SERIELE COMMUNICATIE

Project Arduino semester 2, 2015

Frank Van Aelst

Inhoud

[1. Communicatie en probleemstelling 6](#_Toc438491881)

[1.1 Serieel versus parallel 6](#_Toc438491882)

[2. Verschillende standaarden 7](#_Toc438491883)

[2.1 RS-232, RS422 en RS-485 (soms ook wel EIA-232, EIA-422, EIA-485) 7](#_Toc438491884)

[2.2 I2C of TWI communicatie 9](#_Toc438491885)

[2.2.1 Werking 9](#_Toc438491886)

[2.2.2 De werking van I2C dataoverdracht: 9](#_Toc438491887)

[2.2.3 Voordelen 10](#_Toc438491888)

[2.2.4 Nadelen 10](#_Toc438491889)

[2.2.5 Latere versies 10](#_Toc438491890)

[2.3 Serial Peripheral Interface 11](#_Toc438491891)

[2.3.1 Benaming 11](#_Toc438491892)

[2.3.2 Configuratie 11](#_Toc438491893)

[2.3.3 Start communicatie 11](#_Toc438491894)

[2.3.4 Voordelen 12](#_Toc438491895)

[2.3.5 Nadelen 12](#_Toc438491896)

[2.4 TCP/IP 13](#_Toc438491897)

[2.4.1 Geschiedenis 13](#_Toc438491898)

[2.4.2 Kenmerken 13](#_Toc438491899)

[2.4.3 Lagen 14](#_Toc438491900)

[2.5 FireWire 14](#_Toc438491901)

[2.5.1 Vormen 14](#_Toc438491902)

[2.5.2 Ontwikkeling 15](#_Toc438491903)

[2.6 xDSL 15](#_Toc438491904)

[2.6.1 Varianten 15](#_Toc438491905)

[2.6.2 Apparatuur 16](#_Toc438491906)

[2.6.3 DSL technologieën 16](#_Toc438491907)

[2.7 Integrated Services Digital Network (ISDN) 17](#_Toc438491908)

[2.7.1 Kenmerken 17](#_Toc438491909)

[2.7.2 Algemeen 18](#_Toc438491910)

[2.8 Universal Serial Bus (USB) 19](#_Toc438491911)

[2.8.1 Doelen 19](#_Toc438491912)

[2.8.2 Varianten 19](#_Toc438491913)

[2.8.3 Eigenschappen 20](#_Toc438491914)

[2.8.4 Techniek 20](#_Toc438491915)

[2.9 Local area network 21](#_Toc438491916)

[2.9.1 Toepassingen 21](#_Toc438491917)

[2.9.2 Techniek 21](#_Toc438491918)

[2.10 CAN bus 22](#_Toc438491919)

[2.11 Draadloos netwerk 23](#_Toc438491920)

[2.12 Wireless LAN 23](#_Toc438491921)

[2.13 Bluetooth 24](#_Toc438491922)

[2.13.1 Geschiedenis 24](#_Toc438491923)

[2.13.2 De techniek 25](#_Toc438491924)

[2.13.3 Toepassingen 25](#_Toc438491925)

[2.13.4 Beveiliging 25](#_Toc438491926)

[2.14 IrDA 26](#_Toc438491927)

[2.14.1 Karakteristieken 26](#_Toc438491928)

[2.14.2 Bluetooth versus IrDA 27](#_Toc438491929)

[2.15 ZigBee 28](#_Toc438491930)

[2.15.1 Algemeen 28](#_Toc438491931)

[2.15.2 Netwerkcomponenten 29](#_Toc438491932)

[2.16 WIFI 29](#_Toc438491933)

[2.16.1 Topologieën 30](#_Toc438491934)

[2.16.2 Versleuteling 30](#_Toc438491935)

[2.16.3 ZigBee versus Bluetooth versus wifi 31](#_Toc438491936)

[2.17 Near field communication 32](#_Toc438491937)

[2.17.1 Kenmerken 32](#_Toc438491938)

[2.17.2 Toepassingen 32](#_Toc438491939)

[2.17.3 Problemen 33](#_Toc438491940)

[2.18 Radio-frequency identification (RFID) 33](#_Toc438491941)

[2.18.1 Soorten 33](#_Toc438491942)

[2.18.2 Voor- en nadelen 34](#_Toc438491943)

[2.18.3 Problemen 35](#_Toc438491944)

[2.19 MIFARE 36](#_Toc438491945)

[2.19.1 MIFARE Classic 36](#_Toc438491946)

[2.19.2 MIFARE Ultralight 37](#_Toc438491947)

[2.19.3 MIFARE DESFire 37](#_Toc438491948)

[2.19.4 Veiligheid 37](#_Toc438491949)

[2.20 X10 37](#_Toc438491950)

[2.20.1 Werking X10 power line 38](#_Toc438491951)

[2.20.2 Protocol 38](#_Toc438491952)

[2.21 Andere mogelijke technieken 38](#_Toc438491953)

[3. Toepassingen 40](#_Toc438491954)

[3.1 I2C interface 40](#_Toc438491955)

[3.1.1 LCD display met I2C interface 42](#_Toc438491956)

[3.1.2 Andere toepassingen 43](#_Toc438491957)

[3.1.3 I2C met meerdere Arduino’s 45](#_Toc438491958)

[3.1.4 Nuttige toepassing van dit I2C-bus systeem 45](#_Toc438491959)

[3.2 SPI Interface 46](#_Toc438491960)

[3.2.1 RFID of NFC interface 46](#_Toc438491961)

[3.3 Seriële communicatie of UART-verbinding 47](#_Toc438491962)

[3.4 De praktijk 48](#_Toc438491963)

[3.4.1 Het LCD display aansturen met I2C 48](#_Toc438491964)

[3.4.2 RFID / NFC uitlezen met SPI 49](#_Toc438491965)

[3.4.3 Bluetooth met een serial connection (TX en RX) 53](#_Toc438491966)

[3.4.4 Twee Arduino’s 57](#_Toc438491967)

[3.4.5 RFID lezer met display 57](#_Toc438491968)

[4. BRONNEN 58](#_Toc438491969)

# Communicatie en probleemstelling

Seriële verbinding is al van in de telegraaftijd gekend, de letters werden letter voor letter verstuurd, ook de telex was een seriële toepassing. Maar laten dit voor de geschiedenisles.

Seriële communicatie tussen verschillende componenten heeft het grote voordeel dat je met een minimum aan verbindingen veel kan versturen. Bij parallelle communicatie ben je snel uitgeput wanneer het om beschikbare pinnen gaat. Er zijn verschillende methoden om dit te realiseren, de meest gekende ga ik hier in dit werk proberen kort te bespreken, maar afhankelijk van de beschikbare tijd zal er dieper worden ingegaan in de verschillende protocollen. (protocol = gedragsovereenkomst)

We starten met wat theorie, zeker niet diepgaand, we overlopen de meer gebruikte technieken. Gaan vervolgens kijken hoe we bekabeld een verbinding kunnen realiseren, om daarna draadloos afstanden te overbruggen.

De Arduino kan van “nature” drie verschillende protocol’s aan, deze ga ik ook met een praktijk voorbeeld uitwerken.

## 1.1 Serieel versus parallel

Vooraf dit nog: je kan een 8-bits woord doorgeven op twee manieren, bij parallel gaan die 8-bits allemaal te gelijk door naar de volgende stap. Of je zendt ze een voor een na mekaar naar de volgende stap via een seriële verbinding. Parallel gaat veel sneller omdat er geen tussenstappen zijn, we vergelijken dit wel bij een gelijke kloksnelheid. Een seriële bewerking is complexer, je moet eerst het 8-bits woord inlezen in het geheugen van een schuifregister van de zender, daarna schuiven we dit bit na bit door naar het schuifregister van de ontvanger, om daar het 8-bits woord terug om te zetten naar een 8-bits-parallel woord.

We kunnen met een voorbeeld eenvoudig het probleem schetsen. Stel we willen een LCD display aansturen dan hebben we hiervoor minimum 6 verbindingen nodig. Als we dit serieel zouden oplossen dan komen we met twee verbindingen toe. We sparen dus 4 poorten die we voor iets anders kunnen gebruiken.

Breiden we uit en gaan we met verschillende Arduino’s lokaal allerlei gegevens verzamelen en die daarna naar een centrale computer sturen dan kunnen we vanop een plaatst alles observeren en controleren. We sparen heel wat draad uit door alles te bundelen en deze data via een enkele seriële verbinding naar de Master (hier de PC) te sturen. De lokale Arduino’s zijn de Slaves in dit opzet. Die verbinding kan via een draad zijn, maar ook draadloos.

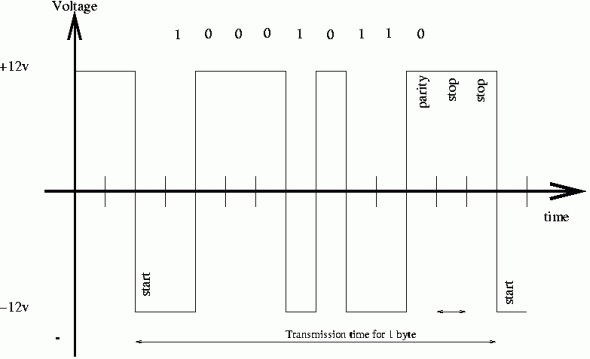
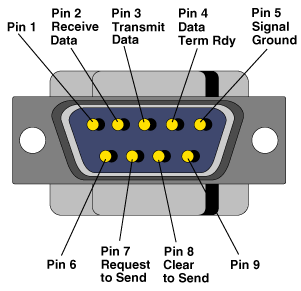
# Verschillende standaarden

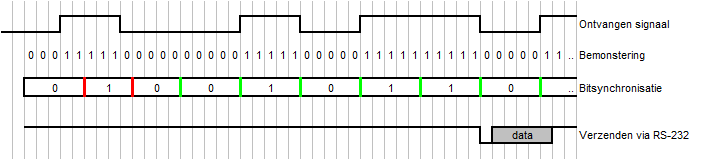
Op Wikipedia vind je veel informatie, in de lijst van de bronnen vind je de linken naar de verschillende artikelen waaruit ik de samenvatting heb gemaakt, uit dit destillaat heb ik enkel de meest belangrijkste zaken behouden die van toepassing kunnen zijn voor ons. Uiteraard is de opsomming zeer leerrijk, maar ik neem aan, ook misschien te veel van het goede als je praktisch bent aangelegd. In dat geval kan je direct naar het derde hoofdstuk waar er enkele toepassingen worden besproken.

## 2.1 RS-232, RS422 en RS-485 (soms ook wel EIA-232, EIA-422, EIA-485)

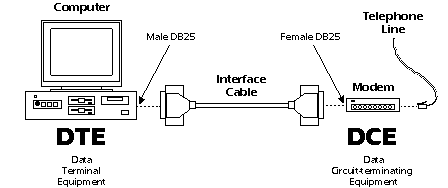
Men spreekt soms ook over UART verbinding. Dit staat voor Universal Asynchronous Receiver Transmitter

Principe:

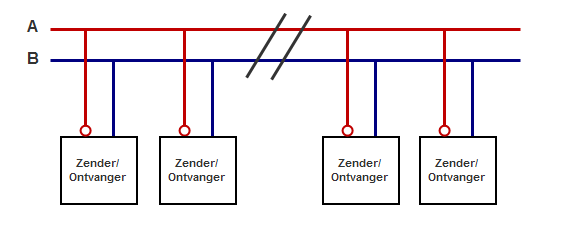




De RS-232 is veruit de oudste seriële verbinding die het levenslicht zag in 1969. Computers hadden tot begin deze eeuw nog een seriële poort, de typische SUBD9 poort, een connector met 9 pinnetjes. De allereerste hadden zelfs 25-pinnen. Je vindt ze nog in industriële omgevingen maar worden al lange tijd vervangen door de USB-poort, die vele malen sneller is. De verbeterde RS-422 en de RS-485 kunnen een grotere afstand overbruggen dan de RS-232, maar verder zijn ze sterk gelijkend. Een kleine opmerking, de RS-485 is eigenlijk een 4-draads systeem en kan in een bus structuur werken. Deze standaard is t.o.v. de eerste versie sterk verbeterd en wordt nog regelmatig gebruikt in industriële toepassingen.



RS-232



RS-485

Even vooruit lopend, deze techniek kan gebruikt worden in draadloze toepassingen



## 2.2 I2C of TWI communicatie

Door Philips ontwikkeld in 1979 en nu onder de vleugels van NXP, die deze standaard verder onderhoud. Het is de afkorting van Inter-IC-bus of ook nog Two-Wire-Interface. Het is zoals de naam al doet vermoeden een bus die gebruikt wordt binnen een kleine (IC) omgeving, meestal binnen een toestel. De betrouwbaarheid van deze bus was oorspronkelijk maar 1m en had een overdrachtsnelheid van 100kbit/sec vandaag is die snelheid al serieus opgevoerd naar 3.4Mbit/sec.

### 2.2.1 Werking

I2C werkt op basis van twee bus lijnen, namelijk SDA (serial data) en SCL (serial clock). Over de SDA-lijn worden de data verzonden en over de SCL-lijn wordt het kloksignaal verzonden. In het onderstaande timingdiagram wordt verduidelijkt hoe de SDA en SCL samenwerken:

[](https://commons.wikimedia.org/wiki/File:I2C_data_transfer.svg)

### 2.2.2 De werking van I2C dataoverdracht:

Data verzenden wordt geïnitieerd met een STARTbit (S) die de SDA het signaal geeft om omlaag getrokken te worden, terwijl de SCL hoog blijft.

SDA zet de eerste databit gelijk, terwijl SCL laag gehouden wordt (gedurende de blauwe tijdsbalk.). De data worden ontvangen, als SCL naar omhoog gaat (groen).

Als de overdracht compleet is wordt een STOPbit (P) verzonden door de datalijn vrij te geven en deze zo in staat te stellen om omhoog getrokken te worden, terwijl SCL continu hoog gehouden wordt.

Ten einde valse detecties te voorkomen, wordt het niveau van de SDA veranderd op de dalende flank (overgang van hoog naar laag) van SCL. Het uitlezen gebeurt op de stijgende flank (de overgang van laag naar hoog) van SCL.

Om te kunnen communiceren heeft I2C één master nodig en minimaal één slave. De master heeft de controle over de I2C-bus en genereert het kloksignaal, startbit en stopbit. De slaves communiceren alleen dan, nadat de master daartoe een verzoek stuurt.

Om te communiceren stuurt de master eerst een startbit. Die bestaat uit een hoog-naar-laagsignaal op de SDA lijn (flankgestuurd) terwijl de SCL-lijn hoog is. Vervolgens stuurt de master een adres plus een read/writebit over de I2C-lijn. De read/writebit geeft aan of de master data wil versturen of wil ontvangen. De slave die het aangeroepen adres heeft, zal dan reageren met een 'acknowledge', zodat de master weet dat het aangeroepen IC actief is.

Nu kunnen de data worden verzonden. Er wordt één byte per keer verzonden plus een 'acknowledge' van de ontvanger om te bevestigen dat de data zijn ontvangen. Nadat de data zijn verstuurd, zal de master de stopbit verzenden: een laag-naar-hoogsignaal op de SDA-lijn (flankgestuurd), terwijl de SCL-lijn hoog is.

Om goed te kunnen werken is het verstandig de beide buslijnen hoog te houden door een pull-upweerstand. De waarde van de weerstand is afhankelijk van de spanning op de bus (bij 3,3 V systemen tussen ongeveer 1,8 kΩ en 2,7 kΩ, maar bij 5V meestal 4,7 kΩ). Dit is ook afhankelijk van de snelheid waarmee men de bus wil laten werken.

### 2.2.3 Voordelen

Bij geschikte toepassingen zijn belangrijkste voordelen:

* Lage kostprijs.
* Eenvoudige bedrading (slechts twee signaalleidingen).
* Weinig soldeerpunten, kleine IC's.
* Uitgebreid gamma IC's met de I2C-interface.
* Compatibele IC's van andere fabrikanten.
* Robuuste bouw.
* Langzame perifere chips kunnen wachtcycli afdwingen.
* Geïntegreerde multimaster mogelijkheid, dat wil zeggen meerdere microcontrollers (masters) kunnen dezelfde bus gebruiken en zelfs onderling communiceren.

### 2.2.4 Nadelen

* Naast de vele voordelen zijn er ook enkele nadelen:
* Als er één aangesloten chip (IC) niet goed functioneert in de I2C -bus, kan dit de hele lijn van I2C blokkeren, zodat er helemaal geen communicatie meer op de I2C-lijnen kan plaatsvinden.
* I2C wordt traag bij grotere hoeveelheden data.

### 2.2.5 Latere versies

In latere versies van de I2C-bus zijn er verschillende verbeteringen aangebracht. Zo is onder andere de maximale snelheid verhoogd naar 400 kbit/sec (Fast-mode) en weer later naar 3,4 Mbit/sec (High-speed mode), is de adresseringsruimte van aangesloten IC's vergroot van 7 naar 10 [bit](https://nl.wikipedia.org/wiki/Bit_(informatica)) en zijn er voorzieningen gekomen om I2C-bussen met verschillende voedingsspanningen te verbinden.

Arduino heeft een speciale library die deze standaard ondersteunt: Arduino Wire Library. Vele modules die je kan kopen voor Arduino werken met deze standaard: sommige LCD module, toetsenborden, sensoren, interfaces, SD readers, enz.

## 2.3 Serial Peripheral Interface

**Serial Peripheral Interface** (SPI) is een synchrone seriële data link tussen ten minste 2 mediums. Er is altijd sprake van 1 master en 1 slave. De communicatie tussen de Master en de Slave gebeurt te allen tijde in full duplex. De start van de communicatie gebeurt door de master chip. Het is mogelijk om meerdere Slaves in te zetten maar ze moeten dan ieder een aparte chip select hebben. Er zijn altijd 4 verbindingen voor communicatie nodig, daarom spreken we over een four-wire seriële [bus](https://nl.wikipedia.org/wiki/Databus_(elektronica)).

### 2.3.1 Benaming

* SCLK : Seriële CLocK: wordt geleverd door de master.
* MOSI : Master Output Slave Input: op deze lijn wordt de data verzonden die de output van de master en de input van de slave is.
* MISO: Master Input Slave Output: de data van de slave wordt hierover naar de master gestuurd.
* SS: Slave Select: Deze lijn wordt actief laag aangestuurd. De lijn voor de geselecteerde slave zal laag zijn. Wanneer de communicatie met de slave gedaan is zal de lijn een logische 1 krijgen.

### 2.3.2 Configuratie

Meestal heeft iedere slave een eigen slave select-lijn, maar in sommige gevallen kunnen verschillende slaves in een keten (daisy-chain) zijn opgenomen, waarbij de MISO-poort van iedere slave is verbonden met de MOSI-poort van de eerstvolgende slave in de keten. De MISO-poort van de laatste slave in de keten is verbonden met de MISO-poort van de master. Alle Slave select-poorten in de keten zijn met elkaar verbonden. Deze configuratie maakt individuele adressering overbodig, maar gaat ten koste van de datasnelheid.

### 2.3.3 Start communicatie

De communicatie start met het selecteren van een juiste werk snelheid of anders verwoord, het selecteren van een kloksnelheid. Deze snelheid kan behoorlijk variëren van 1 MHz tot 100 MHz. De snelheid moet binnen het bereik van de master en de slave liggen. Het is mogelijk dat de master tegen grotere snelheid kan werken dan de slave maar het omgekeerde kan ook.

Vervolgens zal op de juiste slave select lijn een logische 0 gestuurd worden. Als er maar 1 chip (slave) is kan men deze lijn permanent op 0 houden. Het is mogelijk dat de chip pas werkt wanneer hij een edge (van hoog naar laag) detecteert. In dit geval mogen we de lijn niet op een logische 0 houden. Deze slave select hangt zeer nauw samen met het sturen van de klokpulsen. Sommige chips hebben een wachtperiode nodig vooraleer je de klokpulsen naar de slave mag sturen zoals een DAC of ADC. Vervolgens zal er per klok cyclus een volledig duplex signaal doorgestuurd worden. Namelijk zowel de master als de slave zullen een bit doorsturen. De master zal over de MOSI lijn sturen en de slave zal van deze lijn aflezen. Het omgekeerde zal op de MISO lijn gebeuren. De slave zal data sturen en de master zal van deze lijn aflezen. In vele gevallen wordt er gebruikgemaakt van shift registers. Meestal is de register grootte 8 bits en wordt de least significant bit eerst gestuurd maar dit is niet altijd het geval. Wanneer het complete register is doorgestuurd wordt de data verwerkt. Dit kan inhouden dat de data weggeschreven wordt naar het geheugen. Wanneer er meer data verstuurd moet worden zal de data ingeladen worden en beginnen we weer vanaf het begin.

### 2.3.4 Voordelen

* [Full duplex](https://nl.wikipedia.org/wiki/Full_duplex)
* Snellere communicatie dan bijvoorbeeld de [I²C-bus](https://nl.wikipedia.org/wiki/I%C2%B2C-bus)
* Geen limiet aan woord grootte dat doorgestuurd moet worden
* Eenvoudige hardware
* geen behoefte aan adressering
* geen oscillator voor slave apart
* laag energieverbruik
* geen transceivers nodig
* maar 4 pinnen nodig
* Kan zeer hoge kloksnelheden aan

### 2.3.5 Nadelen

* Meer pinnen dan I²C nodig
* Geen controle door de slave (master kan klok vertragen slave niet)
* Geen controle of er wel iets verbonden is
* Maar 1 master maximaal
* Geen error checking
* Gevoelig voor ruis

## 2.4 TCP/IP

**TCP/IP** is een verzamelnaam voor de reeks [netwerkprotocollen](https://nl.wikipedia.org/wiki/Protocol) die voor een grote meerderheid van de netwerkcommunicatie tussen [computers](https://nl.wikipedia.org/wiki/Computer) instaan. Het [internet](https://nl.wikipedia.org/wiki/Internet) is het grootste en bekendste TCP/IP-[netwerk](https://nl.wikipedia.org/wiki/Computernetwerk). De naam TCP/IP is een samentrekking van de twee bekendste protocollen die deel uit maken van de TCP/IP-protocol*stack* (= protocol*stapel*): het [Transmission Control Protocol](https://nl.wikipedia.org/wiki/Transmission_Control_Protocol) (TCP) en het [internetprotocol](https://nl.wikipedia.org/wiki/Internetprotocol) (IP).

### 2.4.1 Geschiedenis

Het internet is een open netwerk. Op dit netwerk maakt men gebruik van het TCP/IP-protocol om gegevens uit te wisselen. TCP/IP is een pakket geschakeld protocol waarbij de gegevens in kleine pakketjes onafhankelijk van elkaar worden verzonden. De communicatiesoftware plaatst de pakketten weer in de juiste volgorde, detecteert eventuele fouten in de ontvangst om indien nodig bepaalde pakketten opnieuw te vragen totdat alle pakketten ontvangen zijn.

Deze manier van werken liet toe om bij de voorloper van internet, [ARPANET](https://nl.wikipedia.org/wiki/ARPANET), informatie in kleine pakketjes te versturen langs verschillende wegen. Zoals zo vaak ging het hier om de oplossing voor een militair probleem. In geval van een oorlog, en bij het platleggen van sommige computers in een netwerk, was het nodig dat de overige computers toch hun gegevens konden blijven uitwisselen. Was een deel van het netwerk er niet meer, dan werden de gegevens langs een andere weg naar elkaar toegestuurd. Dit maakte het netwerk minder kwetsbaar. De doelstelling van de militairen was een netwerk dat altijd bleef werken.

Toch werd na een tijd dit netwerk te licht bevonden en zijn de militairen overgestapt naar [MILnet](https://nl.wikipedia.org/w/index.php?title=MILnet&action=edit&redlink=1" \o "MILnet (de pagina bestaat niet)). Van toen af werd dit protocol tussen de verschillende universiteiten die met elkaar verbonden waren gemeengoed.

### 2.4.2 Kenmerken

Het [internet](https://nl.wikipedia.org/wiki/Internet) is een zogenaamd pakket geschakeld netwerk, zonder garantie op enige service. Een pakketje gegevens kan zonder meer verloren gaan, sterker, bij overbelasting van een bepaalde lijn wordt zelfs aangeraden pakketjes weg te gooien. Over dit onbetrouwbare netwerk wordt met behulp van het [TCP](https://nl.wikipedia.org/wiki/Transmission_Control_Protocol)-protocol een ogenschijnlijk betrouwbare dienst gelegd, waarbij TCP in de gaten houdt of pakketjes (in de juiste volgorde) aankomen, en indien niet, geen bevestiging (acknowledge) stuurt. Indien bij de zender een welbepaalde wachttijd (timeout) verstrijkt, zonder dat er een bevestiging binnen is, dan stuurt deze het pakketje opnieuw.

Vanwege deze kenmerken is TCP/IP erg geschikt voor netwerkdiensten waar geen garantie over de zekerheid en timing vereist is wanneer bepaalde data aan dient te komen. Bijvoorbeeld, bij het downloaden van een fotootje van internet, maakt het niet uit dat er door pakketverlies enige data verloren gaat, zolang dit door TCP maar gecorrigeerd wordt.

Bij een telefoongesprek gelden heel andere wensen. Hier is gewenst dat ieder pakketje exact op het juiste moment aankomt. Pakketjes dienen liefst niet weggegooid te worden, maar als dat toch gebeurt, is het zinloos om ze opnieuw te verzenden, de hapering in het geluid heeft dan al plaatsgevonden. Hiervoor kan dan weer gebruikgemaakt worden van het [UDP](https://nl.wikipedia.org/wiki/User_Datagram_Protocol)-protocol dat losse pakketjes zendt en zo onder de her-verzend-eigenschappen van TCP uitkomt. Omdat echter nog steeds geen enkele garantie bestaat over de timing en zekerheid van de aankomst van gegevens zijn bepaalde eigenschappen inherent aan het systeem.

### 2.4.3 Lagen

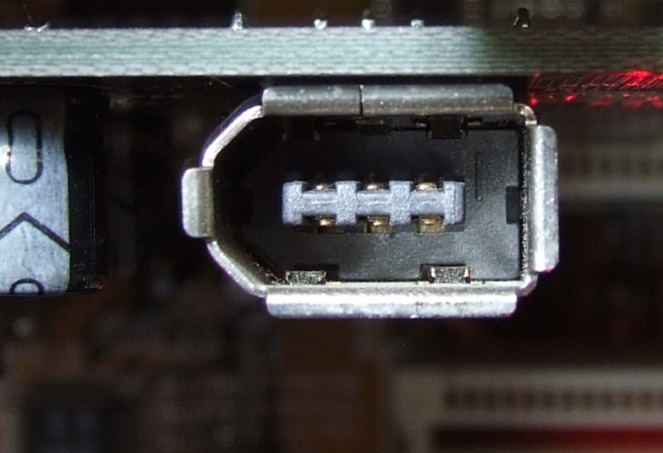
De TCP/IP-protocolstack wordt officieel onderverdeeld in vijf lagen, met elk een eigen functionaliteit. Maar dit zou ons te ver leiden.

De meest gekende toepassing van dit protocol is de netwerkstandaard **Ethernet** (IEEE802.3)

## 2.5 FireWire

**FireWire** ([**IEEE**](https://nl.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers)**1394** en **1394b**) is een seriële [computer bustechnologie](https://nl.wikipedia.org/wiki/Bus_(elektronica)) ontworpen als vervanging van [SCSI](https://nl.wikipedia.org/wiki/SCSI). FireWire heeft daarnaast een (zij het kleinere) plek veroverd in de computerwereld en consumentenelektronica naast [USB 2.0](https://nl.wikipedia.org/wiki/Universal_Serial_Bus). De FireWire is tevens bekend onder de namen IEEE 1394, IEEE 1394b. Soms wordt ook iLink (merknaam van [Sony](https://nl.wikipedia.org/wiki/Sony)) als compatibel genoemd. In sommige publicaties van Sony wordt dat ook vermeld. Het formele standpunt van Sony is echter dat een iLink alleen compatibel hoeft te zijn met andere Sony iLink-aansluitingen.

### 2.5.1 Vormen

In de praktijk komen voornamelijk 4 en 6 pins-FireWire-aansluitingen voor. De aansluitingen zijn rechthoekig. Een vierpins-FireWire-aansluiting is maar heel klein, en heeft een "deukje" op de lange zijde. Bij een zespins aansluiting is een van de twee korte kanten ongeveer een halve cirkel. Het verschil tussen vierpins en zespins is dat in het laatste geval ook voeding wordt geleverd aan het aangesloten apparaat. Er zijn verloopkabels in de handel met aan de ene kant vier en aan de andere kant zes pinnen. Dat maakt het mogelijk om apparaten die zelf geen voeding nodig hebben (dus met 4 pins) aan te sluiten aan een ander apparaat (met 6-pins-aansluiting) dat wel voeding levert.

### 2.5.2 Ontwikkeling

De standaard werd ontwikkeld door [Apple](https://nl.wikipedia.org/wiki/Apple_Computer) en werd in 1998 op de tweede generatie Apple G3-computers (Blue&White modellen) geïmplementeerd. De eerste versie was FireWire 400 en die is inmiddels geëvolueerd tot de tweede generatie: FireWire 800, ook wel aangeduid als FireWire 2. De derde generatie (Next Generation) staat reeds te wachten.

* FireWire 400 (IEEE 1394) - snelheid: 400 [Mbit](https://nl.wikipedia.org/wiki/Megabit" \o "Megabit)/s - 6 pinnetjes.
* FireWire 800 (IEEE 1394b)- snelheid: 800 Mbit/s - 9 pinnetjes.
* FireWire S3200 - snelheid: 3,2 Gbit/s.

De snelheden worden door fabrikanten aangeduid in megabits (Mbit) per seconde. Het is de gebruikelijke eenheid die gebruikt wordt bij het verplaatsen van gegevens via een [seriële](https://nl.wikipedia.org/wiki/Serieel_(informatica)) verbinding. Dezelfde aanduiding wordt ook gebruikt voor andere seriële verbindingen als [USB](https://nl.wikipedia.org/wiki/Universal_Serial_Bus), [ADSL](https://nl.wikipedia.org/wiki/ADSL) en [Ethernet](https://nl.wikipedia.org/wiki/Ethernet), zodat een vergelijking gemakkelijk is. USB en FireWire gebruiken 10 bits voor het verzenden van een byte, 8B10B-[lijncodering](https://nl.wikipedia.org/wiki/Lijncodering). De 2 "loze" bits in deze lijncodering zorgen ervoor dat er niet te veel enen of nullen achter elkaar over de transmissielijn lopen. Hierdoor blijft het signaal gebalanceerd (geen DC-component) en hoeft er geen kloksignaal meegeleverd te worden (dit spaart één geleider uit).

Hoewel USB 2.0 in theorie een hogere snelheid haalt dan FireWire 400, is FireWire in de praktijk toch sneller. Dat komt doordat USB 2.0 in de praktijk slechts snelheden haalt tot 30 MB/s (240Mbit/s). Firewire 400 haalt bijna de theoretische snelheid van 400 Mbit/s, oftewel dus bijna 50 MB/s.

[Thunderbolt](https://nl.wikipedia.org/wiki/Thunderbolt_(interface)) is een techniek die is ontwikkeld door Intel (ontwikkelaar van USB) in samenwerking met Apple (ontwikkelaar van FireWire). Het wordt algemeen gezien als de opvolger van FireWire (FireWire 3200 heeft nooit het levenslicht gezien). Thunderbolt is een combinatie van de standaarden [DisplayPort](https://nl.wikipedia.org/wiki/DisplayPort" \o "DisplayPort) en [PCI Express](https://nl.wikipedia.org/wiki/PCI_Express) over een nieuw gedefinieerde externe interface. Thunderbolt kan dus gebruikt worden om *direct* een beeldscherm, geschikt voor DisplayPort, aan te sturen.

## 2.6 xDSL

**DSL** of **Digital Subscriber Line** is een [digitale](https://nl.wikipedia.org/wiki/Digitaal) datacommunicatietechniek die een relatief hoge [datasnelheid](https://nl.wikipedia.org/wiki/Bitrate) mogelijk maakt over een [twisted-pair](https://nl.wikipedia.org/wiki/Twisted_pair" \o "Twisted pair)-koperdraadverbinding. In het algemeen wordt voor deze verbinding een normale telefoonkabel gebruikt, die van de [telefoon(wijk)centrale](https://nl.wikipedia.org/wiki/Telefooncentrale) naar de gebruiker loopt.

### 2.6.1 Varianten

DSL bestaat in twee varianten:

* Asymmetrisch ([ADSL](https://nl.wikipedia.org/wiki/Asymmetric_Digital_Subscriber_Line), [ADSL2](https://nl.wikipedia.org/wiki/ADSL2)), waar de zendsnelheid niet gelijk is aan de ontvangstsnelheid. Deze wordt vaak gebruikt voor [breedband](https://nl.wikipedia.org/wiki/Breedband)[internet](https://nl.wikipedia.org/wiki/Internet).
* Symmetrisch ([SDSL](https://nl.wikipedia.org/wiki/SDSL)), waar de zend- en ontvangstsnelheid gelijk zijn. Deze wordt behalve voor breedbandig internet ook vaak gebruikt voor bedrijfsnetwerken. In dat geval wordt een SDSL-verbinding gemaakt vanaf de bedrijfsvestigingen naar de wijkcentrales, waar dan via het [ATM](https://nl.wikipedia.org/wiki/Asynchronous_Transfer_Mode)-netwerk van een [internetprovider](https://nl.wikipedia.org/wiki/Internetprovider) speciaal voor dat bedrijf een virtueel netwerk wordt opgezet.

De nieuwere variant, [VDSL](https://nl.wikipedia.org/wiki/VDSL), kan zowel in symmetrische als in asymmetrische modus gebruikt worden, evenals de nieuwste DSL-variant, [VDSL2](https://nl.wikipedia.org/wiki/VDSL2). Deze technologie laat veel hogere doorvoersnelheden toe. Ook is de maximale afstand tot de centrale vergroot.

De term "xDSL" is de verzamelnaam voor diverse DSL-oplossingen zoals ADSL en SDSL.

### 2.6.2 Apparatuur

Aan de kant van de klant is een [DSL-modem](https://nl.wikipedia.org/wiki/Modem) nodig. Deze modem moet de juiste technologie ondersteunen die geactiveerd is op de lijn. Een [splitter](https://nl.wikipedia.org/wiki/DSL-Splitter) is in de meeste gevallen ook nodig om geen last te hebben van storingen door andere toestellen op de lijn.

Aan de kant van de provider van de lijn wordt een [DSLAM](https://nl.wikipedia.org/wiki/DSLAM) voorzien.

### 2.6.3 DSL technologieën

* [IDSL](https://nl.wikipedia.org/w/index.php?title=IDSL&action=edit&redlink=1): gebaseerd op de [ISDN](https://nl.wikipedia.org/wiki/ISDN) technologie, datasnelheid is iets groter dan tweekanaals-ISDN
* [HDSL](https://nl.wikipedia.org/w/index.php?title=HDSL&action=edit&redlink=1): de eerste DSL-technologie die gebruikmaakt van hogere frequenties op koperen twisted-pairkabels
* [HDSL2](https://nl.wikipedia.org/w/index.php?title=HDSL2&action=edit&redlink=1): een verbeterde versie van HDSL
* [ADSL](https://nl.wikipedia.org/wiki/ADSL): snelheid in de ene richting is groter dan in de andere
* [ADSL2](https://nl.wikipedia.org/wiki/ADSL2): een verbeterde versie van ADSL
* [ADSL2+](https://nl.wikipedia.org/wiki/ADSL2%2B): een versie van ADSL2 die de datasnelheid verdubbelt door het spectrum te verdubbelen
* [SDSL](https://nl.wikipedia.org/wiki/SDSL) / [SHDSL](https://nl.wikipedia.org/w/index.php?title=SHDSL&action=edit&redlink=1): een even grote snelheid voor upload en download
* [RADSL](https://nl.wikipedia.org/w/index.php?title=RADSL&action=edit&redlink=1): ontworpen om het bereik en ruistollerantie te vergroten
* [VDSL](https://nl.wikipedia.org/wiki/VDSL)
* [VDSL2](https://nl.wikipedia.org/wiki/VDSL2): een verbeterde versie van VDSL

## 2.7 Integrated Services Digital Network ([ISDN](https://nl.wikipedia.org/w/index.php?title=ISDN&redirect=no))

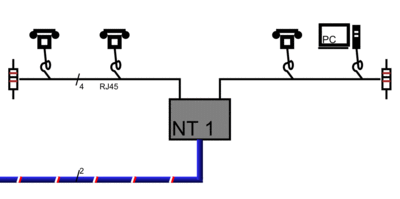
**Integrated Services Digital Network** (**ISDN**) is een vorm van [digitale](https://nl.wikipedia.org/wiki/Digitaal) [telefonie](https://nl.wikipedia.org/wiki/Telefonie). Het is de opvolger van het analoge [POTS](https://nl.wikipedia.org/wiki/POTS). Met ISDN kunnen over een koperen tweedraadsverbinding op wijkniveau meer gegevens worden getransporteerd dan doorgaans met POTS (**P**lain **O**ld **T**elephone **S**ervice) (soms ook wel foutief [PSTN](https://nl.wikipedia.org/wiki/PSTN) genoemd) mogelijk is. ISDN wordt ook wel Annex-B telefonie genoemd.

De Engelse betekenis staat grofweg voor 'dienstintegrerend digitaal netwerk'. Dat betekent dat men niet voor iedere dienst een eigen net nodig heeft maar dat het net in staat is verschillende diensten af te handelen. Over hetzelfde netwerk kunnen niet alleen telefoongesprekken maar ook video- en datadiensten ([Teletex](https://nl.wikipedia.org/wiki/Teletex" \o "Teletex), [Datex](https://nl.wikipedia.org/w/index.php?title=Datex-P&action=edit&redlink=1" \o "Datex-P (de pagina bestaat niet)), [Telefax](https://nl.wikipedia.org/wiki/Telefax), [Telemetrie](https://nl.wikipedia.org/wiki/Telemetrie), ...) gevoerd worden. Omdat ISDN in tegenstelling tot een analoge aansluiting de data digitaal over de lijn stuurt, kan de capaciteit van de leiding beter benut worden.

Een ISDN-verbinding is opgebouwd uit *kanalen*: één of meerdere B-kanalen (Bearer=drager) en één D-kanaal (Data). Het D-kanaal wordt gebruikt voor de signalering van inkomende en uitgaande oproepen (zoals het kiezen van een nummer of het laten rinkelen van een aangesloten telefoontoestel). Voor de daadwerkelijke verbinding, zoals spraak of (fax-)gegevens wordt gebruikgemaakt van de B-kanalen. ISDN-lijnen met 2 B-kanalen worden ook wel aangeduid met "2B+D". ISDN-aansluitingen met 30 B-kanalen worden ook wel aangeduid met "30B+D".

Iedere lidstaat van de [Europese Unie](https://nl.wikipedia.org/wiki/Europese_Unie) beschikt over een ISDN-telecommunicatieinfrastructuur; zo is in België en Nederland ISDN landelijk leverbaar. ISDN geniet een relatief grote populariteit in Nederland, waar ISDN zo'n 20% van de aansluitingen uitmaakt. In België is het aantal ISDN-aansluitingen bij particulieren wegens een ongunstige prijsstelling wat laag gebleven, maar is het bij zakelijke klanten wel populair, waardoor het totaal aandeel van ISDN-lijnen zo'n 17% is. Het grootste aantal ISDN-aansluitingen vindt men in Duitsland, waar ISDN ongeveer een derde van het aantal aansluitingen uitmaakt. Dit is ook zo'n een derde van het aantal aansluitingen wereldwijd.

### 2.7.1 Kenmerken

[](https://commons.wikimedia.org/wiki/File:Home_connections_ISDN.gif)

Aansluitschema. Alle ISDN-telefoontoestellen en andere apparaten zijn met korte leidingen (max. 10 m) aangesloten op de 4-aderige bus. De bus loopt door de NT1. Aan de uiteinden van de bus bevinden zich afsluitweerstanden.

### 2.7.2 Algemeen

Het belangrijkste onderscheid van ISDN ten opzichte van een analoge aansluiting is de digitale signaaloverdracht van centrale tot aan de telefoon. Hierdoor is het mogelijk over een enkele aansluiting meerdere telefoniekanalen aan te bieden. Een ISDN-2-aansluiting stelt twee kanalen ter beschikking, die volledig onafhankelijk van elkaar voor telefoongesprekken, fax of dataoverdracht gebruikt kunnen worden; men kan bijvoorbeeld tegelijk telefoneren en op internet surfen.

Zoals duidelijk is wordt deze techniek hoofdzakelijk voor telefonie of datatransport over langere afstanden gebruikt. Het is familie van xDSL.

Gedurende de tweede helft van de [jaren 1990](https://nl.wikipedia.org/wiki/1990-1999) genoot ISDN een sterke populariteit. Met ISDN kon een hogere snelheid en grotere betrouwbaarheid bereikt worden dan met een analoog modem en de snelle verbindingsopbouw maakte het aantrekkelijk de verbinding op commando te openen en te sluiten. Bovendien kon er tijdens een (soms langdurige) internetverbinding normaal getelefoneerd worden over het tweede B-kanaal. Vooral bij het versturen van grote hoeveelheden data door ontwerpafdelingen, drukkerijen e.d. was ISDN populair omdat meerdere B-kanalen te bundelen zijn tot één snellere verbinding.

Met de komst van ADSL werd ook de noodzaak van een tweede B-kanaal voor scheiding van spraak en data minder.

[VoIP](https://nl.wikipedia.org/wiki/VoIP) lijkt de technologie van de toekomst te worden die ISDN inmiddels zowel op de zakelijke markt als de consumentenmarkt begint te verdringen. Redenen hiervoor zijn dat internet goedkoop is en de prijs niet afhankelijk van de afstand is, dus erg aantrekkelijk voor de consument. Het nadeel van VoIP, gebrek aan [QoS](https://nl.wikipedia.org/wiki/QoS" \o "QoS) (mindere kwaliteit), zal door verbetering van de techniek langzaamaan te verwaarlozen zijn. Daarnaast is het een feit dat de diverse telecom- /netwerk- /internet-leveranciers zo min mogelijk netwerktechnieken willen onderhouden, omdat dit kosten bespaart. Alles over [IP](https://nl.wikipedia.org/wiki/Internetprotocol) is in principe goedkoper dan een apart netwerk voor telefonie, een apart netwerk voor [Internet](https://nl.wikipedia.org/wiki/Internet) en een apart netwerk voor [ATM](https://nl.wikipedia.org/wiki/Asynchronous_Transfer_Mode). 'All-IP' is een uitdrukking die daarbij hoort. IP als protocol was al geschikt om te werken over allerlei onderliggende netwerktechnieken; de tendens is dan ook dat steeds meer netwerk-protocollen over IP getransporteerd worden.

Tegen deze visie valt in te brengen dat de kabels waar het internetverkeer overheen gaat vaak in handen zijn van telefoonbedrijven en over dezelfde kabels vaak ook nog steeds normaal (analoog) telefoonverkeer loopt. Het prijsverschil tussen internettelefonie en klassieke telefonie is dus kunstmatig. De verwachting is dan ook dat telefoonbedrijven blijvend in staat zullen zijn hun telefoniediensten concurrerend te houden, dit over een infrastructuur die veel beter geschikt is voor telefonie dan het internet. De komst van [telefonie over ADSL](https://nl.wikipedia.org/wiki/Telefonie_over_ADSL) illustreert dit, en deze techniek is op ISDN gebaseerd en kan naar de consument zowel als analoge dienst als ISDN-dienst aangeboden worden.

ISDN is tegenwoordig dusdanig verweven met de telefooninfrastructuur dat in veel nieuwere technieken, zoals [GSM](https://nl.wikipedia.org/wiki/GSM_(communicatie)) en [UMTS](https://nl.wikipedia.org/wiki/UMTS) veel ISDN-principes zijn terug te vinden.

## 2.8 Universal Serial Bus (USB)

**Universal Serial Bus** (Universele Seriële Bus), is een standaard voor de aansluiting van [randapparatuur](https://nl.wikipedia.org/wiki/Randapparatuur) op computers.

Het vervangt de langzamere [parallelle](https://nl.wikipedia.org/wiki/Parallelle_poort) en [seriële poorten](https://nl.wikipedia.org/wiki/Seri%C3%ABle_poort), voornamelijk doordat de snelheid van [gegevensoverdracht](https://nl.wikipedia.org/wiki/Gegeven) met USB veel groter is. De standaard is vastgesteld door [Intel](https://nl.wikipedia.org/wiki/Intel) en protocolversie 1.0 werd in[1996](https://nl.wikipedia.org/wiki/1996) geïntroduceerd. Met behulp van de gestandaardiseerde USB-poort konden hardware fabrikanten producten maken die compatibel waren met zowel [pc](https://nl.wikipedia.org/wiki/Personal_computer)'s als Macs. Naast randapparatuur voor computers worden verschillende typen [microcontrollers](https://nl.wikipedia.org/wiki/Microcontroller) voorzien van een USB-poort, bijvoorbeeld om hun toepassing binnen computers en *[embedded systems](https://nl.wikipedia.org/wiki/Embedded_system" \o "Embedded system)* te vereenvoudigen.

Een bijkomend voordeel van USB is, dat deze de stroomvoorziening van de aangesloten randapparatuur kan verzorgen. Ook kan USB-apparatuur aangesloten worden zonder de computer te hoeven herstarten — dit wordt *hotplugging* genoemd.

Hoewel in de naam het woord [bus](https://nl.wikipedia.org/wiki/Bus_(elektronica)) voorkomt, is USB strikt genomen geen bus, omdat er zonder [hub](https://nl.wikipedia.org/wiki/Hub_(computernetwerk)) maar één apparaat per poort aangesloten kan worden.

[FireWire](https://nl.wikipedia.org/wiki/FireWire) is een alternatief voor USB als het gaat om het aansluiten van apparatuur die een hoge [bandbreedte](https://nl.wikipedia.org/wiki/Bandbreedte) vereist, zoals externe [*harddisks*](https://nl.wikipedia.org/wiki/Harddisk) en [videocamera](https://nl.wikipedia.org/wiki/Videocamera)'s.

### 2.8.1 Doelen

De ontwerpers van USB hadden zich een aantal doelen gesteld:

* Het moest een degelijke, goedkope poort worden die ook voor goedkope randapparatuur als muizen gebruikt kon worden.
* De kosten van de bekabeling en connectors mochten niet hoog zijn.
* De constructie moest zo zijn, dat foutieve aansluiting uitgesloten was.
* Er moesten veel apparaten tegelijk via USB aangesloten kunnen worden.
* USB moest voldoende snelheid bieden om [printers](https://nl.wikipedia.org/wiki/Printer) en andere snelle apparatuur als harde schijven aan te kunnen sluiten.

De achterliggende doelstelling is alle afzonderlijke poorten van een pc door één enkele standaard te vervangen.

### 2.8.2 Varianten

Via de USB-kabel kan het aangesloten apparaat van voedingsstroom worden voorzien. USB 2.0 levert maximaal 500 [mA](https://nl.wikipedia.org/wiki/Amp%C3%A8re_(eenheid)) (bij 5 [V](https://nl.wikipedia.org/wiki/Volt_(eenheid))) en dat is genoeg voor eenvoudige apparaten, zoals een muis. USB 3.0 en 3.1 leveren respectievelijk maximaal 900 en 2000 mA. Apparaten die meer [vermogen](https://nl.wikipedia.org/wiki/Elektrisch_vermogen) vergen, moeten een eigen voeding hebben.

Er zijn vijf versies van USB:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Snelheid** | **Naam** | **Jaar van uitkomst** | **Kleur** |
| USB 1.0 | 1,5 Mbit/s | LowSpeed | 1996 | Wit |
| USB 1.1 | 12 Mbit/s | FullSpeed | 1998 | Wit |
| USB 2.0 | 480 Mbit/s | HighSpeed | 2000 | Zwart |
| USB 3.0 | 4,8 Gbit/s | SuperSpeed | 2008 | Zwart (SS) of blauw |
| USB 3.1 | 10 Gbit/s | SuperSpeed+ | 2013 | Blauw |

Dit zijn theoretische snelheden en worden in de praktijk vaak niet gehaald.

### 2.8.3 Eigenschappen

De USB 3.x-variant heeft een stekker met extra aansluitingen om de hoge snelheid te kunnen halen. De extra aansluitingen zijn zodanig in de stekker verwerkt, dat ook oudere stekkers nog passen. De USB 3.x-kabel heeft 9 aders in plaats van 4 bij de oude kabel.

Het is ook mogelijk om een USB-stekker te combineren met een [SATA](https://nl.wikipedia.org/wiki/Serial_ATA)-aansluiting. In 2009 bestaan daartoe verschillende initiatieven.

Inmiddels bestaat ook de draadloze variant van USB, genaamd [Wireless USB](https://nl.wikipedia.org/wiki/Wireless_USB) (WUSB of USB 2.1), die een radiofrequentie gebruikt om te communiceren. WUSB is bruikbaar tot een afstand van 3 tot 10 meter, met een snelheid van 480 Mbit/s bij 3 meter tot 110 Mbit/s bij 10 meter. WUSB gebruikt [encryptie](https://nl.wikipedia.org/wiki/Encryptie).

Enkele eigenschappen van USB zijn:

* De computer is de [host](https://nl.wikipedia.org/wiki/Host).
* USB-kabels mogen maximaal 5 meter lang zijn. Deze lengte is door de tussenkomst van [hubs](https://nl.wikipedia.org/wiki/Hub_(computernetwerk)) te vergroten tot maximaal 30 meter. Voor USB-apparaten die werken volgens de USB 1.1-standaard bedraagt de maximale kabellengte 18 meter.
* USB-apparaten kunnen worden aangesloten zonder de [computer](https://nl.wikipedia.org/wiki/Computer) opnieuw te moeten opstarten en functioneren na aansluiting direct (hotpluggable/hotswappable).

### 2.8.4 Techniek

Met USB is veel meer mogelijk dan met een parallelle poort of seriële poort, terwijl er minder draden worden gebruikt. Dit wordt mogelijk gemaakt door het USB-[protocol](https://nl.wikipedia.org/wiki/Protocol).

Een USB-verbinding bestaat uit vier aders:

* +5 volt,
* nul,
* differential data (D- en D+).

De twee data-aders worden als '[twisted pair](https://nl.wikipedia.org/wiki/Twisted_pair" \o "Twisted pair)' gebruikt om [differentieel](https://nl.wikipedia.org/wiki/Differentieel_(elektronica)) data te versturen: bij een '0' wordt de [spanning](https://nl.wikipedia.org/wiki/Elektrische_spanning) op de pen voor D- hoger gemaakt dan de spanning op de pen voor D+, en voor een '1' wordt de spanning op de pin voor D- lager gemaakt dan de spanning op de pen voor D+. Voor *low speed (1,5 Mbit/s)* en *full speed (12 Mbit/s)* moet de zender zorgen voor een spanning van minstens 2,5 volt tussen de D-- en D+-pennen, terwijl voor *high speed (480 Mbit/s)* de zender moet zorgen voor een stroom van 17,8[mA](https://nl.wikipedia.org/wiki/Amp%C3%A8re_(eenheid)).

Deze [bus](https://nl.wikipedia.org/wiki/Bus_(elektronica)) wordt gebruikt om datapakketten over te sturen, niet alleen voor de daadwerkelijke dataoverdracht, maar ook voor besturingsinformatie. De host is de baas over de bus en neemt het initiatief voor alle dataoverdracht.

## 2.9 Local area network

Een **Local Area Network** (lokaal gebiedsnetwerk), afgekort **LAN**, is een netwerk dat computers en andere toestellen die zich in een lokaal beperkt gebied bevinden, met elkaar verbindt zodanig dat deze met elkaar kunnen communiceren. Toestellen kunnen hierbij fysiek via een gedeeld medium of rechtstreeks met elkaar verbonden zijn. LAN's verschillen van [WAN](https://nl.wikipedia.org/wiki/Wide_area_network" \o "Wide area network)'s door het lokale karakter en doordat er meestal geen lijnen van telecomaanbieders deel van uitmaken. LAN's vindt men typisch bij lokale afdelingen van organisaties, alsook bij particulieren.

In het verleden werden allerlei technologieën gebruikt, zoals ARCNET en [Token Ring](https://nl.wikipedia.org/wiki/Token_Ring). Vandaag de dag worden LAN's vooral gerealiseerd op basis van bekabeld [Ethernet](https://nl.wikipedia.org/wiki/Ethernet) en [wifi](https://nl.wikipedia.org/wiki/IEEE_802.11) en met name in de particuliere sfeer ook met [Homeplug](https://nl.wikipedia.org/wiki/Homeplug). LAN's zijn meestal met een WAN verbonden via een [router](https://nl.wikipedia.org/wiki/Router), [modem](https://nl.wikipedia.org/wiki/Modem) of andere "gateway".

### 2.9.1 Toepassingen

LAN's worden vaak opgezet op locaties waar veel[**computers**](https://nl.wikipedia.org/wiki/Computer)in één ruimte of[**gebouw**](https://nl.wikipedia.org/wiki/Gebouw)te vinden zijn en waar een snelle overdracht van informatie tussen verschillende computers nodig is. Dit is vaak het geval bij[**bedrijven**](https://nl.wikipedia.org/wiki/Bedrijf),[**scholen**](https://nl.wikipedia.org/wiki/Schoolgebouw)en overheidsinstellingen. Tegenwoordig beschikken ook vele particulieren over een LAN. Via het LAN heeft een computer toegang tot andere bronnen die aan het netwerk zijn gekoppeld, zoals andere computers, printers en eventueel andere netwerken. Door de digitale convergentie dienen LAN's vandaag de dag niet alleen voor typische computercommunicatie, maar meer en meer ook voor audio- en videotoepassingen, waaronder digitale televisie en**[voice over IP](https://nl.wikipedia.org/wiki/Voice_over_IP" \o "Voice over IP)**.

### 2.9.2 Techniek

Er bestaan verschillende manieren om verbindingen te leggen. De meest gebruikte technieken zijn bekabelde basisbandverbindingen, zoals [Ethernet](https://nl.wikipedia.org/wiki/Ethernet) via [UTP](https://nl.wikipedia.org/wiki/Twisted_pair) en draadloze verbindingen via [wifi](https://nl.wikipedia.org/wiki/IEEE_802.11). Ook maakt men wel gebruik van [communicatie via het elektriciteitsnet](https://nl.wikipedia.org/wiki/Power_line_communication) of modulatie op bestaande [coax](https://nl.wikipedia.org/wiki/Coax) voor televisie. Een LAN wordt beperkt tot een lokaal gebied, gewoonlijk binnen één gebouw of complex, zoals bijvoorbeeld een bedrijfsterrein. Over het algemeen wordt het bereik van een LAN beperkt door de gebruikte technieken. Indien grotere afstanden overbrugd moeten worden, zoals tussen steden en landen, spreekt men van een [WAN](https://nl.wikipedia.org/wiki/Wide_area_network).

LAN's zijn meestal van het type [*basisband*](https://nl.wikipedia.org/wiki/Basisband) waarbij gebruikgemaakt wordt van *[packet-switching](https://nl.wikipedia.org/wiki/Packet-switching" \o "Packet-switching)*. Twee typen LANs zijn algemeen in gebruik: [*Ethernet*](https://nl.wikipedia.org/wiki/Ethernet) en in mindere mate [Token Ring](https://nl.wikipedia.org/wiki/Token_Ring).

## 2.10 CAN bus

Het *Controller Area Network* (CAN) is een standaard voor een [seriële](https://nl.wikipedia.org/wiki/Serieel_(informatica)) [databus](https://nl.wikipedia.org/wiki/Databus_(elektronica)), die oorspronkelijk is ontwikkeld door [Robert Bosch GmbH](https://nl.wikipedia.org/wiki/Bosch_(bedrijf)), vanaf 1983 tot 1986, om [elektronische](https://nl.wikipedia.org/wiki/Elektronica) [sturingseenheden](https://nl.wikipedia.org/w/index.php?title=Sturing&action=edit&redlink=1) in voertuigen aan elkaar te koppelen.

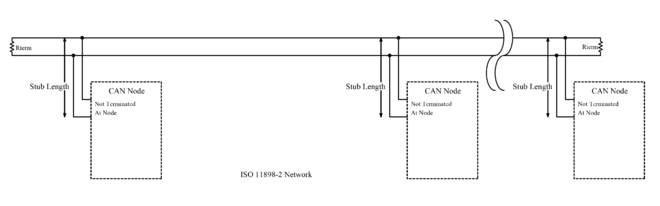
CAN is expliciet ontworpen voor omgevingen met veel [elektromagnetische](https://nl.wikipedia.org/wiki/Elektromagnetisme) storingen en maakt gebruik van twee [differentieel](https://nl.wikipedia.org/wiki/Differentieel_(elektronica)) aangedreven lijnen; de betrouwbaarheid van de signaaloverdracht kan verder worden verhoogd door het gebruik van *[twisted pair](https://nl.wikipedia.org/wiki/Twisted_pair" \o "Twisted pair)*-verbindingen.

De eerste markt voor CAN was de automobielsector. Het systeem werd voor het eerst gebruikt in de Mercedes S-klasse in 1990, maar ondertussen is CAN ook doorgedrongen in andere *[embedded](https://nl.wikipedia.org/wiki/Ingebed_systeem" \o "Ingebed systeem)* toepassingen, zoals machinesturingen en [robots](https://nl.wikipedia.org/wiki/Robot).

[Gegevensoverdracht](https://nl.wikipedia.org/wiki/Gegevensoverdracht) tot 1 [Mbit/s](https://nl.wikipedia.org/wiki/Megabit_per_seconde" \o "Megabit per seconde) (één miljoen bits per seconde) is mogelijk voor een kabellengte onder de 40 meter. Langere netwerken zijn mogelijk als de maximum bit snelheid wordt aangepast; bijvoorbeeld, tot 250 kbit/s (250 duizend bits per seconde) voor een lengte van 250 meter.

Een CAN-bus maakt *[realtime](https://nl.wikipedia.org/wiki/Realtime" \o "Realtime)* communicatie mogelijk: iedere [node](https://nl.wikipedia.org/wiki/Node_(netwerk)) van het CAN netwerk heeft een vaste prioriteit en de boodschap van de node met de hoogste prioriteit krijgt voorrang.

Nieuwere standaarden van netwerkprotocollen voor gebruik in voertuigen zijn [*Media Oriented Systems Transport*](https://nl.wikipedia.org/w/index.php?title=Media_Oriented_Systems_Transport&action=edit&redlink=1) (MOST) en [FlexRay](https://nl.wikipedia.org/wiki/FlexRay" \o "FlexRay).



## 2.11 Draadloos netwerk

Een **draadloos netwerk** is een [computernetwerk](https://nl.wikipedia.org/wiki/Computernetwerk) of [telefoonnetwerk](https://nl.wikipedia.org/wiki/Telefonie) waarbij de aangesloten apparaten niet via fysieke koperen kabels of glasvezelkabels communiceren, maar via [elektromagnetische straling](https://nl.wikipedia.org/wiki/Elektromagnetische_straling) ([radiosignalen](https://nl.wikipedia.org/wiki/Radio), [licht](https://nl.wikipedia.org/wiki/Licht)).

De belangrijkste draadloze technologieën zijn:

Lokale netwerken:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Netwerk** | **gebruik** | **protocol** | **snelheid** | **afstand** |
| [IrDA](https://nl.wikipedia.org/wiki/IrDA) | communicatie met randapparatuur |  | 9,6 [kbit](https://nl.wikipedia.org/wiki/Kilobit" \o "Kilobit)/s tot 16 [Mbit](https://nl.wikipedia.org/wiki/Megabit" \o "Megabit)/s | 1 m. |
| [Bluetooth](https://nl.wikipedia.org/wiki/Bluetooth) | communicatie met randapparatuur |  | 1 [Mbit](https://nl.wikipedia.org/wiki/Megabit" \o "Megabit)/s | 1-100 m. |
| [Wifi](https://nl.wikipedia.org/wiki/Wifi) | lokale netwerken | [IEEE 802.11](https://nl.wikipedia.org/wiki/IEEE_802.11) | 11 [Mbit](https://nl.wikipedia.org/wiki/Megabit" \o "Megabit)/s - 866,7 [Mbit](https://nl.wikipedia.org/wiki/Megabit" \o "Megabit)/s. | 1 - 100 m. |

Netwerken voor [mobiel internet](https://nl.wikipedia.org/wiki/Mobiel_internet):

|  |  |  |  |
| --- | --- | --- | --- |
| **Netwerk** | **gebruik** | **protocol** | **snelheid** |
| [GPRS](https://nl.wikipedia.org/wiki/GPRS) / [EDGE](https://nl.wikipedia.org/wiki/EDGE) | mobiel internet | [GSM](https://nl.wikipedia.org/wiki/GSM_(communicatie)) | 9-21,4 [kbit](https://nl.wikipedia.org/wiki/Kilobit" \o "Kilobit)/s / 128 [kbit](https://nl.wikipedia.org/wiki/Kilobit" \o "Kilobit)/s |
| [UMTS](https://nl.wikipedia.org/wiki/UMTS) / [HSDPA](https://nl.wikipedia.org/wiki/HSDPA) | mobiel internet | [UMTS](https://nl.wikipedia.org/wiki/UMTS) | 384 [kbit](https://nl.wikipedia.org/wiki/Kilobit" \o "Kilobit)/s / 1.8 - 14.4 [Mbit](https://nl.wikipedia.org/wiki/Megabit" \o "Megabit)/s |
| [HSPDA+](https://nl.wikipedia.org/w/index.php?title=HSPDA%2B&action=edit&redlink=1) / [4G](https://nl.wikipedia.org/wiki/4G) | mobiel internet | [UMTS](https://nl.wikipedia.org/wiki/UMTS) | 22-84 [Mbit](https://nl.wikipedia.org/wiki/Megabit" \o "Megabit)/s / 10,3-299,6 [Mbit](https://nl.wikipedia.org/wiki/Megabit" \o "Megabit)/s |

## [https://upload.wikimedia.org/wikipedia/commons/thumb/1/11/PCMCIA-card-750px.jpg/220px-PCMCIA-card-750px.jpg](https://commons.wikimedia.org/wiki/File:PCMCIA-card-750px.jpg)2.12 Wireless LAN

Wireless LAN (afgekort WLAN) is een draadloos [Local Area Network](https://nl.wikipedia.org/wiki/Local_Area_Network" \o "Local Area Network) dat vaak ook toegang geeft tot [internet](https://nl.wikipedia.org/wiki/Internet), meestal gebaseerd op [802.11](https://nl.wikipedia.org/wiki/IEEE_802.11)-protocollen.

Hiervoor zijn meerdere apparaten nodig. Via een apparaat met een draadloze adapter koppel je je aan een zogenaamd [access point](https://nl.wikipedia.org/wiki/Access_point), een andere machine die signalen uitzendt. Heel wat commerciële access-points bevatten ook een [router](https://nl.wikipedia.org/wiki/Router), [switch](https://nl.wikipedia.org/wiki/Switch_(hardware)) en/of [modem](https://nl.wikipedia.org/wiki/Modem). Vandaar dat er ook gesproken wordt van een draadloze router of draadloze modem. Het access point werkt als een draadloze [hub](https://nl.wikipedia.org/wiki/Hub_(computernetwerk)) en is vaak weer aangesloten op een bekabeld netwerk. Dat netwerk is meestal via een [modem](https://nl.wikipedia.org/wiki/Modem), soms via een modem met [routerfunctionaliteit](https://nl.wikipedia.org/wiki/Router) met het internet verbonden. Een router verbindt computers, wanneer deze niet rechtstreeks aan elkaar gekoppeld zijn, op een indirecte wijze. Wanneer deze router tevens signalen via de kabel of telefoonlijn kan coderen en decoderen, beter gezegd moduleren en demoduleren, dan heeft deze ook de functionaliteit van een modem. Dikwijls wordt dan gezegd dat de router het netwerk verbindt met het internet terwijl juist het modemgedeelte van het apparaat dit doet. Bij bijvoorbeeld 'ethernet to the home' (ETTH) is het mogelijk dat de router de verbindende schakel vormt, echter niet veel mensen hebben dit.

De 802.11-standaarden zelf bieden in principe geen encryptie in hun protocol, zodat alle informatie onversleuteld en direct leesbaar door de lucht reist. Toch kun je nog op verscheidene manieren versleuteling gebruiken:

* [WEP](https://nl.wikipedia.org/wiki/Wired_Equivalent_Privacy) (wordt niet langer veilig geacht. Door het verzamelen van veel berichten kan de afluisteraar de 'key' binnen een minuut reconstrueren)
* [WPA](https://nl.wikipedia.org/wiki/Wi-Fi_Protected_Access),
* [WPA2](https://nl.wikipedia.org/wiki/Wi-Fi_Protected_Access).

WPA en WPA2 worden vooralsnog veilig geacht. Net als bij WEP wordt er gewerkt met een 'key', maar deze wordt regelmatig automatisch 'vernieuwd' (renewal).

Wireless LAN is vooral onder de term [wifi](https://nl.wikipedia.org/wiki/Wifi) bekend geworden. Een ander soort Wireless LAN-versie voor middelgroot publiek bereik is [WiMAX](https://nl.wikipedia.org/wiki/WiMAX" \o "WiMAX); dit is in tegenstelling tot Wireless LAN geschikt voor openbaar gebruik in plaats van lokaal.

## 2.13 Bluetooth

**Bluetooth** is een [open standaard](https://nl.wikipedia.org/wiki/Open_standaard) voor [draadloze](https://nl.wikipedia.org/wiki/Draadloos_netwerk) verbindingen tussen apparaten op korte afstand. Dankzij bluetooth kunnen bijvoorbeeld adresgegevens tussen [mobiele telefoons](https://nl.wikipedia.org/wiki/Mobiele_telefoon) worden uitgewisseld, kan snel vanaf een [handheld computer](https://nl.wikipedia.org/wiki/Handheld_computer) worden geprint, of kan een mobiele telefoon worden uitgerust met een draadloze *headset*. De techniek is ontwikkeld door het [Zweedse](https://nl.wikipedia.org/wiki/Zweden) [Ericsson](https://nl.wikipedia.org/wiki/Ericsson).

### 2.13.1 Geschiedenis

[](https://commons.wikimedia.org/wiki/File:Bluetooth_logo_on_mouse_from_aside.jpg)De geschiedenis van bluetooth begint in [1994](https://nl.wikipedia.org/wiki/1994), toen Ericsson zocht naar een goedkope manier om via een [radioverbinding](https://nl.wikipedia.org/wiki/Radio) [communicatie](https://nl.wikipedia.org/wiki/Communicatie) tot stand te brengen tussen mobiele telefoons en andere apparaten. Men had zich ten doel gesteld om allerlei kabels tussen mobiele telefoons en pc-cards, koptelefoons, desktopapparaten et cetera overbodig te maken. Naarmate het onderzoek vorderde, werd het de onderzoekers duidelijk dat de toepassingsmogelijkheden voor een dergelijke korte-afstandsradioverbinding legio waren.

### 2.13.2 De techniek

Bluetooth is een radioverbinding (in de 2,4GHz-band, dit is in het frequentiegebied van [UHF](https://nl.wikipedia.org/wiki/UHF_(radiospectrum))) voor spraak en data op korte afstand. Het werkt '[point to multipoint](https://nl.wikipedia.org/w/index.php?title=Point_to_multipoint&action=edit&redlink=1)', hetgeen inhoudt dat een enkele bron meer 'ontvangers' kan bedienen. Wanneer twee bluetooth apparaten een verbinding hebben opgebouwd, dan ontstaat een zogenoemd [piconet](https://nl.wikipedia.org/wiki/Piconet" \o "Piconet). Er kunnen op dezelfde plek meerdere van dergelijke piconets naast elkaar bestaan, in wat men een [scatternet](https://nl.wikipedia.org/wiki/Scatternet" \o "Scatternet) noemt. Binnen een piconet ondersteunt bluetooth maximaal acht actieve verschillende apparaten, terwijl er in totaal 127 apparaten een verbinding kunnen houden (deze zijn tijdelijk 'geparkeerd').

Normaal gesproken zal het binnen een straal van 1 tot 10 meter functioneren, maar wanneer het zendvermogen wordt opgevoerd, kan de 100 meter worden gehaald. Een zogenoemde 'zichtverbinding' (elkaar kunnen zien) is niet nodig; dankzij de GHz-radioverbinding dringt het bluetooth signaal ook door vaste materialen (zolang het geen metaal is).

De communicatie van digitale spraak behoort tot de standaardmogelijkheden van bluetooth. Bluetooth ondersteunt binnen een piconet tot drie gelijktijdige [full-duplex](https://nl.wikipedia.org/wiki/Full-duplex)-gesprekken.

Omdat bluetooth een vervanger is voor de (korte) kabels, kan het worden gebruikt om allerlei apparaten met elkaar te laten communiceren. De ontwerpers hebben met opzet gebruikgemaakt van een goedkope radiotechniek, zodat bluetooth zonder veel bezwaar in ieder apparaat kan worden ingebouwd. Omdat bluetooth normaal gesproken ook weinig stroom verbruikt (30 [microampère](https://nl.wikipedia.org/wiki/Amp%C3%A8re_(eenheid)) in 'hold mode' en 8-30 milliampère bij een actieve verbinding), kan het ook worden toegepast in mobiele apparaten die afhankelijk zijn van batterijen.

### 2.13.3 Toepassingen

Belangrijke toepassingen zijn het verzenden van bestanden tussen apparaten zoals computers en mobiele telefoons, het zenden van een document of afbeelding van een computer naar een printer, het zenden van toetsaanslagen van een toetsenbord naar een computer, het zenden van een afbeelding van een scanner naar een computer, het zenden van geluid naar een draadloze koptelefoon enzovoort. Tevens wordt bluetooth gebruikt om verkeersinformatie mee in te winnen door middel van het [bluetooth-meetsysteem](https://nl.wikipedia.org/wiki/Bluetooth-meetsysteem).

### 2.13.4 Beveiliging

Omdat de radiosignalen kunnen worden opgevangen door alle ontvangers die zich in de buurt van de bluetooth apparaten bevinden, ondersteunt bluetooth in het basisprotocol [authenticatie](https://nl.wikipedia.org/wiki/Authenticatie) en [encryptie](https://nl.wikipedia.org/wiki/Encryptie). Authenticatie vindt plaats middels een geheime sleutel, die zich op beide apparaten moet bevinden. Het protocol staat het wel toe dat het ene apparaat het andere authenticeert. Na authenticatie is het mogelijk om de verbinding te versleutelen (encryptie).

Als het bluetooth apparaat niet voldoende beveiligd wordt, kan door middel van [bluejacking](https://nl.wikipedia.org/wiki/Bluejacking" \o "Bluejacking) informatie verzonden worden naar het apparaat. Het ongevraagd en dus illegaal lezen van de documenten via bluetooth wordt dan [bluesnarfing](https://nl.wikipedia.org/wiki/Bluesnarfing" \o "Bluesnarfing) genoemd. Verder kan een apparaat onbruikbaar worden gemaakt door middel van [bluesmacking](https://nl.wikipedia.org/w/index.php?title=Bluesmacking&action=edit&redlink=1" \o "Bluesmacking (de pagina bestaat niet)). Dit is een [denial-of-service](https://nl.wikipedia.org/wiki/Denial-of-service" \o "Denial-of-service) aanval middels bluetooth. [Bluesniffing](https://nl.wikipedia.org/w/index.php?title=Bluesniffing&action=edit&redlink=1" \o "Bluesniffing (de pagina bestaat niet)) is het afluisteren van bluetooth-verkeer.

## 2.14 IrDA

Bekend van de afstandsbediening van de [tv](https://nl.wikipedia.org/wiki/Televisie), zien we de **infrarode verbinding** (IrDA) ook bij de [pc](https://nl.wikipedia.org/wiki/Personal_computer)'s. Vooral draagbare pc's (laptops) worden vaak met infrarode poorten uitgerust. Het grote voordeel van een infrarode verbinding is dat er geen kabel nodig is. Twee apparaten hoeven elkaar alleen maar te 'zien' om te kunnen communiceren. Maar wat een voordeel is, kan ook een nadeel zijn; soms kan de verbinding wegvallen omdat er een argeloze hand of een boek tussen de apparaten wordt geschoven.

De infrarode poort is gebaseerd op een standaard die is vastgesteld door de Infrared Data Association (IrDA), een groep van meer dan 150 bedrijven.

### 2.14.1 Karakteristieken

**'point-to-point'** - Een verbinding vindt altijd één op één plaats. Meer dan twee apparaten kunnen niet gelijktijdig communiceren.

**afstand** - Gebruiksafstand is normaal gesproken nul tot één meter. Via versterkers overbruggen we grotere afstanden (zetel => TV)

**richtingsgevoelig** - Om storingen te voorkomen is de lichtbundel gericht, met een stralingshoek van 15 graden.

**afhankelijkheid** - In de verbinding is er sprake van een 'master-slave' afhankelijkheid (in de officiële IrDA-termen 'primary' en 'secondary'). Wanneer er een verbinding tot stand is gebracht is het niet echt van belang welke van de twee welke rol vervult; ieder apparaat kan een zend-opdracht starten.

**snelheid** - Afhankelijk van de kwaliteit van de verbinding en van de toegepaste techniek, kan de snelheid van een IrDA-verbinding 9600 b/s tot 4 Mb/s zijn. De allernieuwste apparaten kunnen zelfs een snelheid tot 16 Mb/s halen.

**spraak** - Er bestaat ook een versie van Infrarood waarbij een 'spraak'-verbinding kan plaatsvinden. De verbinding is hierbij '[full-duplex](https://nl.wikipedia.org/wiki/Full-duplex)', wat betekent dat de verbinding tegelijkertijd twee kanten op werkt, en de benodigde bandbreedte is 115,2 kb/s. Hierdoor kan er geen andere gegevensuitwisseling plaatsvinden tijdens een gesprek. Dit werd toegepast bij een mobiele telefoon in een 'hands-free' kit voor in de auto in de beginjaren.

### 2.14.2 Bluetooth versus IrDA

Bluetooth is net als de infrarode verbinding ([IrDA](https://nl.wikipedia.org/wiki/IrDA" \o "IrDA)), een communicatiemiddel voor de korte afstand. Beide verbindingsmogelijkheden concurreren dus met elkaar. Met name bij het uitwisselen van data, zoals het 'synchroniseren' van een handheld computer met een pc, mikken de beide technieken ook op dezelfde functionaliteit. Zij maken hiervoor zelfs gebruik van hetzelfde 'upper layer' [protocol](https://nl.wikipedia.org/wiki/Protocol) ([OBEX](https://nl.wikipedia.org/wiki/OBEX)) en beide streven ernaar om gebruik te kunnen maken van dezelfde [applicatie](https://nl.wikipedia.org/wiki/Applicatie).

Toch hebben bluetooth en IrDA specifieke eigenschappen, waardoor zij in verschillende situaties de voorkeur verdienen. In een ruimte met veel apparaten op de bluetooth-frequentie (veel mobiele telefoons, bijvoorbeeld), is het eenvoudiger om gegevens uit te wisselen via IrDA; het is dan mogelijk om beide apparaten op elkaar te 'richten', zonder dat andere tussenbeide kunnen komen. Met bluetooth is het wat lastig 'mikken' en daardoor duurt het even voordat bluetooth alle soortgenoten in de buurt heeft ontdekt. Vervolgens kan er nog tijd overheen gaan, voordat uit de naburige apparaten het juiste is geïdentificeerd, waarvoor extra informatie nodig kan zijn. Ook het beveiligingsmechanisme in bluetooth vraagt tijd.

In andere gevallen verdient bluetooth weer de voorkeur. Zo kan met mobiele apparatuur worden gecommuniceerd, zonder dat deze tevoorschijn hoeft te worden gehaald; de mobiele telefoon kan in de tas blijven tijdens het synchroniseren. Bovendien mag, in tegenstelling tot bij IrDA, een apparaat worden bewogen tijdens de communicatie, waardoor het apparaat ook klaar is om te ontvangen wanneer het 'op het lichaam' wordt gedragen. Hierdoor kan de gebruiker van een mobiele telefoon met bluetooth zijn telefoon gewoon in zijn zak laten zitten wanneer hij via een [laptop](https://nl.wikipedia.org/wiki/Laptop) een 'dial up'-verbinding met het internet maakt. De telefoon hoeft niet, zoals bij infrarood, naast de laptop te liggen. Bluetooth kan ook grotere afstanden overbruggen (ongeveer 15 tot 20 meter) terwijl IrDA (infrarood) al na enkele meters geen goede verbinding meer kan maken. Het verbinden met bluetooth is erg makkelijk omdat je bij de meeste bluetooth apparaten een lijst kan opvragen via je pda, mobiele telefoon of laptop welke andere bluetooth apparaten er in de buurt zijn, vervolgens kun je ze makkelijk koppelen. Dankzij het 'multi-point'-karakter van bluetooth is het ook mogelijk om meerdere van bluetooth voorziene apparaten, via een enkel LAN Access Point in een ruimte, toegang te geven tot een (bekabeld) netwerk. Hier kan echter wel de beperkte snelheid van bluetooth een rol spelen. Bluetooth kan maar communiceren met 1 Mb/s (bij IrDA is dat tot 4 Mb/s, respectievelijk 16 Mb/s voor modernere varianten).

Verder is bluetooth niet merkgebonden wat als voordeel heeft dat men bijvoorbeeld in een auto met een bluetooth-[car-kit](https://nl.wikipedia.org/w/index.php?title=Car-kit&action=edit&redlink=1" \o "Car-kit (de pagina bestaat niet)) kan aanmelden met elke mobiele telefoon uitgerust met dit systeem. Hoewel niet elk bluetooth apparaat compatibel is met elk ander bluetooth apparaat. Zo moet het apparaat dat aan bijvoorbeeld een car-kit wordt gekoppeld beschikken over het handsfree profiel. Daarnaast hoeft dan ook niet elke functie te werken met elk toestel. De fabrikanten van de apparaten hebben hier meer informatie over.

Bluetooth concurreert niet met het draadloze LAN 802.11 ([wifi](https://nl.wikipedia.org/wiki/Wifi)). Bluetooth biedt een lager bereik en een lagere bandbreedte, maar is veel goedkoper en energiezuiniger en daardoor beter op grote schaal toe te passen in (mobiele) apparatuur.

## 2.15 ZigBee

**ZigBee** is een [open standaard](https://nl.wikipedia.org/wiki/Open_standaard) voor draadloze verbindingen tussen apparaten op korte afstand. Het is bedoeld als aanvulling op [Bluetooth](https://nl.wikipedia.org/wiki/Bluetooth) en [wifi](https://nl.wikipedia.org/wiki/Wifi), het wordt gebruikt voor het doorsturen van sensorgegevens en voor (proces)besturing (monitoring & control), zoals de gezondheid van een patiënt of de veiligheid in uw huis controleren met behulp van sensoren.

### 2.15.1 Algemeen

ZigBee is de naam voor een standaard voor draadloze [communicatie](https://nl.wikipedia.org/wiki/Communicatie) die ontworpen is vooral voor toepassingen in de industrie. ZigBee gaat bijvoorbeeld van afstandsbedieningen tot de [communicatie](https://nl.wikipedia.org/wiki/Communicatie) tussen machines in een fabriek.

Praktisch voorbeeld van een thuissituatie met ZigBee:

* ZigBee Lamp controller: het licht bedienen op afstand
* Draagbare Panic button: mensen met een slechte gezondheid kunnen met een simpele druk op de knop de hulpdiensten verwittigen via de telefoonlijn
* Deur en raam beveiliging
* ZigBee Mailbox detector: detecteert of er post is geleverd in de brievenbus, handig tegen diefstal
* Computer met ZigBee Human Interface devices: toestellen met software waarmee je het huis kunt automatiseren
* Het huis is geautomatiseerd: Het licht kan op afstand aangestoken worden, er is inbraakbeveiliging (bij inbraak wordt de politie ingelicht en gaat het licht aan), een panic button voor noodgevallen met de gezondheid en detectie van post. Alles wordt gelokaliseerd en geconfigureerd door de PAN coördinator. Dus de coördinator alarmeert de politie en de hulpdiensten.

ZigBee vindt zijn oorsprong in de [IEEE](https://nl.wikipedia.org/wiki/IEEE)-norm 802.15.4. De [IEEE](https://nl.wikipedia.org/wiki/IEEE) 802.15.4 voorziet 3 frequentiebanden waarin ZigBee kan werken: 868,3 MHz ([Europa](https://nl.wikipedia.org/wiki/Europa_(werelddeel))), 902-928 MHz ([Amerika](https://nl.wikipedia.org/wiki/Amerika_(continent))) en 2405-2480 MHz (wereldwijd). De transmissiesnelheid bedraagt maximaal 250 kbps met een bereik van 100 meter en ondersteunt een [netwerk](https://nl.wikipedia.org/wiki/Netwerk_(algemeen)) tot 65.000 apparaten.

ZigBee is een product van de ZigBee Alliance. De ZigBee alliantie is een associatie van bedrijven die samenwerken om (monitoring & control) producten aan te bieden gebaseerd op ZigBee. Deze producten hebben bepaalde eigenschappen: betrouwbaar, laag stroomverbruik, draadloos netwerk, goede prijs/kwaliteit. De alliantie heeft een aantal bekende promotors zoals [Motorola](https://nl.wikipedia.org/wiki/Motorola), [Philips](https://nl.wikipedia.org/wiki/Koninklijke_Philips_Electronics_N.V.), [Samsung](https://nl.wikipedia.org/wiki/Samsung_Group), [Siemens](https://nl.wikipedia.org/wiki/Siemens_AG)…

### 2.15.2 Netwerkcomponenten

Een ZigBee netwerk wordt een **PAN** ([Personal Area Network](https://nl.wikipedia.org/wiki/Personal_Area_Network)) genoemd en bestaat uit 1 coördinator, 1 of meerdere eindtoestellen en 1 of meerdere routers. Dus er zijn 3 verschillende ZigBeetoestellen:

**ZigBee coördinator** (ZC): de coördinator vormt de wortel van de netwerkvertakking. Er is 1 ZigBee coördinator per netwerk en is verantwoordelijk voor de interne werking van het netwerk. De coördinator zet een netwerk op met een gegeven PAN-identifier.

**ZigBee Router** (ZR): de router scant naar een netwerk om lid van te worden. Het kan ook gebruikt worden voor de coördinatie in het netwerk

**ZigBee End Device** (ZED): een End Device moet berichten ontvangen en verzenden op de [netwerklaag](https://nl.wikipedia.org/wiki/Netwerklaag" \o "Netwerklaag).

## 2.16 WIFI

Wi-Fi is een certificatielabel ('logo') voor producten voor [draadloze datanetwerken](https://nl.wikipedia.org/wiki/Draadloos_netwerk), die werken volgens de internationale standaard [IEEE 802.11](https://nl.wikipedia.org/wiki/IEEE_802.11) (*draadloos*[*ethernet*](https://nl.wikipedia.org/wiki/Ethernet) of *wifi*). Producten die volgens deze standaard werken maken gebruik van radiofrequenties in de 2,4GHz- en/of 5,0GHz-band die onder voorwaarden zonder licentie gebruikt mogen worden. De eisen voor dit logo worden vastgelegd door de [Wi-Fi Alliance](https://nl.wikipedia.org/w/index.php?title=Wi-Fi_Alliance&action=edit&redlink=1). Een product komt in aanmerking voor het Wi-Fi-logo als door een onafhankelijk certificatiebureau is aangetoond dat aan bepaalde functionaliteits-, prestatie- en interoperabiliteitseisen is voldaan. Met name het laatste is van belang voor de consument, omdat dit garandeert dat producten met het Wi-Fi-logo samenwerken met producten van andere fabrikanten.

### 2.16.1 Topologieën

Wi-Fi definieert twee verschillende [topologieën](https://nl.wikipedia.org/wiki/Topologie" \o "Topologie): [ad hoc](https://nl.wikipedia.org/wiki/Ad_hoc) en infrastructuur. In ad-hocmodus communiceert een 802.11-client direct met een andere client. De maximale afstand tussen deze stations is daarmee automatisch begrensd tot het bereik van de beide zenders/ontvangers (afhankelijk van vele factoren, echter meestal maximaal zo'n 30 meter). In infrastructuurmodus wordt gewerkt met basisstations, in 802.11-termen [access point](https://nl.wikipedia.org/wiki/Wi-Fi_Access_Point)genoemd. De basisstations zijn onderling verbonden door een [ethernet](https://nl.wikipedia.org/wiki/Ethernet)-infrastructuur. Mobiele stations kunnen overschakelen van het ene naar het andere access point ('roamen'), zonder de verbinding met het netwerk te verliezen (vergelijk [GSM](https://nl.wikipedia.org/wiki/GSM_(communicatie))).

De bandbreedte en het bereik van wifi zijn groter dan die van [bluetooth](https://nl.wikipedia.org/wiki/Bluetooth). Om deze redenen is wifi een van de belangrijkste toegangsmethoden voor een alom aanwezig draadloos [internet](https://nl.wikipedia.org/wiki/Internet). Een keerzijde van wifi, met name vergeleken met Bluetooth, is het [relatief](https://nl.wikipedia.org/wiki/Relatief) hoge [energieverbruik](https://nl.wikipedia.org/wiki/Energie). Dit is bij kleine apparaten met een beperkte [batterijcapaciteit](https://nl.wikipedia.org/wiki/Batterij_(techniek)), zoals [pda](https://nl.wikipedia.org/wiki/Personal_Digital_Assistant)'s, een probleem.

### 2.16.2 Versleuteling

Een belangrijk aandachtspunt bij wifinetwerken is de beveiliging van de door de ether verzonden informatie. Een wifiverbinding kan door middel van verschillende technieken worden versleuteld. De twee prominente standaarden zijn [WEP](https://nl.wikipedia.org/wiki/Wired_Equivalent_Privacy) en [WPA](https://nl.wikipedia.org/wiki/Wi-Fi_Protected_Access). De WPA-standaard is in juni 2004 gestandaardiseerd als [IEEE](https://nl.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers) 802.11i, en WPA2, een verbetering op WPA, is sinds 2006 wijd in gebruik en vereist voor apparatuur met Wi-Fi-certificatie. WEP-beveiliging blijkt in de praktijk makkelijk te kraken; WPA of WPA2 worden daarom aanbevolen. WPA is slechts met zeer veel moeite te kraken, en WPA2 niet of nauwelijks.

#### 2.16.2.1 Wi-Fi Protected Setup (WPS)

WPS is bedacht om de draadloze verbinding te kunnen configureren zonder ingewikkelde sleutels (WEP key of WPA keys) in te hoeven typen. Er zijn twee manieren: *Push Button* en *WPS Personal Identification Number (PIN)*. Bij de *Push Button*-methode moet er binnen circa 1 minuut) een speciale WPS-knop op de draadloze router en op de laptop ingedrukt worden. Beide apparaten wisselen vervolgens automatisch de sleutel uit en de verbinding komt tot stand. De meeste *wireless USB dongles* ondersteunen push-button-setup. Laptops, pc's, iPads en dergelijke ondersteunen *Push Button* niet omdat de speciale knop ontbreekt. De tweede methode, 'PIN', vereist het intypen van een pincode.

### 2.16.3 ZigBee versus Bluetooth versus wifi

De transmissiesnelheid van Zigbee is stukken lager dan [wifi](https://nl.wikipedia.org/wiki/Wifi) en [Bluetooth](https://nl.wikipedia.org/wiki/Bluetooth) omdat het ontwikkeld is met als doel een laag stroomverbruik te hebben. ZigBee, Bluetooth en wifi zijn werkzaam in de industriële, wetenschappelijke en medische ([ISM](https://nl.wikipedia.org/w/index.php?title=Industrial_Scientific_Medical&action=edit&redlink=1)-)radiobanden. Een ZigBee netwerk kan uit veel apparaten bestaan, hierdoor wordt het bereik van het netwerk ook vergroot omdat de apparaten informatie aan elkaar doorgeven tot aan de coördinator.

|  |  |  |  |
| --- | --- | --- | --- |
|  | **ZigBee** | [**Bluetooth**](https://nl.wikipedia.org/wiki/Bluetooth) | [**wifi**](https://nl.wikipedia.org/wiki/Wifi) |
| Standaard | IEEE 802.15.4 | IEEE 802.15.1 | [IEEE 802.11 a, b, g, n](https://nl.wikipedia.org/wiki/IEEE_802.11) |
| Frequentieband | 2.4 GHz, 868 / 915 MHz | 2.4 GHz | 2.4 GHz, 5 GHz |
| Protocol stack | ~ 20 kbit | ~ 1 Mbit | ~ 1 Mbit |
| Datasnelheid | 250 kb/s (2.4 GHz)  40 kb/s (915 MHz)  20 kb/s (868 MHz) | 1-3 Mbps | 11 - 105 Mbps |
| Industriegroep | ZigBee Alliance | Bluetooth SIG | wifi Alliance |
| [Netwerktopologie](https://nl.wikipedia.org/wiki/Netwerktopologie) | Point to point, Ster, Boomstructuur, Mesh | Ster | Point to point, Ster |
| Aantal kanalen | 16 (2.4 GHz)  10 (915 MHz)  1 (868 MHz) | 79 | 11-14 |
| Bereik | 10-70m | 10m | 10-100m |
| Aantal systemen | 65.536 (Theoretisch) | 8 | 32 |
| Beveiliging | 128 AES | ? | RC4, AES, TKIP |

## [https://upload.wikimedia.org/wikipedia/commons/thumb/e/e3/NFC_Tag_Chip.jpg/220px-NFC_Tag_Chip.jpg](https://commons.wikimedia.org/wiki/File:NFC_Tag_Chip.jpg)2.17 Near field communication

**Near Field Communication** of **NFC** is een contactloze communicatiemethode die gebruikmaakt van de ISM-[frequentieband](https://nl.wikipedia.org/wiki/Frequentieband)[[1]](https://nl.wikipedia.org/wiki/Near_field_communication#cite_note-1) op 13,56 MHz.

### 2.17.1 Kenmerken

NFC heeft doorgaans een bereik van ongeveer 10 centimeter. NFC wordt ook wel gezien als een extensie van [*radio frequency identification*](https://nl.wikipedia.org/wiki/Radio_frequency_identification) (RFID). Een RFID-systeem maakt gebruik van een *tag*, een lezer en een *backend* (bijvoorbeeld een database). Een NFC-chip kan in drie verschillende standen werken: tag-emulatie (ook wel passive mode), waar de NFC-chip zich gedraagt als een RFID-tag, active mode waar de NFC zich gedraagt als een reader en peer-to-peermode waarbij het mogelijk is om te communiceren tussen twee NFC-toestellen (bijvoorbeeld bestandstransmissie).

NFC is met diverse RFID-standaarden uitwisselbaar, zoals the ISO/IEC 14443A/B en ISO/IEC 15693, maar ook de [FeliCa](https://nl.wikipedia.org/w/index.php?title=FeliCa&action=edit&redlink=1" \o "FeliCa (de pagina bestaat niet))-card van Sony (dit type tag is geen officiële standaard). De techniek is ontwikkeld en gestandaardiseerd door het [NFC-forum](https://nl.wikipedia.org/w/index.php?title=NFC-forum&action=edit&redlink=1) waar onder andere [Philips](https://nl.wikipedia.org/wiki/Koninklijke_Philips_Electronics_N.V.), [Sony](https://nl.wikipedia.org/wiki/Sony) en [Nokia](https://nl.wikipedia.org/wiki/Nokia_(bedrijf)) deel vanuit maken. Het is vooral bedoeld voor gebruik in [mobiele telefoons](https://nl.wikipedia.org/wiki/Mobiele_telefoon).

### 2.17.2 Toepassingen

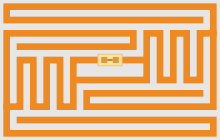
NFC bouwt verder op [RFID](https://nl.wikipedia.org/wiki/RFID)-systemen door ook tweerichtingscommunicatie toe te laten, waar eerdere systemen zoals contactloze smartcards alleen eenrichtingscommunicatie toelieten.[[3]](https://nl.wikipedia.org/wiki/Near_field_communication#cite_note-PopSciNFC-3) Omdat voedingloze NFC-tags ook door NFC-apparaten gelezen kunnen worden, kunnen ze ook eenrichtingsapplicaties vervangen.

* In [België](https://nl.wikipedia.org/wiki/Belgi%C3%AB) lanceerde [Keytrade](https://nl.wikipedia.org/wiki/Keytrade" \o "Keytrade) in december 2012 [KeyKash](https://nl.wikipedia.org/w/index.php?title=KeyKash&action=edit&redlink=1" \o "KeyKash (de pagina bestaat niet)), een systeem om door twee smartphones tegen elkaar te houden geld over te schrijven van de ene eigenaar naar de andere.
* Bluetooth en Wi-Fi-verbindingen: Via de lage snelheidsverbinding van NFC kan een snellere verbinding via [Bluetooth](https://nl.wikipedia.org/wiki/Bluetooth) of [Wi-Fi](https://nl.wikipedia.org/wiki/Wi-Fi) opgezet worden.
* Social networking**:** NFC kan gebruikt worden voor [social networking](https://nl.wikipedia.org/wiki/Social_networking" \o "Social networking), bijvoorbeeld om contactgegevens, foto's of bestanden te delen met anderen.
* Identiteits- en toegangscontrole: Omdat NFC versleuteling ondersteunt kan het meer geschikt zijn voor identiteits- en toegangscontrole dan eerdere RFID-systemen.
* Sinds 2000 wordt het ook op grote schaal toegepast in de [thuiszorg](https://nl.wikipedia.org/wiki/Thuiszorg). De zorgpas van de cliënt wordt door de thuiszorgmedewerker gescand met de NFC-telefoon. Een speciale toepassing op de telefoon registreert de gegevens en stuurt ze direct door via het mobiele netwerk naar het zorgregistratiesysteem van de thuiszorgorganisatie. De thuiszorgmedewerker hoeft daardoor geen administratie meer bij te houden over de geleverde zorg.
* In 2009 rolden uitzendbureaus [*In Person*](https://nl.wikipedia.org/w/index.php?title=In_Person&action=edit&redlink=1) en [*USG People*](https://nl.wikipedia.org/wiki/USG_People) in Nederland een NFC-gebaseerd registratiesysteem uit bij al haar opdrachtgevers. Door gebruik te maken van NFC-passen hoeven medewerkers geen urenbriefjes meer in te vullen.
* Smartphone-automatisering**:** [Smartphones](https://nl.wikipedia.org/wiki/Smartphone) die met NFC uitgerust zijn kunnen NFC-tags of stickers uitlezen om taken te automatiseren. Zo kunnen bijvoorbeeld instellingen aangepast worden, tekst kan verzonden worden, een app kan opgestart worden.

### 2.17.3 Problemen

Het gemak van het gebruik van NFC kan bij verkeerde implementatie echter ook voor problematische situaties zorgen. Zo verscheen in december 2008 de applicatie eCL0WN waarmee chips van biometrische paspoorten kunnen worden uitgelezen en gekopieerd. Ook de in 2008 geïntroduceerde [OV-chipkaart](https://nl.wikipedia.org/wiki/OV-chipkaart) bleek door ontwerpfouten eenvoudig te kraken en zelfs in strijd met de [privacywetgeving](https://nl.wikipedia.org/wiki/Wet_bescherming_persoonsgegevens).

## 2.18 Radio-frequency identification (RFID)

[](https://commons.wikimedia.org/wiki/File:EPC-RFID-TAG.svg)**Radio-frequency identification** (identificatie met [radiogolven](https://nl.wikipedia.org/wiki/Radiogolf), **RFID**) is een technologie om van een afstand informatie op te slaan in en af te lezen van zogenaamde RFID-*tags* die op of in objecten of levende wezens zitten. De lijst van toepassingen is enorm lang.

### 2.18.1 Soorten

Er bestaan RFID-tags in de meest uiteenlopende vormen en afmetingen. Ze kunnen alleen-lezen of lezen/schrijven zijn.

Ze kunnen actief, semiactief/semipassief of passief zijn. Actieve RFID-tags hebben een [batterij](https://nl.wikipedia.org/wiki/Batterij_(elektrisch)) en kunnen worden gelezen en geschreven met een "*remote transceiver*" ook wel "*reader*" of lezer genoemd die met een [antenne](https://nl.wikipedia.org/wiki/Antenne_(straling)) radiogolven zendt en ontvangt. Ze kunnen een signaal over een grotere afstand (van zo'n 100 meter tot zelfs een paar kilometer) uitzenden; ze zenden meestal met een interval hun ID uit. Semi-actieve tags hebben ook een batterij maar zenden alleen als antwoord op een ontvangen signaal. Passieve tags hebben geen eigen energiebron: ze benutten het elektromagnetische veld van een lezer om een stroom te induceren in een spoel, waarmee de chip wordt gevoed. Hierdoor gaat het antwoordsignaal niet over een grote afstand (van enkele centimeters tot ongeveer vijf meter). Tevens zijn er de zogenaamde 'chiploze tags' (zie foto), die gebruikt worden voor eenvoudige identificatie zoals diefstalpreventie. Dit zijn strikt genomen geen RFID-tags omdat ze geen uniek identificatienummer (ID) bevatten. Ze bestaan namelijk uit een afgestemde resonantiekring die op een specifieke frequentie energie absorbeert.

[](https://commons.wikimedia.org/wiki/File:Inside_of_RFID_chip.jpg)Ook de hoeveelheid data kan verschillen van enkele bits tot meer dan 1 [megabit](https://nl.wikipedia.org/wiki/Megabit" \o "Megabit). Al deze mogelijkheden vertalen zich uiteraard ook in de prijs: een eenvoudige passieve tag kost niet meer dan dertig eurocent. Gecompliceerde RFID-tags, die bijvoorbeeld gekoppeld zijn aan [sensoren](https://nl.wikipedia.org/wiki/Sensor) die ook nog de temperatuur of vochtigheid meten, zijn aanzienlijk duurder (soms wel 100 euro per stuk).

De laatste trend binnen de RFID-branche is UHF EPC *Class 1 Gen 2 tag* afgekort *Gen 2*, waarin *gen* staat voor *Generation*. Deze tags leveren betere prestaties dan de voorgaande UHF-standaarden. Hierdoor wordt er steeds meer mogelijk met RFID. RFID-tags zullen nooit de streepjescode geheel gaan vervangen aangezien de kostprijs altijd hoger zal zijn dan het printen van een streepjescode. Kostprijzen voor gen 2 tags liggen tussen de 5 en 20 cent (afhankelijk van het aantal).

2.18.2 Voor- en nadelen

Voordelen van het toepassen van RFID zijn onder meer:

* Unieke code zodat ieder individueel object altijd en overal gevolgd kan worden;
* Er is geen fysiek contact nodig;
* Er is geen zichtlijn nodig (zoals bij de streepjescode);
* Vele (honderden) codes kunnen in een of enkele seconden worden gelezen;
* Veel grotere afstanden zijn mogelijk dan bij de streepjescode (hoewel de techniek ook hier grote vooruitgang boekt);
* Vervalsen van RFID-tags is veel complexer dan de streepjescode;
* Door de unieke codering wordt productvervalsing bemoeilijkt en/of snel opgespoord;
* Door weersinvloeden, vuil, enzovoorts kunnen streepjescodes (in tegenstelling tot RFID-tags) onleesbaar worden.

Nadelen van RFID zijn onder meer:

* [De privacy kan in het geding komen](https://nl.wikipedia.org/wiki/Radio-frequency_identification#Privacybezwaren);
* Als identificatiedocumenten zoals een paspoort een RFID-tag hebben, kunnen regeringen en inlichtingendiensten hier misbruik van maken en mensen volgen;
* Als het identificatienummer van een RFID-tag verbonden kan worden met een individu, kan dit individu gevolgd worden (door [marketeers](https://nl.wikipedia.org/wiki/Marketing), overheidsfunctionarissen, stalkers, dieven of andere criminelen);
* Lees/schrijfmogelijkheden van de RFID-tag kunnen het mogelijk maken dat er ongemerkt fraude wordt gepleegd;
* Een ander probleem is *tag-collision*: als RFID-chips tegelijk worden geactiveerd door een zender en ze tegelijk hun code versturen, kan de ontvanger de verschillende codes niet onderscheiden. Dit wordt voorkomen door middel van selectieve activatie met behulp van *[binary tree](https://nl.wikipedia.org/w/index.php?title=Binary_tree&action=edit&redlink=1" \o "Binary tree (de pagina bestaat niet)) search*-methode totdat slechts één tag reageert.
* Omdat een RFID-reader veel informatie genereert is inzet van een speciaal soort *software* (*middleware/edgeware*) noodzakelijk, hoewel er steeds meer readers op de markt verschijnen die dit zelf kunnen;
* Door het weggooien van verpakkingsmateriaal, tickets enzovoorts met een RFID-chip komt het afval zo vol metalen, dat het alleen nog maar als chemisch afval kan worden opgehaald. Het is in ieder geval niet te hergebruiken.
* RFID kan medische apparatuur op afstand verstoren.
* RFID-tags kunnen (geringe) [elektromagnetische straling](https://nl.wikipedia.org/wiki/Elektromagnetische_straling) veroorzaken.

### 2.18.3 Problemen

Privacy bezwaren

RFID kan aangewend worden voor doeleinden die voorheen slechts fantasie leken, waaronder het volgen van personen met RFID-tags in hun kleren of het traceren van de inhoud van huizen door naar aanwezige RFID-tags te kijken.

* De koper van een product zal zich niet per se bewust zijn van de aanwezigheid van de tag of in staat zijn de tag te verwijderen.
* De tag kan van een afstand worden gelezen zonder dat de persoon dit weet. De afstand is echter beperkt door fysische grootheden als frequentie en antennegrootte van de tag.
* Als een getagd product wordt betaald met een [creditcard](https://nl.wikipedia.org/wiki/Creditcard) of [pinpas](https://nl.wikipedia.org/wiki/Betaalkaart) is het in principe mogelijk om het unieke ID te koppelen aan de identiteit van de aankoper.

Klonen van RFID-tags

Met de juiste apparatuur is het relatief eenvoudig om van een niet-beveiligde chip het ID uit te lezen en dit vervolgens naar een duplicaat-tag te schrijven. De [Radboud Universiteit Nijmegen](https://nl.wikipedia.org/wiki/Radboud_Universiteit_Nijmegen) toonde in 2008 al aan dat de [OV-chipkaart](https://nl.wikipedia.org/wiki/OV-chipkaart) zeer gemakkelijk gekloond kan worden met behulp van relatief goedkope apparatuur. Deze contactloze chipkaart is gebaseerd op de onveilige [MIFARE](https://nl.wikipedia.org/wiki/MIFARE) Classic chip. De voor het klonen gebruikte apparatuur en aansturing is [Open Source](https://nl.wikipedia.org/wiki/Open_Source) ontwikkeld. Het gaat hier om de [proxmark](http://www.proxmark.org/) en zeer goedkope [NFC](https://nl.wikipedia.org/wiki/Near_field_communication) apparatuur die aangestuurd wordt door [libnfc](http://www.libnfc.org/).

Er zijn echter diverse manieren waarop geprobeerd wordt dit tegen te gaan. Voorbeelden hiervan zijn encryptie en het principe van *Physically Unclonable Functions* (PUF’s). Bij het laatste wordt uitgegaan van het gegeven dat elke chip heel kleine fysieke verschillen bevat die voortkomen uit de onoverkomelijke imperfectie van het productieproces.

## 2.19 MIFARE

**MIFARE** is een merk van [NXP Semiconductors](https://nl.wikipedia.org/wiki/NXP_Semiconductors) wat exclusief gebruikt wordt voor de chips in chipcards en lezers van dat bedrijf. De technologieën die onder dit merk worden verkocht, zijn gebaseerd op de ISO/IEC 14443A standaard en werken op een frequentie van 13.56 [MHz](https://nl.wikipedia.org/wiki/Megahertz).

NXP MIFARE producten worden onder meer toegepast in:

* paspoorten
* loyalty kaarten
* toegangs-systemen voor musea, kantoorgebouwen, parkeergarages, hotels, fitness centra
* product identificatie
* consoles voor spelcomputers
* contactloos betalen met je mobiele telefoon
* tol systemen

De bekendste leden uit de MIFARE familie zijn *MIFARE Classic*, *MIFARE Ultralight*, *MIFARE Plus*, *MIFARE DESFire*, *MIFARE4MOBILE*, *MIFARE FLEX* en *MIFARE SDK*.[[1]](https://nl.wikipedia.org/wiki/MIFARE#cite_note-1)

### 2.19.1 MIFARE Classic

De MIFARE Classic kaart is een opslagmedium, waarbij het geheugen is verdeeld in sectoren en blokken die versleuteld worden door een simpele beveiligingstechniek. Dankzij de lage kosten wordt dit type kaart veel gebruikt in het openbaar vervoer zoals bijvoorbeeld in een [OV-chipkaart](https://nl.wikipedia.org/wiki/OV-chipkaart).

De MIFARE Classic 1K heeft een opslagruimte van 1024 bytes, verdeeld in zestien sectoren; elke sector bevat vier blokken en is beveiligd met twee verschillende sleutels, genaamd A en B. Ze kunnen geprogrammeerd worden voor operaties als lezen en schrijven. De MIFARE Classic 4k heeft een opslagruimte van vier kilobyte, verdeeld in veertig sectoren. 32 sectoren zijn even groot als die in type 1k; de laatste acht sectoren bevatten zestien blokken in plaats van vier.

### 2.19.2 MIFARE Ultralight

De MIFARE Ultralight-kaarten hebben 64 bytes, zonder beveiliging. Dit type kaart is dusdanig goedkoop dat het dikwijls wordt gebruikt bij wegwerpkaarten, zoals voetbaltickets.

### 2.19.3 MIFARE DESFire

De MIFARE DESFire-kaarten hebben een geheugen van vier kilobytes, met een 3DES beveiliging. Dit type kaart is veiliger dan bijvoorbeeld de MIFARE Classic-kaarten.

### 2.19.4 Veiligheid

In een presentatie op het [Chaos Communication Congress](https://nl.wikipedia.org/w/index.php?title=Chaos_Communication_Congress&action=edit&redlink=1) in December 2007 toonden Henryk Plötz en Karsten Nohl aan dat zij door middel van [reverse engineering](https://nl.wikipedia.org/wiki/Reverse_engineering) een deel van het [algoritme](https://nl.wikipedia.org/wiki/Algoritme) ontdekt hadden dat gebruikt wordt in de MIFARE Classic chip.

In maart 2008 maakte de Digital Security research group van de [Radboud Universiteit Nijmegen](https://nl.wikipedia.org/wiki/Radboud_Universiteit_Nijmegen) bekend dat zij in staat waren om chipkaarten gebaseerd op de MIFARE Classic chip te klonen en aan te passen. NXP probeerde de publicatie van het onderzoek te stoppen.

In juni 2008 hebben dezelfde onderzoekers van de Radboud universiteit een [Oyster card](https://nl.wikipedia.org/wiki/Oyster_card" \o "Oyster card) (Londen traveler kaart, een soort Lijn-kaart) met dezelfde MIFARE Classic chip gekraakt. Zij bleken in staat om, na een kaart van een andere gebruiker gelezen te hebben, de kaart te kopiëren en het saldo op te hogen en er daarna een dag lang mee te reizen.

## 2.20 X10

X10 is een internationale en open [industriestandaard](https://nl.wikipedia.org/wiki/Industriestandaard) voor een communicatieprotocol tussen zenders en ontvangers voor [domotica](https://nl.wikipedia.org/wiki/Domotica" \o "Domotica) (huisautomatisering), dat gebruikmaakt van het elektriciteitsnet (*X10 power line*) of van radiofrequentie (*X10 RF*).

X10 werd ontwikkeld in 1975 door het Schotse *Pico Electronics* om afstandsbediening van huisapparatuur mogelijk te maken. Het was de eerste domotica netwerktechnologie voor algemeen gebruik en is nog steeds de meest wijdverspreide. Ondanks het bestaan van alternatieven met een hogere bandbreedte, blijft X10 wereldwijd populair in de huisomgeving met een goedkope beschikbaarheid van nieuwe componenten.

### 2.20.1 Werking X10 power line

X10 bestaat uit zenders (controllers) en ontvangers, die in een stopcontact gestoken worden. Een apparaat of lamp wordt aangesloten op de ontvanger. De zender en de ontvanger communiceren over het elektriciteitsnet, waardoor geen extra communicatienetwerk aangelegd hoeft te worden. Voorbeelden van zenders zijn *transceivers* (zet een signaal van een draadloze afstandsbediening om naar een signaal op het elektriciteitsnet) of de computerinterface (kan aangesloten worden op een computer of voert zelf eenvoudige programma's en tijdschema's uit). Voorbeelden van ontvangers zijn lampontvangers (waarmee lampen aan- of uitgeschakeld of gedimd kunnen worden) en apparaat ontvangers (waarmee apparaten met meer vermogen geschakeld kunnen worden).

### 2.20.2 Protocol

De adressering bestaat uit veelvouden van vier bits:

* De eerste vier bits bevatten een "huisselectie"-code, weergegeven als een letter (A tot P, de eerste 16 letters van het alfabet).
* Een of meer "unit selectie"-codes, weergegeven als een getal (01 tot 16); meerdere selectiecodes worden gebruikt om meerdere lichten/apparaten gelijktijdig te sturen.
* De laatste vier bits bevatten het te versturen commando; alle geadresseerde units wachten tot het commando is ontvangen.

Ieder apparaat in huis moet een unieke code krijgen, waardoor maximaal 256 apparaten (16 x 16) storingsvrij in elkaars bereik kunnen worden gebruikt. Tot 16 apparaten gebruikt men in het algemeen 1 huisselectiecode per woning, maar zolang er geen problemen zijn met buren, kunnen meerdere codes hiervoor per huis worden gekozen. Bij problemen met units welke veroorzaakt kunnen worden door signalen van andere woningen, kan een filter worden geplaatst zodat geen signalen het huis verlaten of vreemde signalen het huis niet binnenkomen.

## 2.21 Andere mogelijke technieken

Als we dachten dat we hier na de voorgaande lijst op het eind zijn gekomen hadden we het mis. Al wat hierboven is besproken zijn de meest voorkomende, of liever degene die ik in mijn beroep regelmatig zie passeren. Het zijn ook de kosteloze verbindingen, want vergeet niet, er bestaat nog zo iets als de GSM, de telefoonlijn (denk nog eens, *met enige weemoed*, terug aan de modemtijd) als ook de connecties die meerdere bedrijven hebben tussen hun vestigingen.

Er bestaan nog veel afgeleiden van de besproken technieken. Sommige technieken gebruiken combinaties van de beschreven manieren.

# Toepassingen

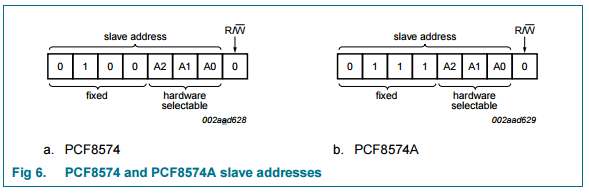
Van de bovenstaande lijst bekijk ik graag enkele seriële protocols. Niet allemaal, omdat het principe van aansturing en gebruik vergelijkbaar is. Zoals vermeld I2C = IIC = TWI.

Ook vind ik het belangrijk om de drie “ingebouwde” communicatie methodes van de Arduino te gebruiken. Onze vriend is uitgerust met I2C, SPI en seriële interface (soms UART genoemd). In de gebruikte toepassingen zal je snel zien dat meerdere systemen door elkaar worden gebruikt, of liever gezegd, delen van elkaar gebruiken in de module.

## 3.1 I2C interface

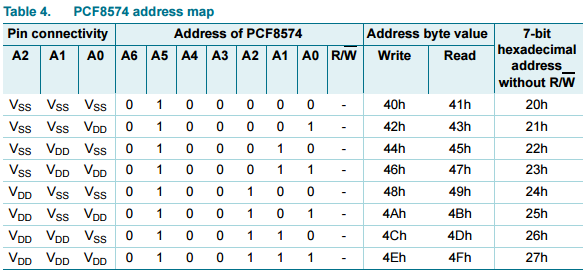
Via onze Chinese leverancier ontving ik een I2C module. Hierop staat de Philips/NXP chip PCF8574A een “Remote 8-bit I/O expander for I2C-bus with interrupt” IC. De datasheets kan je vinden via de link onderaan.

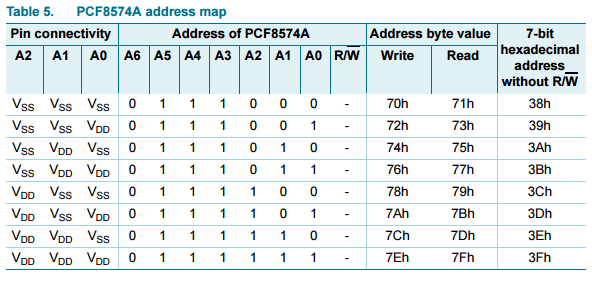
Belangrijk is om te weten wat het adres is van deze module, hiermee weet de controller (Arduino) met wie hij moet communiceren. Volgens de datasheets kan je de adressering aanpassen met de pinnen A0, A1 en A2. De adressering van de IC is volgens onderstaande figuur opgebouwd:



Aangezien we hardware matig maar 3 bits kunnen configureren (A0, A1, A2) hebben we maar 8 mogelijkheden per IC-type. Willen we meer, dan combineren we een PCF8574 met een PCF8574A (= 16 mogelijkheden).

De adresmap uitgeschreven maakt duidelijk wat je moet aanleggen bij schrijven of lezen:





Op de module staat een PCF8574A, de adressen A0, A1 en A2 zijn hoog, dus hebben we het adres 3Fh. Bij controle blijkt dit ook zo te zijn. (Over die controle hebben we het verder nog). De adressering doen we door een soldeerbrugje te leggen aan de respectievelijke adrespadjes.

Het grote voordeel met deze module (of IC) is dat we bij twijfel niet veel adressen moeten uitproberen wanneer we hierover geen weet hebben.

Tot hier het interfacen met de buitenwereld op serieel vlak. Op het IC worden de binnen gekomen bits terug naar een 8-bit woord omgezet en aan de parallelle uitgang aangeboden.

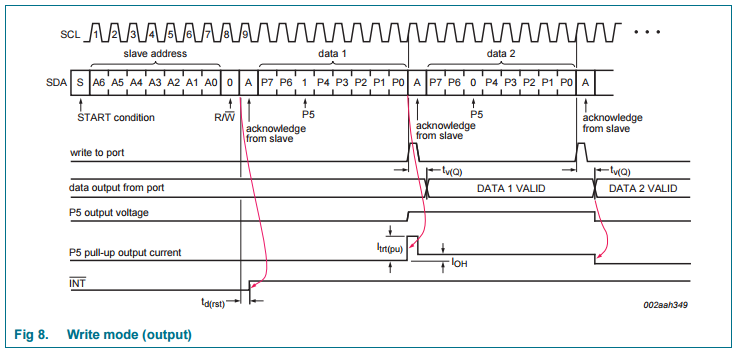
Het IC kan dit in beide richtingen: serial in, serial out en parallel in, parallel out.

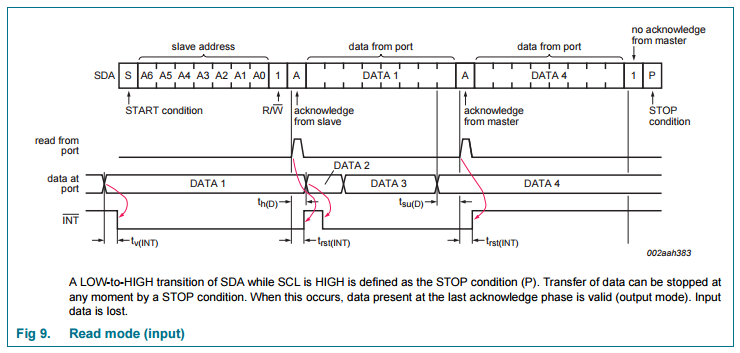
De uitzoeken van het adres doe je met bijvoorbeeld de I2C-Scanner, een programmaatje te vinden op internet <http://playground.arduino.cc/Main/I2cScanner> de volledige uitleg staat hierbij.

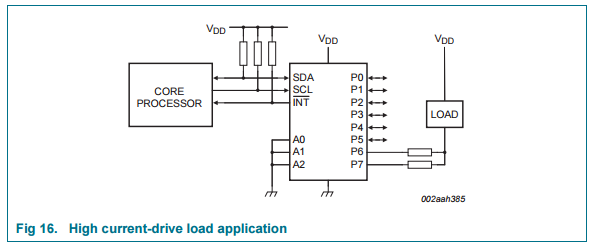
### 3.1.1 LCD display met I2C interface

Een veel gebruikte toepassing van deze module is de aansturing van een LCD display. Normaal heb je minimum 8 verbindingen nodig, met de I2C interface heb je met 4 draadjes genoeg, een grote besparing van pinnen. Zoals we in de onderstaande figuur zien is een SDA en een SCL lijn nodig. SCL staat voor Serial CLock, SDA wil Serial Data zeggen. Ontcijferen we de datastroom dan loopt eerst het adres voorop waarna de informatie (data) volgt.

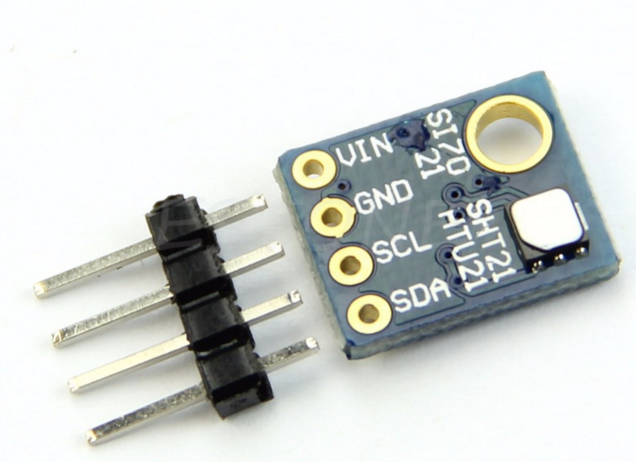
In het parallelle stuk van de chip hebben we 8 I/O pinnen (P0 – P7)



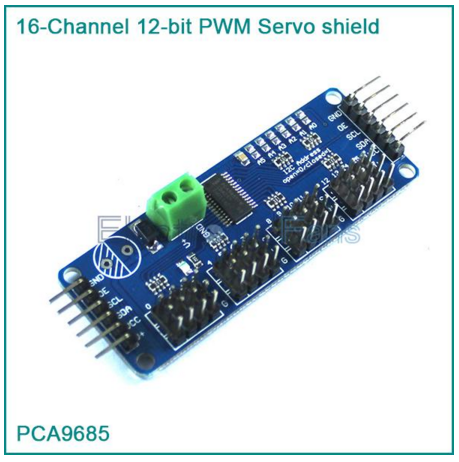
Voor de volledigheid, ook nog het read mode signaal:

Gecombineerd met het parallelle deel, duidelijk is te zien dat de SDA en SCL lijnen een pullup weerstand moeten hebben. Het best plaats je deze op het eind van de (fysieke) lijn.

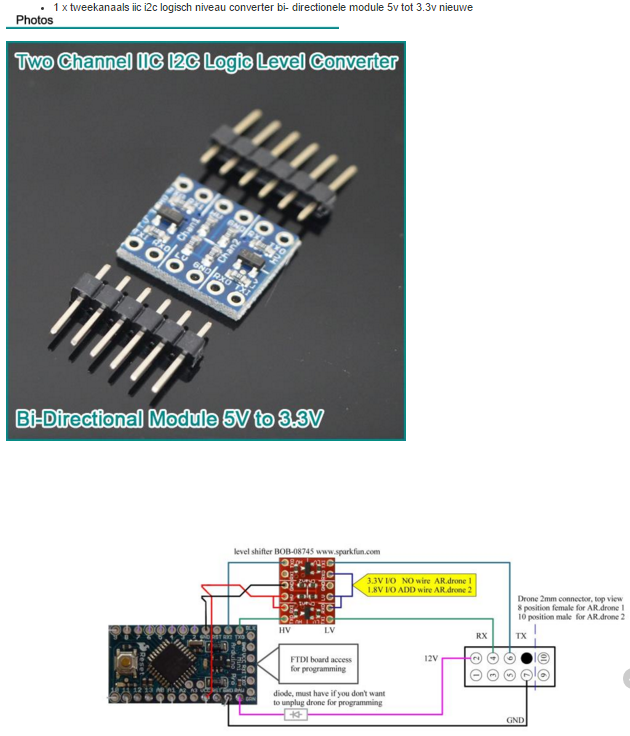
### 3.1.2 Andere toepassingen



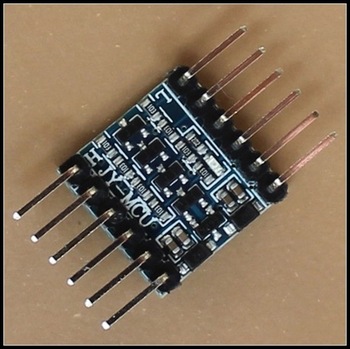
Van dezelfde leverancier hebben we nog enkele I2C applicaties

* SI7021 vochtigheid sensor met I2C interface
* 16 channel PWM 12-bit servo shield met I2C interface PCA9685
* VGA cmos camera
* EEPROM modules
* OLED rgb display module
* Enzoverder (ik keek enkel op de eerste pagina)

Misschien dit nog: zoals gekend zijn er in de Arduino wereld twee voedingsspanningen gangbaar: 5V en 3V3, niet alle module kunnen overweg met beide spanningen, daarvoor zijn er levelshifters ontwikkeld die dit probleem opvangen.



<http://nl.aliexpress.com/item/Two-Channel-IIC-I2C-Logic-Level-Converter-Bi-Directional-Module-5V-to-3-3V/32435434792.html?s=p>

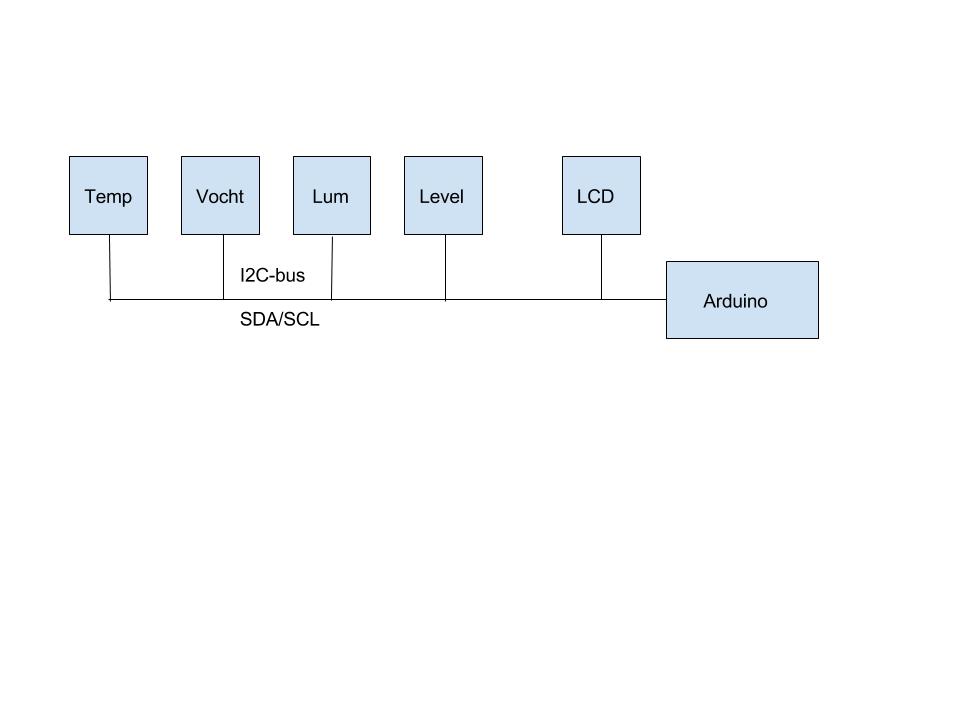


### 3.1.3 I2C met meerdere Arduino’s

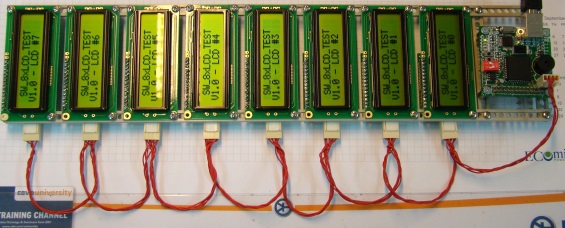
Tot hier toe gebruikten we een enkele controller die een I2C device aanstuurt. Maar het is ook mogelijk om meerdere Arduino’s met elkaar te laten communiceren. Het grote verschil is hier dat de Arduino geen aparte interface kaart nodig heeft maar zelf de nodig pinnen en firmware beschikbaar heeft. Zelfs de nodig libraries zijn vlotjes van internet te plukken (WIRE.lib).

Ze spreken hier van een Master - Slave configuratie, waar er een Arduino het voortouw neemt en de controle in de hand houdt en een andere Arduino die zijn resultaten op vraag van de master doorgeeft, of opdrachten krijgt van die master.

### 3.1.4 Nuttige toepassing van dit I2C-bus systeem

In de toepassingen spraken we over een verbinding tussen een controller en een device. In de bespreking van de PCF8574 hadden we het over adressering. Het is dus mogelijk om meerdere devices aan een Arduino te koppelen, door die laatste telkens een adres mee te geven weet het device of het zijn info moet geven of niet. Je kan dus een Arduino de temperatuur, de vochtigheid, de hoeveelheid licht en de stand van het waterniveau laten opvragen en alles weergeven op een LCD-display, en dit over 2 draden.

Nog een voorbeeld:

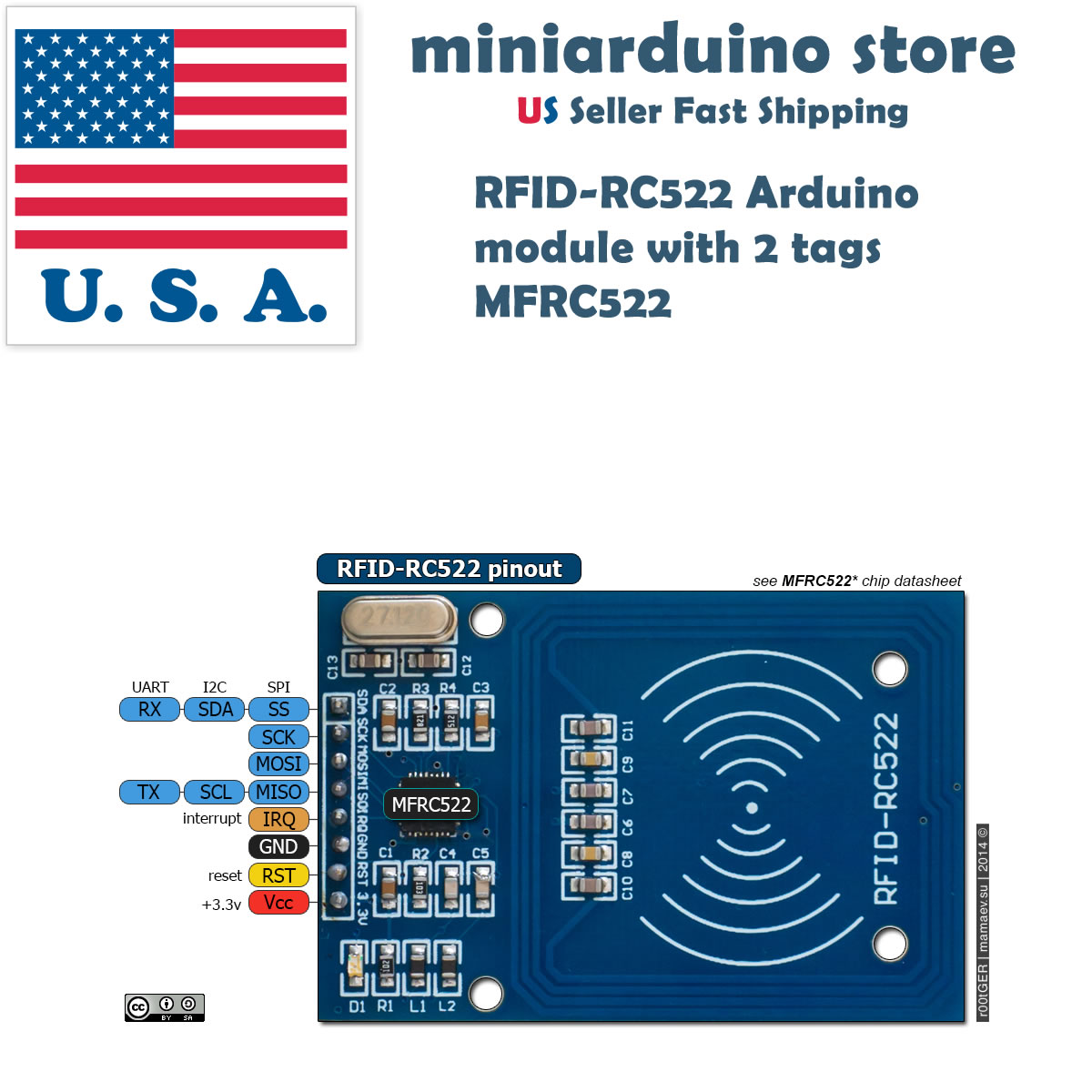


## 3.2 SPI Interface

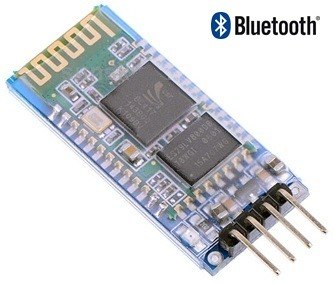
Dit is een 4-draads system

### 3.2.1 RFID of NFC interface

Ook een populaire module is de RFID-RC522 module. Deze module is opgebouwd rond de NXP RC522 chip . Deze IC heeft drie mogelijke interfaces: een seriele (RS232), SPI (Serial Peripheral Interface vergelijkbaar met RS232) en I2C. Wil je bij deze laatste alsnog adressering, dan moet je verdomd goed kunnen solderen op de pinnen van het IC (zie datasheets). Heel belangrijk bij deze module is dat deze op 3V3 werkt, terwijl de Arduino op 5V werkt. Je hebt dus een levelshifter nodig, zoals hiervoor beschreven.



## 3.3 Seriële communicatie of UART-verbinding

Als laatste is de seriele verbinding aan bod. Wanneer we de sketch opladen in de Arduino gebruiken we via de USB deze interface. Communicatie met de Serial Monitor loopt via dezelfde weg. Je voelt wel aan dat we nu ergens een conflictje hebben, enerzijds vertellen we Arduino wat hij moet doen, en anderzijds babbelen we met hem over zijn bevindingen. In het begin van dit boekwerk schreef ik dat de seriële poort geen busstructuur is, dus hangen we meerdere “toepassingen” op dezelfde pinnen is dit vragen om moeilijkheden.

Dit is op te lossen door eerst de sketch in te lezen en PAS DAN de verbindingen te maken met de schakeling. In de praktijk bestaat de mogelijkheid om de Arduino softwarematig aan te passen en meerdere UART verbindingen te laten opzetten, maar de UNO (en directe afgeleiden) heeft dit niet standaard. De Arduino Mega, heeft daarentegen wel drie UARTs.

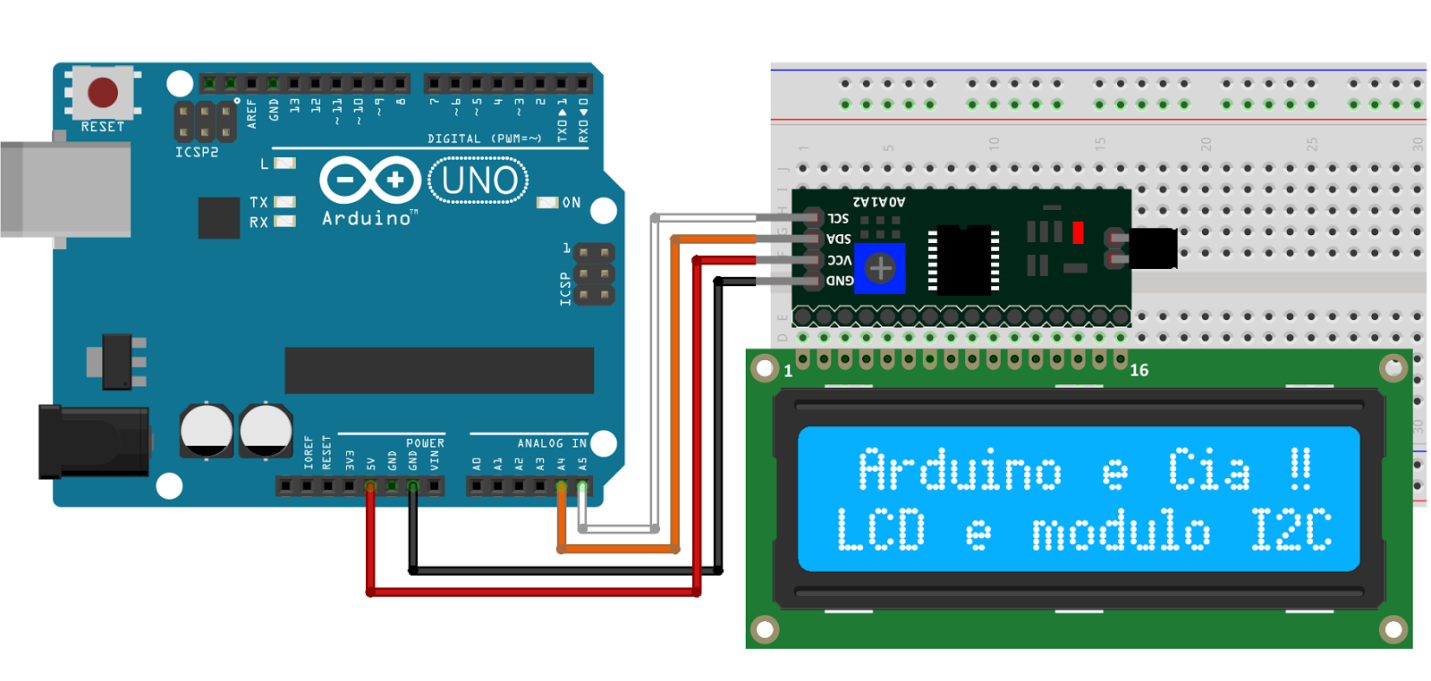
Praktisch zijn op de Arduino Uno dit de digitale poorten 0 (RX) en 1 (TX).

Een module die van deze communicatie techniek gebruikt maakt is de Bluetooth module.

## 3.4 De praktijk

### 3.4.1 Het LCD display aansturen met I2C

Om een LCD display aan te sturen met I2C moeten we even de library downloaden en installeren. Heel belangrijk is dat we de reeds bestaande library wegdoen (vb copy naar andere plaats). We sluiten het LCD aan de Arduino, volgens de voorgeschreven methode: SCL aan A5, SDA aan A4



Het gebruikte testprogramma is voor een 2 x 16 LCD display. Aan de hand van de hierboven beschreven manier kunnen we het adres achterhalen, hier is dit 0x3F.

#include <Wire.h>

#include <LiquidCrystal\_I2C.h>

LiquidCrystal\_I2C lcd(0x3F,16,2); // set the LCD address to 0x3F for a 16 chars and 2 line display

void setup()

{

lcd.init(); // initialize the lcd

lcd.init();

// Print a message to the LCD.

lcd.backlight();

lcd.setCursor(1,0);

lcd.print("Hello, world!");

lcd.setCursor(1,1);

lcd.print("From Arduino!");

}

void loop()

{

}

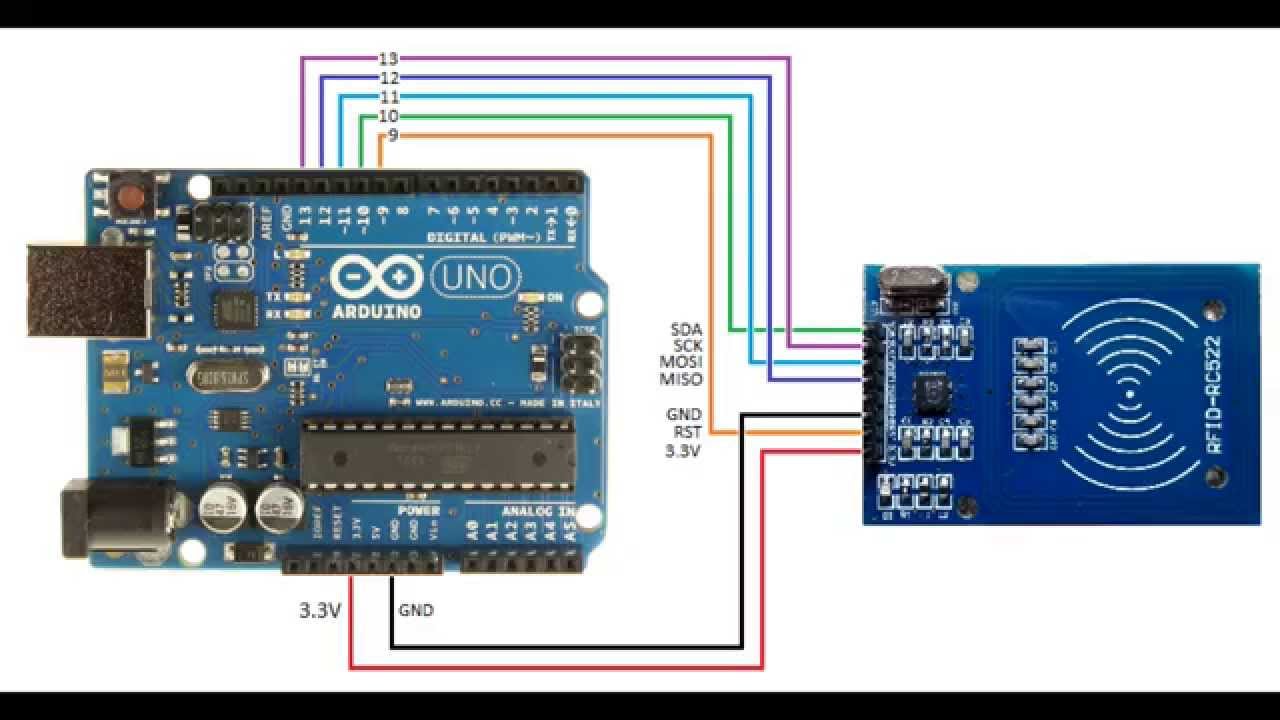
Op het scherm komt: “Hello, world!” ”From Arduino!”

### 3.4.2 RFID / NFC uitlezen met SPI

Gebruik een levelshifter en liefst een actieve, dit wil zeggen dat er transistoren gebruikt worden om het niveau aan te passen, geen weerstanden, dit laatste is niet snel en zou oorzaak kunnen zijn van informatie verlies.

Niettegenstaande je op internet veel mensen de voeding van de kaart correct ziet aansluiten op de 3V3 van de Arduino, zie je ze de andere pinnen rechtstreeks aan de pinnen van de Arduino hangen (=5V). Het kaartje zal dit wel even aankunnen, maar op termijn zal dit sneuvelen. Volgens de datasheet mag er niet meer dan 0.5V bovenop de voedingspanning op de IO-pinnen komen. Reden waarom het wel kan is dat de Arduino geen 5V uitgeeft, maar minder, de overspanning is niet ernstig overschreden, maar het is geen garantie dat het op termijn blijft werken.

Zelf heb ik ook even gezondigd tegen de spanningslevel-regel en een test opstelling gemaakt met een Uno en een RFID-lezer.



Programma van internet geplukt:

/\*

\* http://playground.arduino.cc/Learning/MFRC522

\* https://github.com/miguelbalboa/rfid

\*

\*

\* MFRC522 - Library to use ARDUINO RFID MODULE KIT 13.56 MHZ WITH TAGS SPI W AND R BY COOQROBOT.

\* The library file MFRC522.h has a wealth of useful info. Please read it.

\* The functions are documented in MFRC522.cpp.

\*

\* Based on code Dr.Leong ( WWW.B2CQSHOP.COM )

\* Created by Miguel Balboa (circuitito.com), Jan, 2012.

\* Rewritten by Søren Thing Andersen (access.thing.dk), fall of 2013 (Translation to English, refactored, comments, anti collision, cascade levels.)

\* Released into the public domain.

\*

\* Sample program showing how to read data from a PICC using a MFRC522 reader on the Arduino SPI interface.

\*----------------------------------------------------------------------------- empty\_skull

\* Aggiunti pin per arduino Mega

\* add pin configuration for arduino mega

\* http://mac86project.altervista.org/

----------------------------------------------------------------------------- Nicola Coppola

\* Pin layout should be as follows:

\* Signal Pin Pin Pin

\* Arduino Uno Arduino Mega MFRC522 board

\* ------------------------------------------------------------

\* Reset 9 5 RST

\* SPI SS 10 53 SDA

\* SPI MOSI 11 51 MOSI

\* SPI MISO 12 50 MISO

\* SPI SCK 13 52 SCK

\*

\* The reader can be found on eBay for around 5 dollars. Search for "mf-rc522" on ebay.com.

\*/

#include <SPI.h>

#include <MFRC522.h>

#define SS\_PIN 10

#define RST\_PIN 9

MFRC522 mfrc522(SS\_PIN, RST\_PIN); // Create MFRC522 instance.

void setup() {

Serial.begin(9600); // Initialize serial communications with the PC

SPI.begin(); // Init SPI bus

mfrc522.PCD\_Init(); // Init MFRC522 card

Serial.println("Scan PICC to see UID and type...");

}

void loop() {

// Look for new cards

if ( ! mfrc522.PICC\_IsNewCardPresent()) {

return;

}

// Select one of the cards

if ( ! mfrc522.PICC\_ReadCardSerial()) {

return;

}

// Dump debug info about the card. PICC\_HaltA() is automatically called.

mfrc522.PICC\_DumpToSerial(&(mfrc522.uid));

}

Resultaat op de serial monitor:

Card UID: D4 36 37 5D

PICC type: MIFARE 1KB

Sector Block 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 AccessBits

15 63 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

61 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

14 59 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

13 55 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

54 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

53 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

52 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

12 51 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

49 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

48 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

11 47 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

45 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

10 43 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

41 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

9 39 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

8 35 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

32 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

7 31 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

29 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

6 27 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

25 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

5 23 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

22 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

21 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

20 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

4 19 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

3 15 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

12 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

2 11 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

1 7 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

4 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

0 3 00 00 00 00 00 00 FF 07 80 69 FF FF FF FF FF FF [ 0 0 1 ]

2 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [ 0 0 0 ]

1. D4 36 37 5D 88 08 04 00 62 63 64 65 66 67 68 69 [ 0 0 0 ]

Wat leren we hieruit?

Het is een kaart met 1kB geheugenruimte, 64 rijen bij 16 = 1024bytes

De code van de kaart is D4 36 37 5D

En ze gebruikt het Mifare protocoll

We willen iets meer doen met het resultaat: het is niet duidelijk welke commando’s er beschikbaar zijn. Daarom pluis ik de library uit. Ik zoek op UID in de hoop iets bruikbaars te vinden (Regel 301 -306 van de lib MFRC522.h). Hier vind ik nuttige info: er bestaan dus 3 soorten ID-cards: nl 4-bytes, 7-bytes en 10-bytes. Met de rest van de tekst moet ik iets kunnen doen met “size, uidByte[10]”

// A struct used for passing the UID of a PICC.

typedef struct {

byte size; // Number of bytes in the UID. 4, 7 or 10.

byte uidByte[10];

byte sak; // The SAK (Select acknowledge) byte returned from the PICC after successful selection.

} Uid;

In de sketch schrijven we: byte code0 = mfrc522.uid.uidByte[0]

Even uitrafelen: mfrc522 = de library; uid = de structuur; uidByte[] = commando

Hoger stond in het script: MFRC522 mfrc522(SS\_PIN, RST\_PIN); // Create MFRC522 instance.

We vertellen hier dat de klasse MFRC522, mfrc522 als object heeft, in de omschrijving staat trouwens dat we een “instance” creeeren.

mfrc522.PICC\_DumpToSerial(&(mfrc522.uid));

byte code0 = mfrc522.uid.uidByte[0];

Serial.println(code0,HEX);

byte code1 = mfrc522.uid.uidByte[1];

Serial.println(code1,HEX);

byte byte code4 = mfrc522.uid.uidByte[4];

Serial.println(code4,HEX);

byte code5 = mfrc522.uid.uidByte[5];

Serial.println(code5,HEX);

byte code6 = mfrc522.uid.uidByte[6];

Serial.println(code6,HEX);

Serial.print(code0,HEX);

Serial.print(" ");

Serial.print(code1,HEX);

Serial.print(" ");

Serial.print(code2,HEX);

Serial.print(" ");

Serial.print(code3,HEX);

Serial.print(" ");

Serial.print(code4,HEX);

Serial.print(" ");

Serial.print(code5,HEX);

Serial.print(" ");

Serial.print(code6,HEX);

Serial.println( );

Serial.println( );

byte size1 = mfrc522.uid.size;

Serial.println(size1);

code2 = mfrc522.uid.uidByte[2];

Serial.println(code2,HEX);

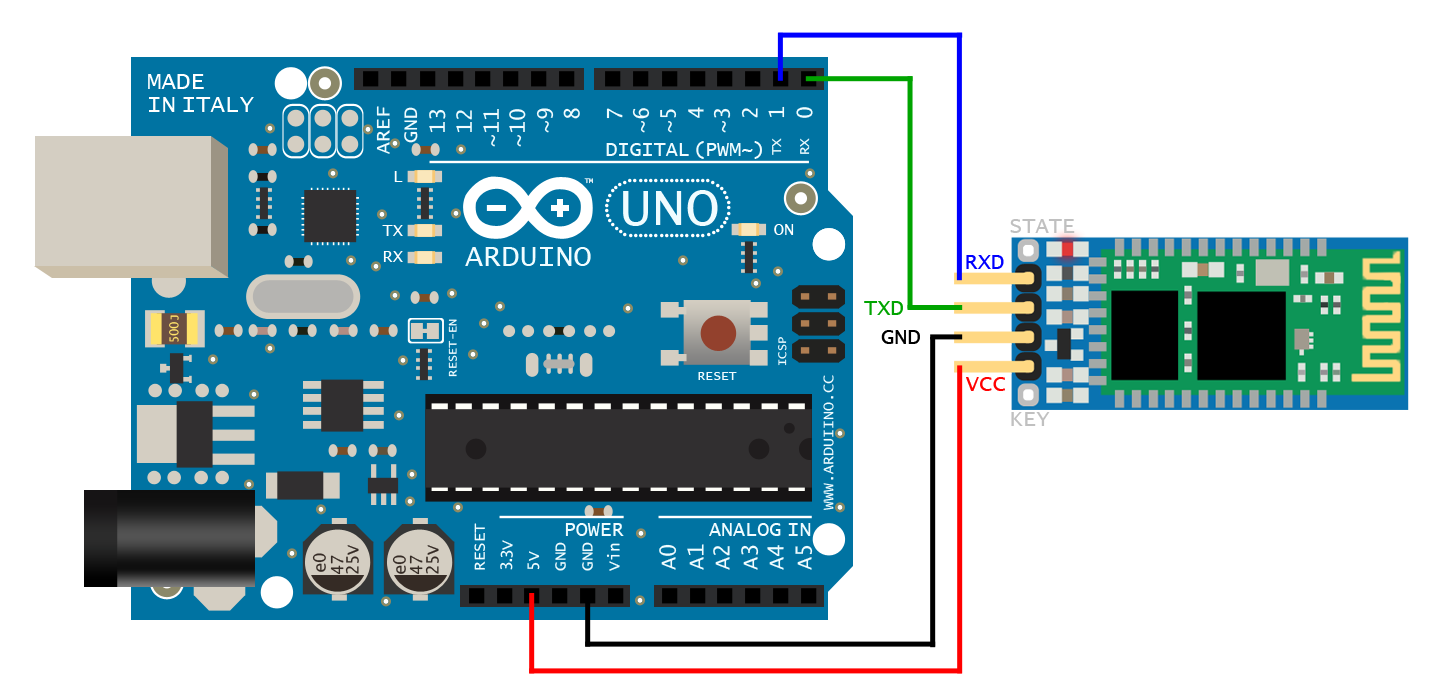
byte code3 = mfrc522.uid.uidByte[3];

Serial.println(code3,HEX);

We kunnen nu de ID in een string zetten en verder uitlezen. Met de info “byte size” halen we het aantal bytes, welke we kunnen gebruiken om met een “for(int i=0; i<size; i++)” het juiste formaat te uitlezen.

Ik laat dit voorlopig even aan degene die meer tijd heeft…

### 3.4.3 Bluetooth met een serial connection (TX en RX)

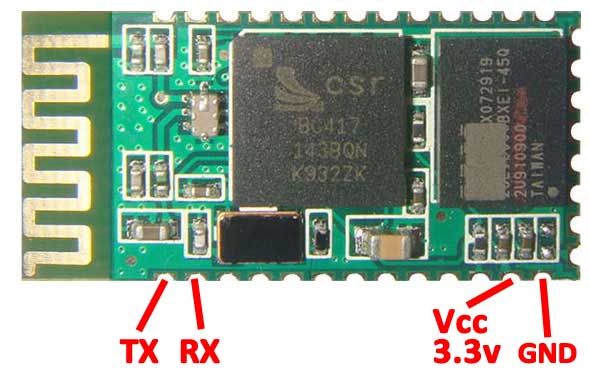
Tot hiertoe werkten we met een draadverbinding, met BT (Bluetooth) gaan we verder en kunnen hiermee gegevens uitwisselen met PC, (smart-)phone en zelfs met een andere Arduino. Laten we in eerste instantie eens een verbinding met de PC maken. Uit het rond snuisteren op fora vond ik dat het paswoord 1234 is van de module, soms ook 12345 (Arduino Bluetooth-board). Of als je een BlueSmirf –model hebt is dit “default”

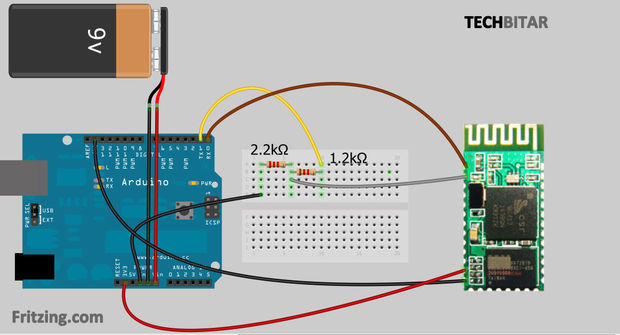
Het model dat ik gebruik is een “JY-MCU” bordje met een HC06 submodule op. Datasheet van de module: <http://www.linotux.ch/arduino/HC-0305_serial_module_AT_commamd_set_201104_revised.pdf>

Je kan de module in drie modes zetten, Master, Slave en Loopback. Voor meer details hierover verwijs ik naar de datasheets. En hou dit voorlopig even buiten de context van dit werk. Nog meer uitleg over deze modules : <http://wiki.pinguino.cc/index.php/SPP_Bluetooth_Modules>

Deze dingen hebben, voor ons althans, een nadeel, ze werken op 5V, maar de signalen mogen maar 3V3 hebben. We moeten dus het veiligst werken met levelshifters. Voor minder dan een euro heb je een Oosterse versie, maar een spanningsdeler op de TX-pin van de Arduino help ook al. Ook belangrijk is te weten wat TX en RX zijn, naast de betekenis TX, transmit of verzenden en RX receive of ontvangen, moet je ook opletten vanuit welk standpunt je dit bekijkt. Wat voor de Arduino TX is, is RX voor de Bluetooth-module, en RX op de Arduino is de TX voor de Bluetooth print.

De eigenlijke module is zoals de figuur hieronder, maar wordt op een drager gezet die o.a. zorgt voor de power en filtering. De module zelf werkt op 2.4GHz, dit is zeer gevoelig, en dan bedoel ik zeer gevoelig. Ook een reden om deze in te pakken in een krimpkous. De antenne komt naar buiten maar het is belangrijk dat je er niet ~~te veel~~ aankomt.

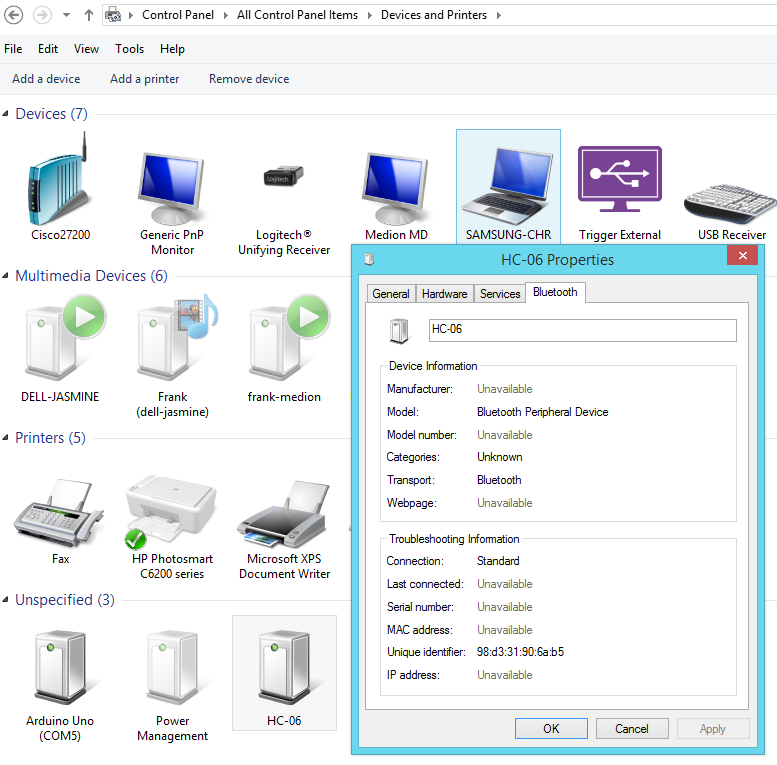




Nog maar een waarschuwing: aangezien de Arduino zijn sketches via de TX en RX pinnen ontvangt via de seriële communicatie, kan je dus niet gelijktijdig de BT-module aansluiten. M.a.w. moet je eerst de sketch uploaden en dan pas de connectie maken met je schakeling. Er is een mogelijkheid om dit te omzeilen door andere pinnen als TX en RX voor de module te definiëren. Anderzijds, eens geprogrammeerd maakt het niet veel meer uit…

#### ***3.4.3.1 Ontdekken van de modul***e

Wanneer we de voeding aansluiten kunnen we al een eerste test doen. Let wel, ik heb nog geen sketch opgeladen en de TX/RX verbinding is er ook nog niet. Op mijn laptop ga ik op zoek naar een bluetooth device. En ja, daar ist ie. De passkey was inderdaad 1234 en het dingetje heet HC-06. We weten dus dat dit deel al werkt. En communiceert op poort COM8 (voor moest dit later nodig zijn). Pas op, dit is de Bluetooth-poort, niet de Arduino poort!



Uit nieuwsgierigheid probeerde ik ook connectie te maken met mijn tablet (Andriod) en ja het werkt. Ik heb hierop een terminal app gezet en kan nu communiceren met de module.

De sketch:

char INBYTE;

int LED = 13; // LED on pin 13

void setup() {

Serial.begin(9600);

pinMode(LED, OUTPUT);

}

void loop() {

Serial.println("Press 1 to turn Arduino pin 13 LED ON or 0 to turn it OFF:");

while (!Serial.available()); // stay here so long as COM port is empty

INBYTE = Serial.read(); // read next available byte

if( INBYTE == '0' ) digitalWrite(LED, LOW); // if it's a 0 (zero) tun LED off

if( INBYTE == '1' ) digitalWrite(LED, HIGH); // if it's a 1 (one) turn LED on

delay(50);

}

Op de tablet komt de tekst: "Press 1 to turn Arduino pin 13 LED ON or 0 to turn it OFF:"

En ja een 1 doet de LED branden, een 0 doet ‘m uit.

Opmerking: het kan niet genoeg gezegd worden: VERGEET NIET DE VERBINDING RX en TX weg te nemen wanneer we uploaden ! Je krijgt anders een pak errors die nergens op slaan, dus “volg je even niet “ trek dan die verbindingen los…

Zoals altijd is het nuttig er iets mee te doen, om het programma te manipuleren zodat de info verder kan gebruikt worden. Ook hier geldt dat dit als aanzet dient en in geval van overschot van tijd er gerust verder mag geëxperimenteerd worden.

char INBYTE;

int LED = 13; // LED on pin 13

int red = 12; // extra ledje op pin 12

void setup() {

Serial.begin(9600);

pinMode(LED, OUTPUT);

pinMode (red,OUTPUT);

}

void loop() {

Serial.println("Press 1 to turn Arduino pin 13 LED ON or 0 to turn it OFF:");

while (!Serial.available()); // stay here as long as COM port is empty

INBYTE = Serial.read(); // read next available byte

if( INBYTE == '0' ) digitalWrite(LED, LOW); // if it's a 0 (zero) turn LED off

if( INBYTE == '1' ) digitalWrite(LED, HIGH); // if it's a 1 (one) turn LED on

if( INBYTE == '2') digitalWrite(red, HIGH); // if it's a 1 (one) turn LED on

if( INBYTE == '3') digitalWrite(red, LOW); // if it's a 0 (zero) turn LED off

if( INBYTE == '4') Blink();

Serial.write(INBYTE); // print op de tablet het getal dat is ingetypt

Serial.write(" "); // wit plaatske

int Som = INBYTE+50; // tel 50(ASCII) op bij dit getal

Serial.write(Som); //schrijf het resultaat

Serial.write(" "); //wit plaatske

int dec = (Som, DEC); //zet het resultaat om naar een DECimaal getal

Serial.write(dec); //schrijf dit decimal getal naar de tablet

Serial.write(" ");

delay(50); // wacht effe

}

void Blink() // knipper twee keer

{digitalWrite(LED, HIGH); // turn the LED on (HIGH is the voltage level)

delay(1000); // wait for a second

digitalWrite(LED, LOW); // turn the LED off by making the voltage LOW

delay(1000);

digitalWrite(LED, HIGH); // turn the LED on (HIGH is the voltage level)

delay(1000); // wait for a second

digitalWrite(LED, LOW); // turn the LED off by making the voltage LOW

delay(1000);}

Het resultaat is zoals verwacht, geen hoogdravende technologie, maar toch…

Op breadboard branden de LEDs of gaan ze uit, ook bij een druk op ‘4’ gaat de LED 2 keer knipperen. Deel 2 van het programma maakt een berekening van de input en geeft het resultaat weer op de tablet. Bij input van een 1 komt er een ‘c’ als antwoord, dit is inderdaad 50 posities verder in de ASCII-tabel.

### 3.4.4 Twee Arduino’s

Het had tof geweest moest ik nog te tijd hebben gehad om twee Arduino’s met elkaar te laten praten. Op verschillende manieren, enerzijds met een draadverbinding en anderzijds met bluetooth.

Op internet is het een en ander hierover te vinden, maar de uitwerking en vooral het uitpluizen wat er gebeurt in de sketch is niet van gekomen. Graag werk ik dit nog wel eens uit in een vervolg van dit werk.

<http://www.instructables.com/id/I2C-between-Arduinos/>

### 3.4.5 RFID lezer met display

We voegen de besproken modules samen, RFID lezer en de LCD-display. Dit geeft een handzaam toestel. Voegen we bluetooth toe dan kan een PC de gegevens verwerken.

Maar ook hier laat ik dit aan iemand met meer tijd, de aanzet is gegeven de uitwerking moet nog gedaan worden.

# BRONNEN

Er zijn veel bronnen geraadpleegd. Met telkens de volledige versie van de besproken interfaces. Zoals je ziet is er zeer veel van internet geplukt.

Het feit dat ik dit werk heb gemaakt heeft me veel zaken bijgebracht. Wetenschap die ik bezat maar die zeer ver in een verloren hoekje van mijn geheugen zat, tot echt nieuwe dingen. Door de opgedane kennis, de “verplichting” dit te moeten doen, en de honger naar een werkend projectje zorgt voor de fun die waarschijnlijk ook bij iemand anders de FUNduino deed ontwikkelen: <http://funmetelectronica.nl/funduino-boards>

<https://nl.wikipedia.org/wiki/I%C2%B2C-bus>

<https://www.arduino.cc/en/Reference/Serial>

<https://nl.wikipedia.org/w/index.php?title=FireWire&redirect=no>

<https://nl.wikipedia.org/wiki/Serial_Peripheral_Interface>

<https://nl.wikipedia.org/wiki/TCP/IP>

<https://nl.wikipedia.org/wiki/Ethernet>

<https://nl.wikipedia.org/wiki/DSL>

<https://nl.wikipedia.org/wiki/Integrated_Services_Digital_Network>

<https://nl.wikipedia.org/wiki/Universal_Serial_Bus>

<https://nl.wikipedia.org/wiki/Local_area_network>

<https://nl.wikipedia.org/wiki/Controller_Area_Network>

<https://en.wikipedia.org/wiki/CAN_bus>

<http://www.ftdichip.com/index.html>

<https://www.arduino.cc/en/reference/wire>

<https://nl.wikipedia.org/wiki/Bluetooth>

<https://nl.wikipedia.org/wiki/IrDA>

<https://nl.wikipedia.org/wiki/Draadloos_netwerk>

<https://nl.wikipedia.org/wiki/ZigBee>

<https://nl.wikipedia.org/wiki/Near_field_communication>

<https://nl.wikipedia.org/wiki/Radio-frequency_identification>

<https://nl.wikipedia.org/wiki/MIFARE>

<https://nl.wikipedia.org/wiki/Wi-Fi>

<https://nl.wikipedia.org/wiki/X10>

<http://www.nxp.com/documents/data_sheet/PCF8574_PCF8574A.pdf>

<http://playground.arduino.cc/Main/I2cScanner>

<http://arduino.stackexchange.com/questions/3042/i2c-2-way-communication-between-arduino-uno-and-arduino-mega>

<http://www.nxp.com/documents/data_sheet/MFRC522.pdf>

<http://nl.aliexpress.com/item/Two-Channel-IIC-I2C-Logic-Level-Converter-Bi-Directional-Module-5V-to-3-3V/32435434792.html?s=p>

<https://www.youtube.com/watch?v=oGZizClfRug>

<http://playground.arduino.cc/Learning/MFRC522>

<https://github.com/miguelbalboa/rfid>

<http://robotosh.blogspot.be/2012/07/arduino-jy-mcu-bluetooth.html>

<https://arduino-info.wikispaces.com/LCD-Blue-I2C>

<http://forum.arduino.cc/index.php?topic=214356.0>

<http://playground.arduino.cc/Main/InterfacingWithHardware>

<http://www.instructables.com/id/Cheap-2-Way-Bluetooth-Connection-Between-Arduino-a/?ALLSTEPS>

<http://robotosh.blogspot.be/2012/07/arduino-jy-mcu-bluetooth.html>

<http://www.mitchellpage.com.au/research/?p=263>

<http://forum.arduino.cc/index.php?topic=256260>

<http://www.instructables.com/id/Arduino-RFID-Door-Lock/?ALLSTEPS>

<https://sites.google.com/site/arduinomega2560projects/home/level-1/arduino-rfid-rc522>

<http://tronixstuff.com/2010/10/20/tutorial-arduino-and-the-i2c-bus/>

<https://learn.sparkfun.com/tutorials/i2c>

<http://blog.nearfuturelaboratory.com/2007/01/11/arduino-and-twi/>

<https://www.arduino.cc/en/Reference/Wire>

<https://github.com/omersiar/RFID522-Door-Unlock/blob/master/NoSerial/NoSerial.ino>

<https://community.particle.io/t/getting-the-rfid-rc522-to-work-solved/3571>

<https://dangerousthings.com/wp-content/uploads/2013/12/PN532_-Manual_V3.pdf>

<https://www.addicore.com/v/vspfiles/downloadables/Product%20Downloadables/RFID_RC522/RFIDQuickStartGuide.pdf>

<http://fablabamersfoort.nl/en/node/173>

<http://www.jeremyblum.com/2011/07/08/tutorial-12-for-arduino-rfid-card-reading/>

<https://www.youtube.com/watch?v=XJjOZpdOcqk>

nog een leuk dingetje:

<https://www.youtube.com/watch?v=sD1XfVCltd0>