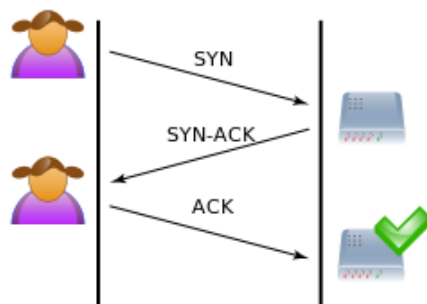
Toepassing	Protocol	Poort	Opmerking
FTP	TCP	21	Service/File Transfer
SSH/SFTP	TCP	22	Service/Secure File Transfer
TELNET	TCP	23	Service
SMTP	TCP	25	Email
HTTP/BRWebservice	TCP	80*	BRWebservice / API's
HTTPS/Azure/API	TCP	443	Microsoft Azure Eventhubs/API's
Modbus/BRModbus	TCP	501	Communicatie met derden
SMTP	TCP	2525	Email
BRWebservice	TCP	9001	Alternatief voor UDP 9000
BRScheduler	TCP	9051	BRControls Storingsserver
BRTrending	TCP	9052	BRControls Trendserver
BRCollect	TCP	9058	BRControls Databaseserver
FTP	TCP	40000 - 40010	Service/File Transfer
NTP	UDP	123	Tijdserver
SNMP	UDP	161-162	Managements- en prestatieinformatie
BRWebservice	UDP	9000*	BRWebservice

* = Minimaal benodigd voor BRWebservice

3 - Netwerkbegrippen

3.6.2 Verbinden

Om een TCP verbinding aan te maken, zal de aanvrager een SYN pakket versturen naar het opgegeven IP-adres. Indien het opgegeven adres bestaat, en deze toegekend is aan een BRControls regelaar, zal deze reageren met een bevestiging. Ook stuurt hij een aanvraag voor verbinding naar het bron-adres (SYN-ACK). Als dat bron-adres deze aanvraag bevestigt (ACK), is de verbinding tot stand gekomen, en kan de dataoverdracht beginnen. Deze manier van verbinding wordt 'hand-shaking' genoemd.



Afb. 25

Een TCP pakket zal elk pakket uitrusten met een controlesom (CRC), en een volgnummer. Het volgnummer is het aantal bytes data wat verstuurd is (exclusief TCP header). De controlesom is een wiskundige berekening over vrijwel het complete TCP pakket. Als een van deze twee niet klopt, zal het ontvangen pakket opnieuw opgevraagd worden. Deze twee controlemechanismen maken samen van het TCP een zeer robuust verbindingsprotocol.

3.6.3 Fouten

Bij het verbinden van de regelaar kan echter de configuratie van het netwerk dit onmogelijk maken. Indien de firewall de poort blokkeert, kan er geen verbinding gemaakt worden. BRConfig zal dan ook de regelaar niet kunnen vinden. De foutmelding '**Socket Error 10060**' zal getoond worden.

Indien er een '**Socket Error 10061**' tevoorschijn komt, is de geselecteerde poort nog niet open gezet, en wordt de verbinding door de regelaar geweigerd. De regelaar zit dan wel op betreffend IP-adres, maar wordt aangeroepen met de verkeerde poort.

Er zijn vele foutmeldingen mogelijk. Voor een compleet overzicht verwijs ik u naar de documentatie van BRConfig. In Appendix A van die documentatie staan alle mogelijke foutmeldingen beschreven.

3 - Netwerkbegrippen

3.7 UDP

Het User Datagram Protocol (UDP) is een van de kernprotocollen van het internet. Het protocol wordt vooral gebruikt in toepassingen waarbij de dataoverdracht minder kritisch is als bij TCP.

Het UDP protocol is niet connectie georiënteerd zoals TCP. Een datapakket wordt verzonden naar het opgegeven IP-adres. Óf het pakket daadwerkelijk aankomt op de bestemming, is niet belangrijk voor het UDP protocol (het fire-and-forget principe).

Ook binnen het UDP wordt met poorten gewerkt. De poort die BRControls standaard gebruikt is poort **9000**. Indien deze poort niet beschikbaar is, of de verbinding is niet betrouwbaar, kan er gekozen worden voor TCP poort 9001. Deze is echter wel langzamer. De uitleg omtrent de poorten in het hoofdstuk 'TCP' is beschreven, geldt ook voor het UDP protocol.

Aangezien het daadwerkelijke verbinding maken niet tot de taken behoort van het UDP protocol en er binnen het UDP protocol ook geen echte controlemechanismen aanwezig zijn, is dit protocol sneller dan TCP. Er hoeft immers minder te worden berekend, en de overhead per pakket is ook minder dan bij TCP.

Omdat de dataoverdracht naar een BRControls regelaar wel degelijk belangrijk is, is door BRControls een eigen protocol ontwikkeld (BouwHuis Communication Protocol (**BHCP**)), dat zich op de UDP laag bevindt. Dit protocol zorgt o.a. voor de foutcontrole. Verkeerd ontvangen data zal op een soortgelijke manier als TCP opnieuw opgevraagd worden.

Binnen het BHCP wordt gebruik gemaakt van het **BHCP-ID**. Dit is een ID dat uniek moet zijn binnen een netwerk van BRControls regelaars.



Hoofdstuk 4

Talstelsels

4 - Talstelsels

4 Talstelsels

Een talstelsel is een systeem om getallen weer te geven door middel van enkele cijfers en/of karakters. Binnen de programmatuur van BRControls wordt er gewerkt met de volgende talstelsels:

- **Binair** (grondtal 2)
- **Hexadecimaal** (grondtal 16)

Op de volgende pagina's worden deze stelsels behandeld.

Uiteraard maakt BRControls ook gebruik van de standaard talstelsels **decimaal** (grondtal 10), **duodecimaal** (grondtal 12) en **sexagesimaal** (grondtal 60). Aangezien iedereen hier dagelijks mee werkt zullen deze verder niet behandeld worden.

4.1 Binair talstelsel

Het binaire of tweetallige talstelsel is een positiestelsel, waarin een getal wordt voorgesteld door een rijtje van de cijfers 1 en 0. Een dergelijk cijfer wordt in deze context een bit ("binary digit") genoemd.

Een binaire variabele is een variabele die twee elkaar uitsluitende waarden kan aannemen, zoals 1 of 0, + of –, Ja of Nee, Waar of Onwaar, Aan of Uit.

Het binaire talstelsel is een positiestelsel, waarin iedere positie overeenkomt met een macht van 2. Bijvoorbeeld het getal 0101 in het binaire talstelsel representeert het getal 5 ($1 + 0 + 4 + 0$) in het decimale stelsel.

Bij geautomatiseerde opslag en communicatie van gegevens (zoals binnen en tussen computers in de ruime zin van het woord) worden deze vaak binair gecodeerd, dat wil zeggen als een reeks bits. Voor een kortere notatie wordt zo'n reeks bits vaak vertaald naar het hexadecimale of het octale stelsel, die beide nauw verwant zijn met het binaire. Zie ook BCD-code, als een tussenvorm tussen decimaal en binair.

Het octale en hexadecimale stelsel worden door computerprogrammeurs gebruikt bij taken waarbij ze de bitconfiguratie van het getal willen zien, omdat er direct hardware aangesproken wordt. In de hardware bestaat informatie uitsluitend in de vorm van reeksen enen en nullen.

Octale en hexadecimale getallen zijn uit binaire getallen af te leiden, namelijk door de binaire cijfers in groepjes van 3 (octaal) of 4 (hexadecimaal) te verdelen en deze groepjes van 3 respectievelijk 4 binaire cijfers steeds tot één octaal respectievelijk hexadecimaal cijfer om te zetten. Dit principe geldt voor alle getalstelsels waarvan het aantal cijfers een macht van twee is.

4 - Talstelsels

Van binair naar decimaal

Om een binair getal te vertalen naar een decimaal getal, hoeft men slechts te kijken naar de posities waar een 1 staat. Voor ieder binair cijfer 1 berekent men de door de positie van dit cijfer aangegeven macht van twee, en wel: $2^{\text{positie} - 1}$. De som van de op deze wijze berekende reeks decimale getallen geeft de waarde van het binaire getal decimaal weer. De eerste positie is de meest rechtse en komt overeen met het getal 1. De tweede positie, de tweede van rechts, komt overeen met het getal 2, de derde van rechts met 4, enz.

Binair	Decimaal
00000	0
00001	1
00010	2
00011	3
00100	4
00101	5
00110	6
00111	7
01000	8
01001	9
01010	10

Binair	$2^{(\text{positie van de 1}) - 1}$	Decimaal	Binair	$2^{(\text{positie van de 1}) - 1}$	Decimaal
100000	2^5	32			
010000	2^4	16	010000	2^4	16
001000	2^3	8			
000100	2^2	4	000100	2^2	4
000010	2^1	2			
000001	2^0	1	000001	2^0	1
111111	$2^5+2^4+2^3+2^2+2^1+2^0$	63	010101	$2^4+2^2+2^0$	21

Simpel gezegd: bereken voor elk cijfer 1 in het binaire getal, de overeenkomstige macht van 2. Een binair getal van 6 cijfers, bijvoorbeeld 111111, wordt vertaald in (van links naar rechts) 32, 16, 8, 4, 2 en 1. De som $32 + 16 + 8 + 4 + 2 + 1 = 63$ is de decimale waarde van dit binaire getal. Zo wordt 010101 $16 + 4 + 1 = 21$ in decimale waarden.

Eenvoudig omrekenen

In	256	128	64	32	16	8	4	2	1	Uit
001101010	0	0	1	1	0	1	0	1	0	=106
			+64	+32		+8		+2		
100010000	1	0	0	0	1	0	0	0	0	=272
	+256				+16					
57				-32	-16	-8	0	0	-1	=11001
				1	1	1	0	0	1	

Bovenstaande tabel is een eenvoudig hulpmiddel voor het omrekenen van binair naar tientallig en andersom. Stel er is het binaire getal 001101010. Vul dit in de tabel in en kijk naar de waarde in de bovenste rij. Bij het voorbeeld zijn dit de waarden 64, 32, 8 en 2. Door deze op te tellen is nu bekend hoeveel 001101010 in het tientalligstelsel is, namelijk 106. Het tweede voorbeeld - 100010000 - wordt dan 272.

Een andere methode bestaat erin om bij de eerste "1" links te starten en het volgende algoritme toe te passen. 1 onthouden, schuif een plaats naar rechts. Hiervoor doen we $1 \times 2 = 2$ en onthouden 2. We komen op het tweede cijfer terecht. Is dit 0 dan doen we $2 + 0 = 2$ en schuiven een plaats op naar rechts. Hiervoor doen we $2 \times 2 = 4$. Was het tweede cijfer 1 dan deden we $2 + 1 = 3$ en schuiven we een plaats naar rechts. Hiervoor doen we $3 \times 2 = 6$. Deze methode wordt verder toegepast tot het einde der cijfers. Toegepast op het binaire getal 001101010 geeft dit: 1 wordt 1 plaats opgeschoven en wordt 2; $2 + 1 = 3$ en na opschuiven wordt het 6; $6 + 0 = 6$ en wordt na opschuiven 12; $12 + 1 = 13$ en wordt na opschuiven 26; $26 + 0 = 26$ en wordt na opschuiven 52; $52 + 1 = 53$ en wordt na 1 plaats opschuiven 106. Er zijn verder geen cijfers meer en de uitkomst is dus 106.

4 - Talstelsels

Andersom is iets moeilijker. Stel we willen het getal 57 omzetten. Dan zoeken we eerst het grootste getal in de bovenste rij dat kleiner is dan of gelijk aan 57, namelijk 32. Op die plek zetten we al een 1. Dit wordt dan (000)100000. Dan trekken we 32 van 57 af, dat wordt 25. Voor dit getal zoeken we weer het grootste getal in de bovenste rij dat kleiner is dan of gelijk aan 25, namelijk 16. Ook voor de 16 zetten we een 1, dus (000)110000. We trekken 16 van 25 af, dat wordt 9. We zoeken weer het grootste getal in de bovenste rij dat kleiner is dan of gelijk aan 9, namelijk 8. Voor deze zetten we weer een 1. (000)111000. $9-8=1$. Nu hoeven we niet verder te zoeken, want de 1 is makkelijk gevonden. Ook deze wordt toegevoegd. Zo hebben we relatief eenvoudig berekend dat 57 binair 000111001 ofwel 111001 is.

Eenvoudiger kan ook op de volgende manier. We beginnen het binaire getal van rechts naar links te noteren. Is het getal oneven dan legt men rechts een 1 neer. We trekken van het oorspronkelijke getal 1 af en gaan één plaats naar links door het overblijvende getal te delen door 2. Is dit getal oneven dan legt men op de tweede plaats van rechts te beginnen een 1 neer. In het andere geval een 0. We trekken respectievelijk 1 of 0 af van het getal en gaan verder een plaats naar links door dit getal te delen door 2.

Toegepast op 57 geeft dit het volgende. 57 is oneven en we schrijven rechts een 1. $57-1=56$, we schuiven een plaats naar links op en delen hiervoor 56 door 2 en dit geeft 28. 28 is even en we schrijven dus een 0 (de twee laatste cijfers van de binaire notatie zijn reeds bekend: 01). We schuiven de overblijvende 28 een plaats naar links en delen hiervoor 28 door 2 en dit geeft 14. 14 is even en we schrijven dus een 0 (de drie laatste cijfers van de binaire notatie zijn reeds bekend: 001). We schuiven de overblijvende 14 een plaats naar links en delen hiervoor 14 door 2 en dit geeft 7. 7 is oneven en we schrijven dus een 1 (de vier laatste cijfers van de binaire notatie zijn reeds bekend: 1001). $7-1=6$, we schuiven een plaats naar links op en delen hiervoor 6 door 2 en dit geeft 3. 3 is oneven en we schrijven dus een 1 (de vijf laatste cijfers van de binaire notatie zijn reeds bekend: 11001). $3-1=2$, we schuiven een plaats naar links op en delen hiervoor 2 door 2 en dit geeft 1. 1 is oneven en we schrijven dus een 1 (de zes cijfers van de binaire notatie zijn bekend: 111001).

4 - Talstelsels

4.1.1 Boleaanse operatoren

Een booleaanse operator is een logische operator die vooral in de wiskunde en informatica wordt gebruikt. Booleaanse operatoren zijn gebaseerd op de booleaanse algebra. Het resultaat van een booleaanse bewerking heeft slechts twee mogelijke resultaten: waar (1) of onwaar (0). In verschillende talen die in de wiskunde en informatica worden gebruikt, bestaan er verschillende aanduidingen (tekens) voor de booleaanse operatoren.

AND

De operator **AND** (én) is de logische conjunctie. **A AND B** is alleen waar als **A** en **B** beide waar zijn, in alle andere gevallen is het resultaat onwaar.

Waarheidstabel

<i>A</i>	<i>B</i>	$A \wedge B$
0	0	0
0	1	0
1	0	0
1	1	1

OR

De operator **OR** (of) is de logische disjunctie.

A OR B is waar als **A** waar is of **B** waar is of beide waar zijn. Het resultaat is onwaar als zowel **A** als **B** onwaar zijn.

Waarheidstabel

<i>A</i>	<i>B</i>	$A \vee B$
0	0	0
0	1	1
1	0	1
1	1	1

XOR

De operator **XOR** (eXclusive OR) is de exclusieve disjunctie.

A XOR B is waar als **A** waar is en **B** onwaar of als **A** onwaar is en **B** waar

Waarheidstabel

<i>A</i>	<i>B</i>	$A \underline{\vee} B$
0	0	0
0	1	1
1	0	1
1	1	0

4 - Talstelsels

Door het toevoegen van een **NOT** functieblok in logi.CAD op de uitgang van de **AND**, **OR** of **XOR**, zijn alle bovenstaande functies te inverteren waardoor een **NAND**, **NOR** en **XNOR** zullen ontstaan.

NAND

Waarheidstabel

A	B	$A \overline{\wedge} B$
0	0	1
0	1	1
1	0	1
1	1	0

NOR

Waarheidstabel

A	B	$A \overline{\vee} B$
0	0	1
0	1	0
1	0	0
1	1	0

XNOR

Waarheidstabel

A	B	$A \leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

4 - Talstelsels

4.2 Hexadecimaal talstelsel

Hexadecimaal betekent letterlijk zestientallig.

Het is een talstelsel waarbij niet, zoals gebruikelijk, met tien cijfers wordt gewerkt, maar met zestien cijfers. De cijfers 0 t/m 9 worden daarom uitgebreid met 'A' (=10) t/m 'F' (=15), ook wel 'a' t/m 'f'. In deze context zijn dat dus ook cijfers, geen letters.

In de computerwereld wordt de hexadecimale voorstelling van getallen veel gebruikt, omdat deze manier van representeren goed aansluit bij de binaire representatie in de computer.

Het woord 'hexadecimaal' wordt vaak afgekort als hex, hoewel dit 'zes' betekent.

Codering

Met een binair getal van vier bits (nibble) kunnen de getallen 0 t/m 15 decimaal worden weergegeven en dus ook een hexadecimaal getal bestaande uit slechts één (hexadecimaal) cijfer (0..F).

Door steeds groepen van vier opeenvolgende bits in een binair getal als een hexadecimaal cijfer te schrijven ontstaat een hexadecimaal getal, dat voor ons overzichtelijker is dan de rij 0-en en 1-en.

De rij 11000101011000100101110101110010 bijvoorbeeld is voor mensen praktisch onleesbaar. Daarom worden de cijfers in groepjes van vier (nibbles) gegroepeerd. Dat wordt dan 1100-0101-0110-0010-0101-1101-0111-0010. Ieder viertal wordt vervolgens in een hexadecimaal cijfer omgezet: C5625D72. Dit is veel overzichtelijker.

Notatie

Om duidelijk te maken dat men een hexadecimale waarde bedoelt, worden vaak enkele tekens toegevoegd. Bovendien geldt in bijna elke programmeertaal de eis dat een waarde met een 'echt' cijfer begint (dus niet met A-F). Het hexadecimale getal 35 kan geschreven worden als '35x' of '35h', en in een programmeertaal als '0x35'. Zou men in een programmeertaal '35' schrijven, dan wordt dat decimaal opgevat.

Enkele voorbeelden voor het hexadecimale getal ABCD:

- ABCDh (begint met een letter, niet mogelijk in veel programmeertalen)
- 0ABCDh (door een nul toe te voegen wordt dat probleem verholpen)
- 0xABCD (meest gebruikte notatie)
- \$ABCD
- x'ABCD'

4 - Talstelsels

Diverse getalnotaties vergeleken

hex	dec	oct	bin
00	0	000	0000 0000
01	1	001	0000 0001
02	2	002	0000 0010
03	3	003	0000 0011
04	4	004	0000 0100
05	5	005	0000 0101
06	6	006	0000 0110
07	7	007	0000 0111
08	8	010	0000 1000
09	9	011	0000 1001
0A	10	012	0000 1010
0B	11	013	0000 1011
0C	12	014	0000 1100
0D	13	015	0000 1101
0E	14	016	0000 1110
0F	15	017	0000 1111
10	16	020	0001 0000
11	17	021	0001 0001
64	100	144	0110 0100
FF	255	377	1111 1111
100	256	400	1 0000 0000

4 - Talstelsels

4.3 Datatypes

Binnen de apparatuur van BRControls wordt er gebruik gemaakt van verschillende datatypes.

De verschillende datatypes zijn:

Type	Bits
Bit	1
Nibble	4
Byte	8
Word	16
Floating point / real	32
Floating point (no multiply)	32
DWORD	32
Long	32
Integer	32
Double float	64
QWORD	64

Negatieve waarden

Een datatype kan signed of unsigned zijn.

Een **signed** type geeft aan dat het datatype ook **negatieve waarden** kan bevatten (het MSB is het signbit). Een unsigned datatype geeft aan dat de waarde uitsluitend positieve waarden kan bevatten.

Bij een signed waarde komt de 0-waarde in het midden van het bereik te liggen.

Bijvoorbeeld:

- Een unsigned WORD heeft een waarde van 0..65535
- Een signed WORD heeft een waarde van -32767...+32767

Een analoge ingang(AIR), uitgang(AOR) en setpoint (SP) gebruiken als data type een real. Dit is een 'drijvend komma getal' ook wel 'floating point' genoemd. Deze term mag vergeten worden; wat wel belangrijk is, is het feit dat een real een heel klein getal, of een heel groot getal kan bevatten. Het kleinste getal wat kan worden opgeslagen in een real is een getal met de komma circa 37 plaatsen naar voren. Het grootste getal wat kan worden opgeslagen is een getal met de komma 37 plaatsen naar achteren. Hieruit voortkomende kan gesteld worden dat de minimum of maximum waarde van de real binnen BRControls producten nooit gehaald zal worden.

Een digitale ingang(DI) of uitgang(DO) gebruikt als data type een boolean. Dit is een 1 bits 'getal', die de waarde 0 (false) of 1 (true) kan hebben. Dit geldt ook voor een digitale waarde extern protocol (SIODI).

Een alarm (AL), analoge waarde extern protocol (SIOAL), Control register (CONTROL) of een variabele (VAR) heeft als data type een integer. Dit is een 32-bits getal, waarvan de minimale waarde -2147483648 en de maximale waarde +2147483648 is. Dit betreft dus een signed waarde.

Een BUS-punt (BUS) en scada punt (SCD) kunnen alle soorten waardes bevatten.

Een (PT) gebruikt als waarde een UDINT. Dit is een unsigned integer die loopt van 0...4294967295.

4 - Talstelsels

4.3.1 Endianness

Onder endianness of bytevolgorde verstaat men in de informatica de manier waarop woorden, die zelf uit meerdere bytes bestaan, in het computergeheugen worden opgeslagen. Het gaat daarbij om de volgorde in het geheugen van de bytes die samen een woord vormen. Wordt de meest significante byte het eerst geschreven, dan spreekt men van big-endian; schrijft men juist de minst significante byte eerst, dan van little-endian. Sommige systemen hebben aspecten van beide, die noemt men middle-endian.

Als voorbeeld kan gedacht worden aan de manier waarop we onze (decimale) getallen schrijven. Als eerste noteren we het meest significante cijfer en vervolgens steeds het minder significant. Het belangrijkste einde, het "big end", komt eerst; deze manier wordt big-endian genoemd (zie de etymologie). Bij het uitspreken van getallen gebruiken we deze manier ook, met uitzondering van 13 tot en met 99, want daar noemen we het minst belangrijke deel eerst.

Endianness bij computers

Het probleem van endianness treedt onder andere op bij bestandsformaten, communicatieprotocollen en registers in computerapparatuur. Er zijn verschillende manieren om dit probleem op te lossen. De eenvoudigste is door simpelweg te kiezen voor een bepaalde endianness en apparatuur die hiervan afwijkt, de conversie zelf laten doen. Het internet is bijvoorbeeld big-endian. Alle apparatuur dient hier te communiceren volgens deze afspraak, zelfs als beide kanten van een verbinding normaal gesproken little-endian zijn.

Bij het bewaren van een 32 bitswaarde, bijvoorbeeld 4A3B2C1D (hexadecimale notatie) op geheugenplaats 100, kunnen de verschillende bytes als volgt bewaard worden:

Big-endian

	100	101	102	103	
...	4A	3B	2C	1D	...

De meest significante byte 4A wordt hier dus eerst geplaatst. Dit noemt men big-endian (ezelsbruggetje: "big end first").

Little-endian

	100	101	102	103	
...	1D	2C	3B	4A	...

Hier wordt de minst significante byte eerst gezet, dit heet little-endian (ezelsbruggetje: "little end first").

Geen van de genoemde systemen heeft specifieke voordelen, maar Intel gebruikt in zijn x86-processors het little-endian-systeem, waardoor deze tegenwoordig veruit het meest toegepast wordt bij processoren. Bij de uitwisseling van gegevens tussen computers met verschillende endianness kunnen fouten ontstaan indien geen rekening wordt gehouden met dit verschil.

Voetnoot

Deze documentatie is met de grootst mogelijke zorgvuldigheid samengesteld. Indien u toch fouten ontdekt of opmerkingen/toevoegingen heeft aan dit document verzoeken wij u een email te sturen aan documentatie@brcontrols.com

© 2021 BRControls Products BV