# **Installatie Handleiding**

# **Alarm IP-Converter**

Document Versie 2.22

Software Versie 3.05 OEM ASB Alleen vanaf Hardware versie 1.2

### Artikelen:

- IPC-GPRS Alarm IP-Converter in Kunststof Behuizing
- IPC-GPRS Alarm IP-Converter PCB
- IPC-Comfort Alarm IP-Converter Comfort in Kunststof Behuizing
- IPC-Comfort Alarm IP-Converter PCB
- IPC-Easy Alarm IP-Converter Comfort in Kunststof Behuizing
- IPC-Easy Alarm IP-Converter PCB

### Accessoires:

- · Universele Kunststof Behuizing Inclusief Sabotage
- S-Blade Interne GPRS-Antenne
- Buitenantenne GPRS met Montagebeugel
- 5 Meter Verlengset GPRS-Antenne
- 10 Meter Verlengset GPRS-Antenne
- 20 Meter Verlengset GPRS-Antenne





### ATTENTIE

De Alarm IP-Converter is helemaal getest en voorzien van de laatste software. Wij adviseren echter om bij installatie nog een keer te controleren of er een nieuwere software versie beschikbaar is voor u. U doet dit door de procedure te volgen zoals beschreven in hoofdstuk "Remote software update" van deze handleiding.

Environmental Class: II Certification Body: 0560 Manufactory Name: ASB-Security BV NEN-EN 50136-2:2011, NEN-EN 50136-1-1:1998, NEN-EN 50136-1:2012, NEN-EN 50136-2-1 ATS classes (NEN-EN 50136-1-1:1998): ATS1, ATS2, ATS3, ATS4, ATS5, ATS6 ATS categories (NEN-EN 50136-1:2012) : SP1,SP2,SP3,SP4,SP5,SP6, DP1,DP2,DP3,DP4

REQ registratie: REQ0182

INCERT certified: C03200475

**C** Dit product, Alarm IP-Converter, voldoet aan de volgende bepalingen van de EG richtlijnen: EMC richtlijn 89/336/EEG, Laagspanningsrichtlijn 73/23/EEG

Copyright © 2012 ASB-Security BV

Het is niet toegestaan dit document in zijn geheel of gedeeltelijk te kopiëren of op andere wijze te reproduceren zonder schriftelijke toestemming vooraf van ASB-Security BV.



# Inhoudsopgave

1 Introductie	5
2 Kenmerken IP-Converter	6
2.1 Algemeen	6
2.2 Kenmerken	6
2.3 Uitvoeringen	6
3 Installatie	7
3.1 Uitpakken	7
3.2 Voorbereiding	7
3.3 Plaatsen	7
3.4 Aansluitgegevens	7
3.5 Beschrijving aansluitpunten	8
3.6 Hardware configuratie Jumper settings	9
3.7 GPRS SIM kaart	10
3.8 LED-display	10
3.9 LED-indicaties	12
3.10 Druktoets	12
3.11 Remote software update	13
4 Configureren IP-Converter (IPC)	14
4.1 Inleiding	14
4.2 Configureren via Web Interface	14
4.2.1 Cross-over netwerkkabel	14
4.2.2 Het IP-adres van de IP-Converter	14
4.2.3 Instellen IP-adres van PC	14
4.2.4 Web Interface login	15
4.2.5 Web Interface Configuratie - IP Parameters	15
4.2.6 Web Interface Configuratie - RCT Parameters	17
4.2.7 Web Interface Configuratie - Advanced GPRS Parameters	19
4.2.8 Web Interface Configuratie - Alarm Interface	20
4.2.9 Web Interface Configuratie - I/O (Input/Output)	21
4.2.10 Web Interface Configuratie – Advanced PSTN Interface	22
4.2.11 Web Interface Configuratie – SIP Parameters	23
4.2.12 Web Interface Configuratie – Advanced Sip Parameters	24
4.2.13 Web Interface Configuratie - Security	25
4.2.14 Web Interface Configuratie - Date & Time	25
4.2.15 Web Interface Configuratie – Maintenance (Onderhoud)	26
4.2.16 Web Interface - Diagnostics	27
4.2.17 Web Interface - Alarm buffer weergave	28
4.2.18 Web Interface - Log weergave	28
4.2.19 Web Interface - Help weergave	29
4.3 GSM / GPRS modem.	29
5 Specificaties	30
5.1 Technische aeaevens	30
5.2 PSTN-protocollen ( zie BIJLAGE voor geteste panelen).	30
5.3 Seriële interfacing ( zie BIJLAGE voor geteste panelen)	
5.3.1 Aritech CD3401 V1.4 / CD150.01 V 6.22:	30
5.3.2 GALAXY 8 <sup>.</sup>	31
5.3.3 NX 8 <sup>.</sup>	32
5.3.4 DSC PANELEN (DVACS MODULE)	33
5.3.5 ATS3000, 4000, 4500 (Vanaf V04.06.44)	
5.4 Antenne	
6 KORTE INI FIDING IP	
6 1 Inleiding	36
6.2 Het OSI-model	
6.3 De lagen 1 en 2	
6.4 IP. Adressering en netwerkklassen	
6.5 Switches, routers en hubs	
6.6 Routering	
6 7 DNS	42
6.8 Protocollen / Poortnummers	42 42
7 Algemene informatie	ΔΔ
8 BIJI AGE A Geteste nanelen	
9 BLILAGE B Frequently Asked Questions	∓3 ⊿7
	+/

10 BIJLAGE C Poorten Overzicht	48
11 BIJLAGE D Inbedrijfstelling	49
12 BIJLAGE E Flowchart Inbedrijfstelling	50
13 BIJLAGE E ATS 1 t/m 6 configuratie	51



# 1 Introductie

De informatie in dit handboek stelt u in staat de Alarm IP-Converter (IPC) te programmeren en te installeren.

Het gebruik van DSL en IP-netwerken neemt steeds meer toe omdat de communicatiekosten verlaagd worden en het aantal toepassingen wordt verhoogd. Integratie van applicaties over één communicatielijn zorgt tevens voor lagere operationele kosten in de organisatie. De verbinding kan optimaal worden gebruikt voor bijvoorbeeld alarmoverdracht, elektronisch betalen (pinnen), bellen (IP-telefonie) en centraal opgestelde applicaties.

Met behulp van de Alarm IP-Converter van ASB-Security B.V. kunnen alarmmeldingen van uw beveiligingssysteem via een IP/VPN netwerk op een veilige, gegarandeerde manier naar een Particuliere Alarm Centrale (PAC) worden verstuurd.

De Alarm IP-Converter wordt in deze handleiding regelmatig afgekort met IPC.

# 2.1 Algemeen

Met behulp van de Alarm IP-Converter van ASB-Security B.V. kunnen alarmmeldingen van uw beveiligingssysteem via een IP/VPN netwerk op een veilige, gegarandeerde manier naar een Particuliere Alarm Centrale worden verstuurd (conform NEN-EN 50136 1/2).

De IP-Converter is via PSTN (Analoge lijn) te koppelen met het beveiligingssysteem. Op deze wijze kunnen de meldingen transparant naar een PAC worden verstuurd. Het is ook mogelijk het beveiligingssysteem serieel te koppelen. Optioneel kan worden gekozen voor een GPRS back-up mogelijkheid.

# 2.2 Kenmerken

- Alarmtransmissie conform NEN-EN 50136-1-1:1998 (ATS1 AT6) en NEN-EN 50136-1:2012 (SP1-SP6 en DP1-DP4)
- Toepasbaar op IP/VPN Internet
- 13VDC gevoed vanuit het beveiligingssysteem
- GPRS-backup (optioneel)
- · Flash-prom technologie
- · Analoog koppelvlak voor beveiligingssystemen met analoge kiezer
- Gestandaardiseerde protocollen SIA en CID ondersteund (zie BIJLAGE voor geteste systemen)
- Serieel koppelvlak voor beveiligingssystemen (BIJLAGE voor geteste systemen)
- · Locale diagnose via 7-segment display en diverse LED indicaties.
- · IP-adres ontvanger, handmatige invoer of via het telefoonnummer van de kiezer
- · Configuratie via web interface
- · Paswoord beveiligd (voor web toegang)
- Alarmbuffer van 50 posities, incl. datum/tijd, PAC IP-adres en status. Deze zijn uit te lezen via Web Interface. De status geeft weer of het betreffende alarm al bevestigd is
- Default configuratie die in 90% van de gevallen zal functioneren zonder dat daarbij instellingen door de gebruiker/installateur nodig zijn (Comfort/Easy markt)
- DHCP ondersteuning
- PSTN lijn monitoring

# 2.3 Uitvoeringen

Er zijn een aantal uitvoeringen van de IP-Converter beschikbaar:

- IP-Converter Comfort
- IP-Converter Easy
- IP-Converter GPRS

Afhankelijk van het toegepaste type IP-Converter zijn de volgende opties beschikbaar:

	IPC-Easy	IPC-Comfort	IPC- GPRS
Interface	Analoog koppelvlak	Analoog koppelvlak	Analoog en serieel koppelvlak
PSTN lijn monitoring	X	V	V
GPRS Back-up	Х	Х	V
PSTN Back-up	Х	Х	V
Up/Downloading naar Alarm Paneel	Х	V	V
Verification of Performance (VoP)	Х	V	V
Zone ingang (b.v. voor tamper schakelaar)	Х	Х	V
Uitgang (FTC primaire/secundaire verbinding)	Х	Х	V



# 3 Installatie

## 3.1 Uitpakken

In de verpakking treft u aan:

- De Alarm IP-Converter
- Deze installatiehandleiding
- Shielded CAT5 UTP netwerkkabel
- 18k/0,5W weerstand

# 3.2 Voorbereiding

Voordat u de Alarm IP-Converter kunt aansluiten moet u controleren of de volgende onderdelen aanwezig zijn:

- De IP-Converter
- 13VDC voedingspanning
- Werkende Internet/VPN aansluiting
- · Beveiligingssysteem met PSTN-kiezer of seriële koppeling
- PC (voor programmering IP-Converter)
- · Eventueel een cross-over netwerkkabel voor lokale programmering

# 3.3 Plaatsen

- Installatie dient alleen door de erkende vakman te gebeuren
- Installeer de IP-Converter zodanig dat hij te allen tijde goed bereikbaar is
- · Stel de unit niet bloot aan extreme warmte en/of direct zonlicht
- · Plaats de unit niet op een koude of vochtige plaats
- Plaats de unit niet direct naast een TV, radio, videorecorder of computer. Bewaar tenminste 50 cm afstand, om storing te voorkomen
- De kunststof behuizing heeft een afmeting bxhxd van 125x210x40 mm
- · Houdt rekening met ruimte voor aan- en afvoer van kabels aan boven- en onderzijde
- Bij gebruik van GPRS kunnen er mogelijk problemen zijn met het bereik. Bijvoorbeeld bij plaatsing in een kelder. Dit heeft impact op de dienstverlening. Mobiel geeft geen garanties op netwerken en heeft ook geen beschikbaarheidgegevens. Advies is bij installatie van de GPRS, met je (KPN) mobiel de bereikbaarheid te testen (aantal bereikbaarheidsstreepjes of GPRS data verkeer). Ook is het mogelijk om via het diagnosevenster in de browser af te lezen wat het ontvangst is.

# 3.4 Aansluitgegevens

Afbeelding: Aansluitgegevens IP-Converter



#### 3.5 Beschrijving aansluitpunten

# Voedingspanning (+13V en GND)

De voedingspanning t.b.v. de IP-Converter is 13 +1/-2 VDC. De voedingskabel mag niet langer zijn dan 30 meter. Het stroomverbruik bedraagt:

- · Comfort/Easy uitvoering: 150-200 mA
- GPRS uitvoering: 170-280mA

### **Ingang IN**

Deze ingang kan geactiveerd worden door het aanbrengen van een 0 VDC spanning (kortsluiten naar GND). Dit is een Normaal gesloten contact (NC). Op de Ingang IN zijn geen EMC testen uitgevoerd, en daarom valt deze ingang niet onder de certificatie

### **Uitgang OUT**

Deze uitgang is een open collector uitgang die naar massa (0 VDC) geschakeld is. Als de uitgang actief is, wordt deze uitgang hoog. De te schakelen apparatuur (Z) wordt aangesloten tussen de klem 'OUT' en de positieve voedingsspanning +13 VDC. De uitgang kan maximaal 50 mA stroom leveren. De werking van deze uitgang wordt bepaald in de programmering. De uitgang zal actief worden wanneer de PAC bereikbaar is. Op de uitgang UIT zijn geen EMC testen uitgevoerd, en daarom valt deze uitgang niet onder de certificatie.

### Ethernet

De LAN, of Ethernet netwerk interface voldoet volledig aan de IEEE 802.3 / IEEE 802.3 u 10Base-T / 100Base-TX standaard. De Interface ondersteunt MDI/MDI-X auto cross-over functie (Auto-MDI), wat wil zeggen dat zowel een "rechte" als "cross-over" verbindingskabel kan worden toegepast.

### OPMERKING: Auto-MDI staat standaard uit. Met jumper J16 kan dit geactiveerd worden.

Afbeelding: Ethernet interface



# Receive -Serieel RS232/RS485

6

De IP-Converter beschikt over een RS232/RS485 communicatie poort, de functie van deze poort (RS232 of RS485) kan worden ingesteld met jumper J12.

Voor de RS232 configuratie dient u de aansluitklemmen Rx, Tx, en GND te gebruiken.

Voor de RS485 configuratie dient u de aansluitklemmen A, B, en GND te gebruiken (in deze versie niet van toepassing). Op de seriële poort zijn geen EMC testen uitgevoerd, en daarom valt deze poort niet onder de certificatie

### Tip & Ring

De Tip en Ring aansluitklemmen zijn de aansluitklemmen voor de modemkiezer van het alarm paneel. Gebruik hiervoor een norm88 telefoonkabel of een kabel met dezelfde specificaties (0,5 mm2 kern).

De lijnspanning zal wegvallen onder de volgende omstandigheden:

- Lokale ethernet verbinding is niet aanwezig en er is een FTC geconstateerd op de backup verbinding.
- Comfort/Easy uitvoering: Bij constatering van een FTC indien de lokale internet verbinding niet aanwezig is.



### Tip' & Ring'

Op de Tip' en Ring' aansluitklemmen kan een bestaande analoge (PSTN) lijn worden aangesloten (voor back-up toepassing). Gebruik hiervoor een norm88 telefoonkabel of een kabel met dezelfde specificaties (0,5 mm2 kern). Let op: De instellingen van de IP-Converter worden niet gebruikt bij de PSTN back-up interface. Alleen de instellingen van het alarm paneel worden gebruikt.

# 3.6 Hardware configuratie Jumper settings

### Afbeelding: Jumpers IP-Converter



De jumpers op de IP-Converter hebben de volgende betekenis: *Tabel : Betekenis van de verschillende jumpers op de IP-Converter* 

Jumper	Betekenis	Fabrieksinstelling
J3	Reset (Herstart)	Niet geplaatst
J8	Pull up 750 Ω RS485	Optioneel
<b>J</b> 9	Afsluitweerstand 120 $\Omega$ RS485	Optioneel
J11	Pull down 750 Ω RS485	Optioneel
J12	RS485 / RS232 instelling	Geplaatst als RS232 instelling
J16	Auto-MDI functie Ethernet poort	Niet geplaatst = functie gedeactiveerd

### Jumper J3

Door deze jumper kortstondig kort te sluiten kunt u de IP-Converter herstarten.

### <u>Jumper J8 + J11</u>

Deze jumpers zijn van toepassing indien de seriële poort als RS485 poort wordt geconfigureerd. Om een juist referentie niveau op de bus te creëren moeten de "Pull up  $750\Omega$ " en "Pull down  $750\Omega$ " jumpers geplaatst worden.

### Jumper J9

Ook deze jumper is alleen van toepassing indien de seriële poort als RS485 poort wordt geconfigureerd. Een RS485 bus dient aan twee zijden te worden afgesloten. Het doel van de afsluiting dient ervoor om reflecties tegen te gaan. Met deze jumper plaats u de afsluitweerstanden aan IP-Converter zijde.

### Jumper J12

Met behulp van deze jumper wordt bepaald of de aanwezige seriële poort volgens het RS232 of RS485 protocol functioneert.

Afbeelding: RS485 RS232









### Jumper J16

Met behulp van deze jumper kan de "Auto cross-over" functie van de Ethernet poort worden ge(de)activeert. Door het plaatsen van de jumper wordt de "Auto cross-over" functie geactiveerd.

### OPMERKING: Geadviseerd wordt deze functie uitgeschakeld te laten. De jumper dient dus niet te worden geplaatst.

#### 3.7 **GPRS SIM kaart**

RS485

### **SIM Abonnement**

Maak gebruik van een SIM kaart met abonnement. OPMERKING: Pre-paid kaarten kunnen niet gebruikt worden.

### **SIM Plaatsen**

Maak voor het verwisselen van de GPRS SIM kaart de IP-Converter spanningsloos. Schuif de GPRS SIM kaart op de aangegeven plaats zoals afgebeeld in de modem. U kunt de kaart nu voorzichtig doordrukken tot deze uit zichzelf vergrendeld. De kaart kan verwijderd worden door de kaart een klein stukje in de modem te drukken. Vervolgens kan de kaart uit de modem worden gehaald.

Afbeelding: Plaatsen GPRS SIM Kaart



#### **LED-display** 3.8

Het 7-segment display op de IP-Converter geeft exact weer wat de status van het apparaat is. In normale toestand geeft het display de zgn. 'Moving Worm' weer hetgeen aanduidt dat het apparaat normaal functioneert. Afbeelding: Illustratie van een zgn. 'Moving Worm'



In geval van storingen of in geval dat tussenkomst van een installateur gewenst is kunnen er in het display verschillende codes verschijnen. ledere code bestaat uit een combinatie van een letter en een cijfer tussen 0 en 9. Het display toont beurtelings de letter en het cijfer. Aan de hand van de volgende tabel kunt u bepalen wat de verschillende codes betekenen en hoe de vereiste actie luidt:

Tabel: Betekenis van de codes in het LED display op de IP-Converter

Code	Betekenis	Vereiste Actie
Moving Worm	Normaal bedrijf	Geen
U	Opstart procedure	Geen
u	Opstart procedure software update	Geen
xx-xx-xx	Versienummer	Geen*
Dec. Punt continu	Primaire en Secundaire PAC bereikbaar	Geen
Dec. Punt knipperend	Primaire of Secundaire PAC niet bereikbaar	Afhankelijk van error code
Dec. Punt uit	Primaire en Secundaire PAC niet bereikbaar	Afhankelijk van error code

С	Communicatie via Analoge poort	Geen
С	Software update	Geen
Exx	Foutcode	Zie tabel foutcodes

\* Na opstarten zal de Software versienummer van de IP-Converter kort worden weergegeven.

Tijdens opstarten wordt de configuratie gelezen en geactiveerd. Op dit moment worden ook een aantal tests uitgevoerd om de geldigheid en de werking van de configuratie vast te stellen. De volgende tabel geeft een opsomming weer van mogelijke fouten die kunnen optreden. Sommige fouten kunnen meteen na opstarten worden vastgesteld. Een fout wordt onmiddellijk in het LED display weergegeven met een 'E' gevolgd door het nummer. ledere fout heeft bovendien een prioriteit zodat alleen de fout met de hoogste prioriteit (1 is het hoogste) wordt weergegeven. Bij opstarten worden alle fouten opgeheven en worden de tests opnieuw doorlopen. Tijdens normaal bedrijf worden fouten ook onmiddellijk gedetecteerd en weergegeven.

### Tabel: Betekenis van de foutcodes

Fout code	Omschrijving	Prioriteit
E01	MAIN: Ethernet Link	1
E02	MAIN: Geen IP-adres van de DHCP server	2
E03	MAIN: Geen juist IP-adres geconfigureerd	3
E04	MAIN: Geen juist Subnet Mask	4
E05	MAIN: Geen juist Default Gateway IP-adres	5
E06	MAIN: Default Gateway niet bereikbaar	6
E07	MAIN: IP conflict op het LAN	7
E08	MAIN: Geen juist PAC IP-adres geconfigureerd	8
E09	MAIN: Geen juist PAC IP-adres van paneel gekregen	9
E10	MAIN: Geen verbinding met de alarm ontvanger mogelijk	10
E11	MAIN: Ack Timeout	11
E12	PSTN: Paneel kiest niet (timeout na of-hook)	12
E13	PSTN: Paneel stuurt geen data (timeout na kiezen)	13
E14	PSTN: Ongeldige data van paneel gekregen Algemene fout code	14
E15	MAIN: Geen route voor dit klantnummer	15
E16	MAIN: Failed To Connect	16
E33	BACKUP: GPRS PUK code vereist	17
E34	BACKUP: GPRS SIM kaart probleem	18
E35	BACKUP: GPRS Niet geregistreerd op het netwerk	19
E36	BACKUP: GPRS Kan helemaal geen verbinding maken	20
E37	BACKUP: Geen juist IP-adres geconfigureerd	21
E38	BACKUP: Geen juist Subnet Mask geconfigureerd	22
E41	BACKUP: Geen juist PAC IP-adres geconfigureerd	23
E43	BACKUP: Geen verbinding met alarm ontvanger mogelijk	24
E44	BACKUP: Ack Timeout	25
E48	BACKUP: Geen route voor dit klantnummer	26
E49	BACKUP: Failed To Connect	27
E65	SERIEEL: Geen verbinding	28
E66	SERIEEL: Verkeerd klantnummer geconfigureerd	29





# 3.9 LED-indicaties

De diverse LED's op de IP-Converter helpen u bij het vaststellen van de correcte werking cq. toestand van de IP-Converter.

Afbeelding: LED indicaties IP-Converter



#### Tabel: Betekenis van de indicaties LED's op de IP-Converter

Led	Kleur	Betekenis	Gewenste toestand
D3	Groen	Voeding PCB	Aan
D7	Groen	Voeding GPRS-modem	Aan
D8	Geel	PSTN status	-
D9	Groen	Watchdog timer LED	Aan/knipperend
D10	Rood	GPRS status	- (Aan bij verbonden met GPRS netwerk)
D14	Rood	PSTN back-up actief	-
D15	Rood	Uitgang status	-
D16	Geel	LAN 100MB	Aan (bij 10Mb uit)
D17	Groen	LAN Link up	Aan/knipperend
D20	Groen	GPRS-Netwerk info	Zie beschrijving <b>D20</b>

Tabel: D20 GPRS indicaties voor netwerk beschikbaarheid

Deze LED geeft informatie betreffende de netwerkbeschikbaarheid en belstatus.

D20 LED status	Modem status
Uit	Modem is uitgeschakeld
Snel knipperend (Periode van 1s, 0.5s aan)	Netwerk zoeken / niet aangemeld
Langzaam knipperend (Periode van 3s, 0.3s aan)	Aangemeld, volledig operationeel
Aan	Modem verstuurt data

Nu de functie van de diverse indicaties bekend zijn kan de IP-Converter worden geconfigureerd.

Stel voor het testen van alarmsituaties wel de PAC hiervan op de hoogte!

### 3.10 Druktoets

Met de druktoets op de IP-Converter kunnen een aantal functies worden geselecteerd. Deze kunnen worden geselecteerd door achtereenvolgens een aantal keren op de toets te drukken.

De cyclus is als volgt: I ===F ===A ===H ===S ===t Moving worm

LET OP!: Nadat u een selectie heeft gemaakt moet u wachten totdat de gekozen optie stopt met knipperen. Pas dan is de selectie geldig.



Hieronder volgt een beschrijving: **I = IP-adres weergave:** Met behulp van deze optie kan het IP-adres en "Subnet mask" van de IPC zichtbaar gemaakt worden. Dit kan makkelijk zijn indien gebruik wordt gemaakt van DHCP.

De weergave is als volgt: IP= ... - ... - ... || ...

Voorbeeld: IP adres 192.168.1.200 met subnetmask 255.255.255.0 wordt weergegeven als: IP=192-168-001-200|| 24

**F** = Factory default: Deze functie maakt het mogelijk de IP-Converter terug te brengen naar fabrieksinstellingen. Nadat de optie "F" is geselecteerd zal deze nog enkele malen blijven knipperen en vervolgens 2 seconden continu oplichten, de IP-Converter is nu teruggebracht naar fabrieksinstelling. Na het factory default maken zal de IPC automatisch opnieuw opstarten.

**A = Clear Alarmbuffer:** Deze functie maakt het mogelijk de alarmbuffer van de IP-Converter leeg te maken. Na de optie "A" zal deze nog enkele malen blijven knipperen en vervolgens 2 seconden continu oplichten. De alarmbuffer is nu leeg.

**H = Help mode:** Om verbinding te maken met het technisch beheercentrum van ASB moet de IPC in de "H" stand worden gezet. Dit kan op verzoek van de operator van ASB-Security worden gedaan. De operator kan dan op afstand de instellingen van de IPC bekijken en eventueel helpen met het tot stand brengen van de verbinding. (RMS server 080.112.203.008)

**S = Save mode:** Om configuratie instellingen in de IP-Converter te kunnen wijzigen moet de IP-Converter in deze mode worden gezet. Dit is gedaan uit veiligheidsoverwegingen. Op deze manier zal lokaal toegang moeten worden verleend voordat (Web Interface) settings kunnen worden aangepast. Nadat de optie "S" is geselecteerd zal deze nog enkele malen blijven knipperen en vervolgens continu oplichten. De IP-Converter accepteert nu wijzigingen. Wacht totdat de selectie actief is en de 'S' gestopt is met knipperen! Voor de comfort en easy versie is de 'S' mode niet nodig om settings in de webpagina te wijzigen.

**t = Test mode:** Deze functie wordt gebruikt door ASB om de IP-Converter te testen tijdens productie. Gebruik deze functie niet, tenzij expliciet aangegeven door onze technische medewerkers.

# 3.11 Remote software update

Indien tijdens opstarten de druktoets ingedrukt wordt gehouden tot er een "c" verschijnt, zal de IPC verbinding proberen te maken met de update server om nieuwe software te uploaden. Bij remote software update maakt de IP-Converter geen gebruik van DHCP maar de laatst opgeslagen IP settings. Het is dus belangrijk dat de IPC van te voren een keer helemaal is opgestart. Het IP-adres van de update server wordt geprogrammeerd in de webpagina onder "Configuration → Maintenance". In het display verschijnt "U" gevolgd door "u" en "c", de decimale punt van het 7- segment display zal knipperen ter indicatie van de dataoverdracht. De upload tijd bedraagt afhankelijk van de snelheid van uw lijn circa 5 à 10 minuten.

LET OP: Tijdens remote update mag de IP-Converter niet spanningsloos gemaakt worden, omdat dit kan leiden tot permanente beschadiging van het flash geheugen.

**OPMERKING:** Voordat de software update uitgevoerd kan worden dient de IP-Converter eerst een keer helemaal te zijn opgestart.

Tabel: Foutcodes m.b.t. remote software update

Fout code	Omschrijving
E0	Niet de juiste software aanwezig op de update server
E99	Data upload fout
E98	Geen geldige update server settings

# 4 Configureren IP-Converter (IPC)

# 4.1 Inleiding

De IPC heeft een aantal vrij te programmeren parameters waarmee de werking van de IPC aan elke situatie kan worden aangepast. Alle parameters zijn opgeslagen in FLASH en worden ook bewaard tijdens de afwezigheid van de voedingsspanning.

De IP-Converter kan via de web interface geconfigureerd worden.

# 4.2 Configureren via Web Interface

Het configureren van de IP-Converter via de geïntegreerde Web Interface kan via een IP netwerk of rechtstreeks vanuit een PC naar de IP-Converter via een "rechte" als een "cross-over" netwerkkabel.

### 4.2.1 Cross-over netwerkkabel

Afbeelding: Penbezetting Cross-over kabel



### 4.2.2 Het IP-adres van de IP-Converter

Om verbinding te krijgen met de Web Interface dient u het IP-adres van de IP-Converter te weten.

• IP-adres uitlezen (zie hoofdstuk: Druktoets)

I = IP-adres weergave: Met behulp van deze optie kan het IP-adres en "Subnet mask" van de IPC zichtbaar gemaakt worden. Dit kan makkelijk zijn indien gebruik wordt gemaakt van DHCP. De weergave is als volgt: IP= ... - ... - ... || ...

• Voorbeeld IP-adres 192.168.1.200 met subnetmask 255.255.255.0 wordt: IP=192-168-001-200||24

# 4.2.3 Instellen IP-adres van PC

Om het IP-adres van uw laptop of PC te wijzigen gaat u als volgt te werk.

Kies bij de eigenschappen van de LAN-verbinding voor de eigenschappen van het Internet protocol (TCP/IP) en vul een vast IP-adres in. Het Subnetmasker zal automatisch ingevuld worden. Verder zijn er geen instellingen nodig. Klik 'OK' om de wijzigingen door te voeren. Let op: het IP-adres van de PC moet in hetzelfde netwerk als het IPadres van de IP-Converter zitten.

### Afbeelding: IP-adres PC wijzigen

Algemeen Verificatie Geavanceerd	Algemeen	
Verbinding maken via: Broadcom 440x 10/100 Integrated Controller	IP-instellingen kunnen automatisch deze mogelijkheid ondersteunt. Als netwerkbeheerder naar de geschi	h worden toegewezen als het netwerk s dit niet het geval is, dient u de kte IP-instellingen te vragen.
Configureren		en toewijzen
Deze verbinding heeft de volgende onderdelen nodig:	Het volgende IP-adres gebru	iiken:
ST NWLink NetBIOS	IP-adres:	192 . 168 . 191 . 100
3 NWLink IPX/SPX/NetBIOS-compatibel transportprotoc     1      1	<u>S</u> ubnetmasker:	255 . 255 . 255 . 0
<	Standaard-gateway:	
Installeren Verwijderen Eigenschappen	Automatisch een DNS-server     O De volgende DNS-serveradr	radres laten toe <u>w</u> ijzen essen ge <u>b</u> ruiken:
Transmission Control Protocol/Internet Protocol. Het	Voorkeurs-DNS-server:	
standaard-WAN-protocol dat communicatie biedt tussen verschillende, met elkaar verbonden netwerken.	Alternatieve DNS-server:	
Pictogram in systeemvak weergeven gedurende de verbinding		Geavangeerd
		OK Annulere

### 4.2.4 Web Interface login

Open een webbrowser op de PC en voer in de adresbalk het IP-adres van de IP-Converter in. In het venster verschijnt het inlogscherm van de IP-Converter.

Er zijn 2 manieren om in te loggen:

- 1. Admin: standaard paswoord: 'asb'
- 2. User: standaard paswoord: 'user'

Als user zijn niet alle schermen zichtbaar!

Bestand Bewerken Beeld Geschiedenis Bladwijzers Extra Help TP-Converter®   ASB-Security BV Meest bezocht Aan de slag Laatste nieuws & Aanbevolen websites & Web Slice-galerie IP-Converter® Login ] IP-Converter® requires < <i>Login&gt;</i> , please enter your credentials below. Login as Admin P Password proceed	🛿 IP-Converter®   ASB-Security BV - Mozilla Firefox 📃 🔲	
IP-Converter®   ASB-Security BV     Image: SearchEF 1.2 Customic	<u>B</u> estand Be <u>w</u> erken Beeld <u>G</u> eschiedenis Bl <u>a</u> dwijzers E <u>x</u> tra <u>H</u> elp	
Meest bezocht Aan de slag Laatste nieuws Anbevolen websites Web Slice-galerie          Image: Converter Con	IP-Converter®   ASB-Security BV     +	7
Meest bezocht Aan de slag Laatste nieuws Anbevolen websites Web Slice-galerie	♦ ♦ [①] http://192.168.10.159/cgi-bin/index.cgi	
[IP-Converter® Login] IP-Converter® requires < <i>Login&gt;</i> , please enter your credentials below. Login as Admin P Password	🧖 Meest bezocht 📋 Aan de slag 底 Laatste nieuws 🎉 Aanbevolen websites 🙆 Web Slice-galerie	
[IP-Converter® Login ] IP-Converter® requires < <i>Login</i> >, please enter your credentials below. Login as Admin ♥ Password		
[IP-Converter® Login] IP-Converter® requires <login>, please enter your credentials below. Login as Admin Password proceed</login>		
IP-Converter® Login ] IP-Converter® requires < <i>Login</i> >, please enter your credentials below. Login as Admin ♥ Password proceed	LID Convertor® Login 1	
IP-Converter® requires < <i>Login</i> >, please enter your credentials below. Login as <u>Admin</u> ♥ Password proceed	[ IP-Converter® Login ]	
IP-Converter® requires < <i>Login</i> >, please enter your credentials below. Login as <u>Admin</u> ♥ Password proceed	· · · · · · · · · · · · · · · · · · ·	
Login as Admin V Password proceed	IP-Converter® requires < <i>Login</i> >, please enter your credentials below.	
Password	Login as Admin 💌	
proceed	Password	
proceed		
	proceed	
Copyright © 2011 ASB-Security BV. All Rights Reserved	Copyright © 2011 ASB-Security BV. All Rights Reserved	
W3C THTML W3C CBB	W3C XHTML W3C CSS	

## 4.2.5 Web Interface Configuratie - IP Parameters

Na invoer van het juiste paswoord komt u in het configuratie scherm.

IP Parameters	
Enter the IP-Converter IP settings below LAN. If you choose to use DHCP, the in values do NOT represent the settings o	w. The IP settings can be automatically configured using DHCP. Make sure that a DHCP server is available on you nput boxes for IP adress, Subnet Mask and Default Gateway parameters will be disabled. If DHCP is enabled these bitained via DHCP.
DHCP enabled	
IP Address	0.0.0
Subnet Mask	0.0.0
Default Gateway	0.0.0
Save	
NOTE: By clicking 'Save' the IP setting	s will be saved, but NOT activated. To activate these settings, please reboot your IP-Converter.

# DHCP

Deze parameter bepaalt of DHCP wordt toegepast. Sluit de IP-Converter aan op het netwerk alvorens hem op spanning te brengen.

Fabrieksinstelling: actief

SB-Security BV

### **IP-adres**

In deze parameter wordt het IP-adres van de IP-Converter ingevoerd. Fabrieksinstelling: 000.000.000.000

### **Subnet Mask**

In deze parameter wordt het Subnet Mask ingevoerd. Fabrieksinstelling: 000.000.000.000

### **Default Gateway**

In deze parameter wordt het IP-adres van de Default Gateway ingevoerd.

Fabrieksinstelling: 000.000.000.000

### Save (Niet voor comfort en easy type)

Nadat u de wijzigingen heeft doorgevoerd dient er een aantal keren op de druktoets van de IPC gedrukt te worden totdat er een knipperende 'S' zichtbaar is in het LED-display. Indien de 'S' niet meer knippert kunt u de wijzigingen naar de IPC schrijven middels de "Save" knop, vervolgens dient de IPC te worden herstart. (onder tabblad maintenance (onderhoud))

Mocht u niet in save mode staan en toch op de "Save" knop drukken dan verschijnt de volgende pop-up:





# 4.2.6 Web Interface Configuratie - RCT Parameters

Ca	onfiguration Diag	nostics Alarmbuffer	Log	Help	Logout	
IP Parameters	CT Parameters	Alarm Interface   I/O	SIP Parameters	s Security	Date&Time	Maintenance
RCT Parameters						
The Receiving Centre Transco phone number to pass the Ro telephone number in the diale address is received via DTMF option, you must clear the al	eiver (RCT) IP adress CT IP address. If this er has to be configure , this RCT 1 IP addre armbuffer first and the	must be configured below. option is enabled, the IP-C d like an IP address and m ss will be used for all RCT in reboot the IP-Converter.	Check the option: 'Re onverter 'learns' the Ri ust be 12 digits (for e: 1 AoIP alarm transmi:	eceiver IP Addres CT 1 IP address xample: 192.168. ssions. If you wis	s via DTMF' if you w during the first dial a 2.41 = 1921680020 h to change the IP :	ish to use the dialer ttempt. The 41). Once a valid IP address using this
General						
PSTN Backup						
Local ACK		$\checkmark$				
ATS Configuration						
O Single Path 1 (SP1)	O Single Path 2	(SP2) <sup>O</sup> Single Path	3 (SP3)			
O Single Path 4 (SP4)	O Single Path 5	(SP5) O Single Path	6 (SP6)			
O Dual Path 1 (DP1)	O Dual Path 2 (I	DP2)  OP2)  Dual Path 3	(DP3)			
O Dual Path 4 (DP4)	O CUSTOM					
RCT 1						
Replace account code						
Account code		000000				
Receiver IP Address via	DTMF					
Receiver IP Address		0.0.0.0				
Reporting time						
RCT 2						
Connection type		🔍 Not used 🛛 💿	GPRS <sup>O</sup> E	thernet		
Replace account code					Advanced	
Account code		000000				
Receiver IP Address		0.0.0.0				
Reporting time when RC	CT1 is active	24 HOURS	4			
Reporting time when RC	CT1 is deactive					
Save						
NOTE: By clicking 'Save' the	RCT settings will be	saved, but NOT activated. <sup>-</sup>	o activate these setti	ngs, please rebo	ot your IP-Converter	

### **GENERAL (ALGEMEEN)**

Indien RCT1 en RCT2 geconfigureerd zijn, dan zal er eerst geprobeerd worden om het alarmbericht via RCT 1 naar de meldkamer te versturen. Indien RCT1 niet beschikbaar is dan zal er automatisch geprobeerd worden om het alarm bericht via RCT2 te versturen naar de meldkamer. Indien beide alarmtransmissiepaden (RTC1 en RCT2) niet aanwezig zijn kan het alarmbericht niet verstuurt worden naar de meldkamer.

### PSTN Back-up

Deze parameter bepaalt of er een PSTN lijn als back-up wordt toegepast.

Fabrieksinstelling: niet actief

OPMERKING: Indien deze optie wordt geactiveerd dient optie "PAC IP-adres via DTMF" uit te staan.

### Local ACK (mode of operation)

In deze parameter wordt aangegeven of de acknowledge (Kiss-off) wordt gegeven zodra de IPC (lokaal) de melding heeft ontvangen (Store-and-forward) of pas als de melding door de ontvanger is bevestigd (Pass-through). Deze parameter is alleen instelbaar bij een PSTN koppeling.

In verband met de lengte van transmissietijden wordt geadviseerd om de optie Local Acknowledge te activeren *Fabrieksinstelling: actief (store & forward mode)* 

## ATS CONFIGURATIE (Verbindingstype)

In deze parameter kan bepaald worden het verbindingstype voor de Europese richtlijnen NEN-EN 50136-1:2012. Bij het selecteren van een verbindingstype zal de parameters die in de onderstaande tabel in de column zijn weergegeven automatisch de juiste waarde krijgen. Met de optie CUSTOM kunnen deze waardes worden aangepast.

Verbindingstype	RCT 1 Reporting time	RCT 2 Connection type	RCT 2 Reporting time when RCT1 is active	RCT 2 Reporting time when RCT 1 is deactive
Single Path 1	24 uur	Not used		
Single Path 2	24 uur	Not used		
Single Path 3	30 minuten	Not used		
Single Path 4	3 minuten	Not used		
Single Path 5	90 seconden	Not used		
Single Path 6	20 seconden	Not used		
Dual Path 1	24 uur	GPRS	24 uur	24 uur
Dual Path 2	30 minuten	GPRS	24 uur	30 minuten
Dual Path 3	3 minuten	GPRS	24 uur	3 minuten
Dual Path 4	90 seconden	GPRS	5 uur	90 seconden

Fabrieksinstelling: Dual Path 3

### **RCT1 (PRIMAIRE VERBINDING)**

### Replace account code (Vervang klant nummer)

Deze parameter bepaalt of het klantnummer wordt uitgelezen via de DTMF string welke door de aangesloten kiezer wordt verstuurd.

Fabrieksinstelling: niet actief

### Account code (Klant nummer)

In deze parameter kan het klantnummer vast worden ingevoerd. De lengte is 4 cijferig voor CID en 6 cijferig voor SIA.

Fabrieksinstelling: 000000

### Receiver IP-address via DTMF (PAC IP-adres via DTMF)

Deze parameter bepaalt of het PAC-adres wordt uitgelezen via de DTMF string welke door de aangesloten kiezer wordt verstuurd. In dit geval wordt het gekozen telefoonnummer vertaald naar het PAC IP-adres. *Fabrieksinstelling: Actief* 

### Receiver IP-address (PAC IP-adres)

In deze parameter kan het IP-adres van de ontvanger (PAC) worden ingevoerd. *Fabrieksinstelling: 000.000.000.000* 

### Reporting time (Rapportage tijd)

In deze parameter kan de rapportage tijd die de verbinding naar de meldkamer controleert worden aangepast. *Fabrieksinstelling: 3 minutes (3 minuten)* 

### RCT 2 (BACKUP VERBINDING)

### Connection type (Connectie type)

Deze parameter bepaalt of de backup verbinding gebruikt wordt.

• Not used; De backup verbinding wordt niet gebruikt

- GPRS; De backup verbinding is GPRS
- Ethernet; De backup verbinding is een 2de vaste verbinding (Geen GPRS verbinding)

Fabrieksinstelling: GRPS

#### Replace account code (Vervang klant nummer)

Deze parameter bepaalt of het klantnummer wordt uitgelezen via de DTMF string welke door de aangesloten kiezer wordt verstuurd.

Fabrieksinstelling: niet actief

#### Account code (Klant nummer)

In deze parameter kan het klantnummer vast worden ingevoerd. De lengte is 4 cijferig voor CID en 6 cijferig voor SIA.

Fabrieksinstelling: 000000

### Receiver IP-address (PAC IP-adres)

In deze parameter kan het IP-adres van de ontvanger (PAC) worden ingevoerd. *Fabrieksinstelling: 000.000.000.000* 

# <u>Reporting time when RCT 1 is active (Rapportage tijd wanneer de primaire verbinding aanwezig is)</u>

In deze parameter kan de RCT 2 kan de rapportage tijd die de verbinding naar de meldkamer controleert worden aangepast. Deze interval tijd is wanneer de primaire verbinding aanwezig is. *Fabrieksinstelling: 24 hours (24 uur)* 

rabileksinstelling. 24 nours (24 uur)

# <u>Reporting time when RCT 1 is deactive (Rapportage tijd wanneer de primaire verbinding niet aanwezig is)</u>

In deze parameter kan de RCT 2 kan de rapportage tijd die de verbinding naar de meldkamer controleert worden aangepast. Deze interval tijd is wanneer de primaire verbinding niet aanwezig is. *Fabrieksinstelling: 3 hours (3 uur)* 

### 4.2.7 Web Interface Configuratie - Advanced GPRS Parameters

	Configuration	Diagnostics	Alarmbuffer	Log	Help	Logout	
IP Parameters	RCT Paramet	ers   Alarm Int	erface   I/O	SIP Parameters	Security	Date&Time	Maintenance
Advanced GPRS p	arameters						
Pincode				Re-type			
Apn	inte	rnet					
Username	gue	est					
Password	gue	est					
Manual select Opera	tor 🗖						
OrenatesId	0			Unknown opera	tor 👻		

### **Pincode**

In deze parameter kan de pincode van de GPRS kaart worden ingevoerd. *Fabrieksinstelling: 0000* 

### <u>Apn (Access point name)</u>

In deze parameter kan de naam van het toegangspunt van de GPRS kaart worden ingevoerd. *Fabrieksinstelling: internet* (Default voor KPN)

### Username (Gebruikernaam)

In deze parameter wordt de gebruiker naam van de GPRS kaart ingevoerd. *Fabrieksinstelling: guest* (Default voor KPN)

### Password (Paswoord)

In deze parameter wordt het paswoord van de GPRS kaart ingevoerd. *Fabrieksinstelling: guest* (Default voor KPN) **OPMERKING: Apn / Username / Password dient u bij de provider van de SIM kaart aan te vragen.** 

### Manual select Operator (Handmatige selectie operator)

Selecteer deze optie om handmatig een operator te selecteren. Indien men in het grensgebied installeert kan het zijn dat er ongewenst gebruik wordt gemaakt van een buitenlandse operator. Met deze optie kan men voor één operator kiezen

### **Operator Id (Operator)**

In het diagnose window (Zie hoofdstuk: Web Interface Diagnostics) wordt weergegeven welke operators aanwezig zijn.

OPMERKING:Bij GPRS wordt standaard elke 24 uur een poll bericht verstuurd om te controleren of de transmissieweg aanwezig is.

### 4.2.8 Web Interface Configuratie - Alarm Interface

	Configuration	Diagnostics	Alarmbuffer	Log	Help	Logout	
IP Parameters	RCT Paramete	ers Alarm Inter	face   1/0	SIP Parameters	Security	Date&Time	Maintenance
PSTN Interface							
Select your dialer prot	ocol below.						
Dialer protocol	Au	to Detect SIA/CID		~			Advanced
Lico DSTM lino Ma	nitoring 🔲	0 00000 00 000	1				Advanced
USE F STIN III E MIC							
Contal Indonésia							
Serial Internace	ſ	No	Socurity pa	roword	000000000000000000000000000000000000000		
Serial protocor	t code		Computer s	ddroce	1		
Serial poll range	l coue [	000000	Dort number	r.	1500		
ochar poir range	l	0	Titan src 11	P Address		.0	
			Titan src 21	P Address	0 0 0	0	
			Titan src 3	P Address	0 0 0	. 0	
			Titan src 4	P Address	0.0.0	. 0	
			Titan src 5	P Address	0.0.0	. 0	

### **PSTN INTERFACE**

### **Dialer protocol (Kiezer protocol)**

In deze parameter wordt aangegeven welk protocol het op de analoge poort aangesloten paneel uitstuurt.

- Auto Dectect SIA/CID: De IP-Converter zal na de eerste melding detecteren of het paneel doormeldt via SIA of CID, waarna de IP-Converter zich vervolgens automatisch configureert. Let op deze optie werkt niet bij SATEL panelen.
- Of selecteer juiste verbinding voor het type paneel dat wordt toegepast, zie BIJLAGE.
- Voor (X)SIA Bell (103) Multi Account, CID 1400Hz/2300Hz Multi Account en CID 1600Hz/2100Hz Multi Account wordt de parameter "Main account code" (Hoofd klant nummer) zichtbaar. Als er meerdere klant nummers ingesteld staan in het paneel, kan hier het hoofd account nummer ingegeven worden. Fabrieksinstelling: 000000

### Use PSTN Line Monitoring (Activeren van de PSTN lijn monitoring)

Met deze parameter kan aangegeven worden of er PSTN lijn monitoring plaats vindt tussen de IPC en het paneel. **LET OP: Een 18k/0,5W weerstand moet tussen de aansluitpunten TIP en RING van het paneel geplaatst worden!** Bij een breuk in de PSTN lijn zal de SIA code LT0002 (Line Trouble) worden verstuurd. Bij herstel van de PSTN lijn de SIA code LR0002 (Line Restore)

Fabrieksinstelling: Niet actief

### SERIEEL INTERFACE

### Serial protocol (Serieel protocol)

In deze parameter wordt aangegeven welk protocol het op de seriële poort aangesloten paneel uitstuurt.

- De te selecteren protocollen zijn: Aritech MPI, Galaxy, NX8, Dvacs, ATS
- Voor ATS zijn de volgende parameters van belang:
  - · Serial poll account code: Fabrieksinstelling: 000000
  - · Security password: Fabrieksinstelling: 000000000
  - · Computer address: Fabrieksinstelling:1
  - Titan src 1 t/m 5 IP Address: Fabrieksinstelling: 0.0.0.0
  - Port number: Fabrieksinstelling: 1500
     D.m.v het instellen van het Computer adres, Titan src IP adres en Poort nummer kan er up en downloading plaatsvinden via de seriële poort naar het ATS paneel.
- Voor ARITECHMPI is de parameter "Serial poll range" (Serieel reeks blokken) van belang. In deze parameter kan het aantal toegepaste blokken worden aangegeven Let op: aan ontvangstzijde dienen een opeenvolgend aantal klantnummers te worden gereserveerd. Fabrieksinstelling: 0

Fabrieksinstelling: No

### Serial poll accountcode (Serieel Klant nummer)

In deze parameter kan het klantnummer wat wordt gebruikt voor de seriële communicatie worden ingevoerd. *Fabrieksinstelling: 000000* 

### 4.2.9 Web Interface Configuratie - I/O (Input/Output)

	Configuration	Diagnostics	Alarmbuffer	Log	Help	Logout	
IP Parameters	RCT Paramet	ers   Alarm Int	erface   <u>I/O</u>	SIP Parameters	s Security	Date&Time	Maintenance
1/0							
Output		FTC	•				
Use input	[	-					
Account code		000000					
SIA code alarm	[	ГА					
SIA code restore	[	ſR					
Zone number	0	)					
Zone text		Famper					
Save							
NOTE: By clicking 'Save	e' the I/O settings v	vill be saved, but I	NOT activated. To a	activate these settin	igs, please reboo	t your IP-Converter.	

### <u>Output</u>

In deze parameter wordt aangegeven wanneer de uitgang schakelt naar GND.

- FTC: Failed to Connect. Indien de verbinding wegvalt, schakelt de uitgang naar GND.
- FTC Primary: Failed to Connect Primary. Indien de primaire verbinding wegvalt, schakelt de uitgang naar GND.

**ASB-Security BV** 



 FTC BACKUP: Failed to Connect BACKUP. Indien de backup verbinding wegvalt, schakelt de uitgang naar GND.

Fabrieksinstelling: FTC

### Use input (Gebruik ingang)

Ingang aan en uitzetten. *Fabrieksinstelling: niet actief* 

### Account code (Klantnummer)

Accountcode welke mee gestuurd wordt bij het aansturen van de ingang. *Fabrieksinstelling: 000000* 

### SIA code alarm (SIA code alarm)

SIA code welke meegestuurd wordt bij het aansturen van de ingang. *Fabrieksinstelling: TA* 

### SIA code restore (SIA code herstel)

SIA code welke meegestuurd wordt bij het herstellen van de ingang. *Fabrieksinstelling: TR* 

### Zone number (Zone nummer)

Zone nummer wat meegestuurd wordt bij het aansturen van de ingang. *Fabrieksinstelling: 0* 

### Zone text (Zone tekst)

Zone tekst welke meegestuurd wordt bij het aansturen van de ingang. *Fabrieksinstelling: Tamper* 

### 4.2.10 Web Interface Configuratie – Advanced PSTN Interface

	Configuration	Diagnostics	Alarmbuffer	Log	Help	Logout	
IP Parameters	RCT Parameter	ers   Alarm Int	erface   I/O	SIP Parameters	s   Security	Date&Time	Maintenance
Gain Parameters							
Enter the gain configura	tion						
Tx Gain	2	2 -					
Rx Gain		1 -					
Save							
NOTE: By clicking 'Sav	e' the interface setti	ings will be saved	, but NOT activated	d. To activate these	settings, please	reboot your IP-Conv	erter.

### **GAIN PARAMETERS**

### Tx Gain (Transmit versterking)

In deze parameter wordt de PSTN zendversterking ingesteld. Deze parameter dient alleen in overleg met onze technische medewerkers te worden gewijzigd.

Fabrieksinstelling: 2

In deze parameter wordt de PSTN ontvangstversterking ingesteld. Deze parameter dient alleen in overleg met onze technische medewerkers te worden gewijzigd.

Fabrieksinstelling: 1

### 4.2.11 Web Interface Configuratie – SIP Parameters

	Configuration	Diagnostics	Alarmbuffer	Log	Help	Logout	
IP Parameters	RCT Paramete	ers   Alarm Int	erface   I/O	SIP Parameters	Security	Date&Time	Maintenance
SIP Parameters Enter the SIP configurat Receiver ID asb Receiver IP 0 SIP ID asb PSTN number 1234	on 0 . 0 . 0 56789		Advanced	]			
Save NOTE: By clicking 'Save	' the SIP settings v	vill be saved, but	NOT activated. To	activate these setting:	s, please rebo	ot your IP-Converter.	

Voor up/downloading is er minimaal 150Kbps (voor zowel upload als download) vrije bandbreedte vereist.

### Receiver ID

In deze parameter wordt het receiver ID (van de Up-/Download Converter) ingevuld. Deze parameter dient overeen te komen met de parameter "Receiver ID" in de Up-/Download Converter. Deze parameter is van belang voor het "inbellen" van het paneel naar de "up-download" software.

Fabrieksinstelling:asb

### **Receiver IP**

In deze parameter wordt het IP-adres van de Up-/Download Converter ingevuld. Deze parameter is van belang voor het "inbellen" van het paneel naar de "up-download" software.

Fabrieksinstelling: 0.0.0.0

### <u>SIP ID</u>

In deze parameter wordt het SIP ID ingevuld. Deze parameter dient overeen te komen met de parameter "SIP ID" in de Up-/Download Converter. Deze parameter is van belang voor het inbellen van "up-download" software naar het paneel.

Fabrieksinstelling: asb

### **PSTN number**

In deze parameter wordt het PSTN nummer ingevuld die wordt gebeld door het paneel om verbinding te maken met de "up-download" software van het paneel.

Fabrieksinstelling: 123456789

ASB-Security BV

# 4.2.12 Web Interface Configuratie – Advanced Sip Parameters

	Configuration	Diagnostics	Alarmbuffer	Log	Help	Logout	
IP Parameters	RCT Paramete	ers   Alarm Inte	erface   I/O	SIP Parameters	Security	Date&Time	Maintenance
Advanced SIP Para Enter the Advanced SIP of SIP port 5060 RTP port 7000 Jitter size 200	meters						
Network Parameter	rs						
Enter the Network configu	iration						
Use the device's I	P address						
Enter public IP ad	ldress:						
Use STUN protoc	ol to discover r	ny public IP					
Save							
NOTE: By clicking 'Save'	the Advanced SIP	settings will be s	aved, but NOT ac	tivated. To activate the	se settings, pl	ease reboot your IP	-Converter.

### SIP Port

In deze parameter wordt het SIP (Session Initiation Protocal) poort nummer ingevuld. Deze parameter dient overeen te komen met de parameter "SIP port" in de Up-/Download Converter. LET OP: Deze poort dient ook geforward te worden naar het IP-adres van de IP-Converter

Fabrieksinstelling: 5060

### **RTP Port**

In deze parameter wordt het poort nummer van het RTP (Real Time Protocol) spraak (VoIP) data ingevuld. Deze parameter dient overeen te komen met de parameter "RTP Port" in de Up-/Download Converter. **LET OP: Deze poort dient ook geforward te worden naar het IP-adres van de IP-Converter** 

Fabrieksinstelling: 7000

### Jitter size

In deze parameter wordt de jitter size van het RTP protocol ingevuld. De grote van de "jitter size" bepaalt de vertraging in milliseconden van de spraak (VoIP) data. **Deze parameter dient alleen in overleg met onze technische medewerkers te worden gewijzigd.** 

Fabrieksinstelling: 200

### **Network Parameters**

In deze parameter wordt bepaald op welke manier de IP-Converter verbinding maakt met de Up-/Download Converter.

- Use the device's IP address Gebruik deze optie als de Up-/Download Converter is aangesloten op hetzelfde netwerk als de IP-Converter (zonder NAT router)
- Enter NAT IP address Gebruik deze optie als de Up-/Download Converter is aangesloten via een NAT router. Vul het public IP adres van de NAT router in.
- Use STUN to discover my public IP Gebruik deze optie als de IPC is aangesloten via internet. Het STUN (Simple Traversal of UDP through NAT) protocol zorgt er voor dat het public IP adres van de NAT router automatisch wordt bepaald.

Fabrieksinstelling: use STUN to discover my public IP



# 4.2.13 Web Interface Configuratie - Security

	Configuration	Diagnostics	Alarmbuffer	Log	Help	Logout	
IP Parameters	RCT Paramete	ers   Alarm Int	erface   I/O	SIP Parameters	Security	Date&Time	Maintenance
Security Admin WEB Password User WEB Password	ord		Re-type Re-type				
Save							

### Admin WEB password (Administrator WEB paswoord)

In deze parameter wordt het paswoord geprogrammeerd wat toegang geeft als administrator tot de WEB browser, het is verstandig het standaard paswoord te wijzigen.

Fabrieksinstelling: asb

### User WEB password (Gebruiker WEB paswoord)

In deze parameter wordt het paswoord geprogrammeerd wat toegang geeft als gebruiker tot de WEB browser, het is verstandig het standaard paswoord te wijzigen.

### Fabrieksinstelling: user

OPMERKING: Uit veiligheidsoverwegingen wordt het ingevoerde paswoord niet zichtbaar gemaakt tijdens intypen, om misverstanden te voorkomen dient het paswoord dan ook 2 x te worden ingevoerd. OPMERKING: Na drie keer foutief inloggen zal de IPC blokkeren waardoor je 1 minuut niet meer kunt inloggen.

### 4.2.14 Web Interface Configuratie - Date & Time



### Date (Datum)

In deze parameter kan de datum worden aangepast (in het formaat DD/MM/JJJJ).

### Time (Tijd)

In deze parameter kan de tijd worden aangepast (in het formaat HH:MM:SS).

Opmerking: Deze pagina haalt de huidige datum en tijd van de IP-Converter. Als de NTP (Network Time Protocol) server correct is ingesteld dan zal de datum en tijd automatisch goed gezet worden (zie optie NTP server in Configuration - Maintenance)

# 4.2.15 Web Interface Configuratie – Maintenance (Onderhoud)

	Uniguration Diagnostics Al	ambuner Log	neip Logout	
IP Parameters   R	CT Parameters   Alarm Interfac	e   I/O   SIP Parameters	Security   Date&Time	Maintenance
Maintenance				
The latest software version of specified here.	an be retrieved from the ASB update	server using the update method d	lefined in the manual. The IP addr	ess of the server is
Update server	80 . 112. 203. 6			
VoP server	80 . 112. 203. 5	VoP Service Number	0	
RMS server	0 0 0 0	RMS ID		
NTP server	193. 67 . 79 . 202			
Log Level	CLevel 0 CLevel 1			
Save	Factory Default		Reboot	

### **Update server**

In deze parameter kan het IP-adres van de update server worden ingevoerd. Dit kan nodig zijn indien u nieuwe software wilt downloaden.

Fabrieksinstelling: 080.112.203.006

### **VoP server**

In deze parameter kan het IP-adres van de Verification of Performance (VoP) server worden ingevoerd. Dit is nodig indien u Verification of Performance wilt.

Fabrieksinstelling: 080.112.203.005

### VoP Service Number

In deze parameter kan het VoP Service nummer ingevoerd worden. Indien u Verification of Performace afneemt, krijgt u dit nummer van het ASB beheercentrum. *Fabrieksinstelling: 0* 

### **RMS server**

In deze parameter kan het IP-adres van een Remote Management Server (RMS) worden ingevoerd. Dit geeft de mogelijkheid om van afstand in te loggen door het beheercentrum. *Fabrieksinstelling: 000.000.000* 

### RMS ID

In deze parameter kan het RMS ID nummer ingevoerd worden. Indien u RMS afneemt, krijgt u dit nummer van het ASB beheercentrum.

Fabrieksinstelling: (Niet ingevuld)

### **NTP server**

In deze parameter kan het IP-adres van een Network Time Protocol worden ingevoerd, deze wordt gebruikt tijdens opstarten en om periodiek de tijd te synchroniseren.

Fabrieksinstelling: 193.67.79.202

### Log Level

Hiermee wordt bepaald welke log entries er opgeslagen worden in de log buffer van de IPC. In log level 0 wordt alles gelogt. In log level 1 worden de poll berichten ("Transmit ack" en "Poll ack") achter wegen gelaten, dit om het log niet in korte tijd vol te laten lopen.

Fabrieksinstelling: 0



Met behulp van deze knop kan de IP-Converter worden herstart. Dit is nodig nadat wijzigingen in de configuratie zijn doorgevoerd.

### **Factory default**

Met behulp van deze knop kunnen de instellingen van de IP-Converter worden teruggezet naar de fabrieksinstellingen.

## 4.2.16 Web Interface - Diagnostics

Conf	iguration Diagnostics Alarmbuffer Log Help Logout
Primary RCT	Fully operational : No errors
Serial Panel	ERROR . SIMI CAID
GPRS STATE	DISCONNECTED
GPRS IP ADDRESS	
GPRS #CALLS	0
GPRS TX KBytes	0
GPRS RX KBytes	0 Niek zwistekte
NAT settings	Last Public IP detected with STUN: 83 137 143 67
Infa	prodefensional in incompleteneorial factority on other and
Mac Address	00:05:b1:00:2a:08
Type	GPRS
Software version	V03.01 [[Thu Jul 28 17:11:42 CEST 2011
Hardware version	V1.2
UEM	ASB

### **Connectie status**

In dit venster wordt de actuele status van de primaire verbinding, back-up verbinding en seriële verbinding weergegeven. Ook vind u hier aanvullende informatie betreffende het GPRS modem. Bij de GPRS operators ziet meteen welke operators beschikbaar waren tijdens het opstarten van de IP-Converter

**GPRS** Operators

- = 1 = verbinding toegestaan maar niet verbonden
- = 2 = verbinding met operator

= 3 = verbinding niet toegestaan

Naam operator = "NL KPN" id operator = 20408

### NAT settings

Dit venster geeft informatie over het de NAT parameters settings.

### <u>Info</u>

Informatie gegevens betreffende de hard- en software versie en het MAC adres van de IP-Converter.

**ASB-Security BV** 

# 4.2.17 Web Interface - Alarm buffer weergave

	Configuration	Diagnostics	Alarmbuffer	Log	Help	Logout	
imary RCT							
						Clear all	Test RCT1
ackup RCT (GP	RS)						Test RCT2
							A COLOR MARK

In deze weergave worden de 50 posities van de primaire en backup alarmbuffer weergegeven. Alle alarmen zijn voorzien van datum/tijd, Alarm, PAC IP-adres en een status. De status geeft weer of het betreffende alarm al bevestigd is.

### <u>Clear</u>

Via de "Clear" knop is het mogelijk om het alarm buffer te wissen. Als bijvoorbeeld het PAC IP adres niet goed is ingesteld, of als er een verkeerde PSTN interface is geselecteerd dan bevinden er zich alarm meldingen die niet worden bevestigd door de PAC. Via de "Clear" knop kunnen deze dan worden verwijderd.

### Test RCT 1/2

Via de Test RCT1 en Test RCT2 is het mogelijk om een test melding te versturen naar de PAC.

### 4.2.18 Web Interface - Log weergave

	Configuration	Diagnostics	Alarmbuffer	Log	Help	Logout	
og History							

In deze weergave wordt het Log geheugen van de IP-Converter weergegeven. Bij een herstart of bij het spanningsloos maken van de IP-Converter, wordt de log buffer gewist.



### 4.2.19 Web Interface - Help weergave

Deze handleiding is ook digitaal te bekijken, u kun hem raadplegen onder het tabblad Help. De handleiding wordt van internet gedownload (internet verbinding is noodzakelijk).

### 4.3 GSM / GPRS modem

Hieronder volgen de specificaties van het toegepaste GSM/GPRS-modem

Quad-band EGSM 850 / 900 / 1800 / 1900Mhz Uitgangsvermogen

Klasse 4 (2W) @ 850 / 900Mhz

Klasse 1 (1W) @ 1800 / 1900Mhz

Gevoeligheid

-107 dBm (typ.) @ 850 / 900Mhz

-106 dBm (typ.) @ 850 / 900Mhz

Afbeelding: GSM/GPRS modem

SIM kaart houder



# **5** Specificaties

# 5.1 Technische gegevens

- Voedingsspanning: 13 +1/-2 VDC
- Stroomverbruik: 150-200mA. (zonder GPRS modem); 170-280mA. (Met GPRS modem).
- Omgeving temperatuur: 0-50 °C
- · Vochtigheid: max. 90%, niet condenserend
- Afmetingen: (OEM print) LxBxH 140x83x24 mm.
- Gewicht: (OEM print) plm. 0,1 Kg
- Ethernet: 10Base-T / 100Base-TX; Ondersteund MDI/MDI-X auto cross-over functie

# 5.2 PSTN-protocollen (zie BIJLAGE voor geteste panelen)

De volgende PSTN-protocollen worden ondersteund:

- Auto Detect SIA/CID
- (X)SIA protocollen
  - (X)SIA Bell103
  - (X)SIA Bell103 Multi Account
  - (X)SIA SATEL
  - (X)SIA SATEL Multi Account
- DTMF protocollen
  - CID 1400Hz/2300Hz (Default)
  - CID 1600Hz/2100Hz
  - CID 1400Hz/2300Hz Multi Account
  - CID 1600Hz/2100Hz Multi Account
- Fast Format
  - Fast Format 1400Hz
  - Fast Format 1600Hz

# 5.3 Seriële interfacing (zie BIJLAGE voor geteste panelen)

Met de volgende panelen en modules is seriële interfacing mogelijk, hierbij is voor diverse panelen een seriële module vereist:

- Aritech CD3401
- Galaxy 8
- NX 8
- Dvacs
- ATS 3000, 4000, 4500

### 5.3.1 Aritech CD3401 V1.4 / CD150.01 V 6.22:

Het paneel wordt via de MPI232 interface aangesloten aan de IPC. De Pin aansluitingen tussen Aritech CD3401 en de IPC:

IPC (aansluitklem) === Paneel Aritech CD3401 (DB9)

- Tx === Rx (Pin 2)
- Rx === Tx (Pin 3)
- GND === GND (Pin 5)

De toets " $\sqrt{}$ " van het keypad is de enter toets en "X" de escape toets. Door middel van de " $\downarrow$ " en " $\uparrow$ " toets kunt u door het menu scrollen. Via de toets "0" gaat men terug.

Het hoofd systeem van de Aritech is de CD3401 V6.0 (101298-4).

Om in te schakelen toetst u "0" gevolgd door "1122". Uitschakelen gebeurd met "0" gevolgd door "1122". De programmeer code wordt geactiveerd met "0" gevolgd door "1278".

### <u>Serial settings</u>

De Serial Interface module account code van de Aritech CD3401 paneel is "1213". In de programmeer mode menu "1278" kunt u de zones configureren door te scrollen door het menu tot u bij "ingangen" bent.

### MPI 232 paneelinterface instellingen:

Op de MPI 232V2 sw V2.30: RS232

- 9600 Baud
- 8 databits
- no parity
- 1 stop bit

Account code 6 digits Account code (poll id) 3 digits event numbers meerdere events per call text in SIA "AT" must be send every 8 sec.

Tijdens het programmeren van de MPI-232 dient de dipswitch 3 "OFF" te staan, de andere staan allen op 'ON'. Eenmaal geprogrammeerd, wordt de dipswitch 3 ook op 'ON' gezet.

### IPC moet als volgt ingesteld worden:

Paneel

- (0) Type: (3) ARITECH
- (1) Poll id: 000001 Poll ID is gelijk aan instelling in paneel.
- (2) Poll id range : 4 Aantal blokken (max. 8)

### Het Aritech paneel moet als volgt ingesteld worden:

### Central station 1 menu

- 1. Account code 1 : 000001
- 2. Account code 2 : 000002
- 3. Account code 3 : 000003
- 4. Account code 4 : 000004
- 5. Account code 5 :
- 6. Account code 6 :
- 7. Account code 7 :
- 8. Account code 8 :
- 9. Network address: 1

Op de meldkamer dient een opeenvolgende reeks aansluit/prom nummers gereserveerd te worden. Dus als het aansluit/prom nummer 000100 is en er worden 4 blokken ingesteld dan dienen de nummer 000100 tot 000103 gereserveerd te worden.

Pollrange in de IP-Converter dient ingesteld te worden en is afhankelijk van het aantal blokken. Indien het aantal blokken 4 is dan stelt u de Pollrange in op 4.

### 5.3.2 GALAXY 8:

Het paneel wordt via de externe RS232 interface rev1.1 aangesloten aan de IPC. Voor de bekabeling naar het paneel volgt hieronder de aansluitingen.

De Pin aansluitingen tussen Galaxy en de IPC:

IPC (aansluitklem) === Paneel Galaxy (DB9 to DB25)

- Tx === Rx (Pin 3)
- Rx === Tx (Pin 2)

**ASB-Security BV** 



### • GND === GND (Pin 7)

#### Paneel instellingen:

Op de centrale:

Op adres 56 kiest men bij mode voor RS232, direct. Dan dient men te selecteren voor SIA level 02 / 03. De verschillende triggers dienen aangezet naargelang men al dan niet wil statusveranderingen doorsturen. Tenslotte dient men de account code in te vullen in 6 karakters. Zorg dat het 6 cijferig Poll ID voor zowel IPC als paneel gelijk ingesteld staan.

De externe RS232 module (SW: V2.01, CS: 047D).

In menu "56" (Modem/Kiezer = Modem/Dialer) configureert men de RS232 poort na selecteren van "A  $\rightarrow$  Kies de volgende instellingen voor de RS232 poort:

- "1 = Mode" on "1=Direct",
- "2 = Format" on "1=SIA" en selecteer level 2 of 3,
- "3 = Klantnummer (Account number)", Stel de IPC identiek in.

In menu "52" (Progr. Zones) kunt u de zones configureren van het paneel.

Opmerking: Op de externe RS232 module rev 1.1 (SW: V 1.20) dient men via de dipswitch in te stellen:9600, 8, 1, N. Met andere woorden alle switchen staan op OFF behalve switch 6 en 8 die op ON dienen te staan.



### 5.3.3 NX 8:

Het paneel wordt via de NX-584 V.01F0 1.06 interface aangesloten aan de IPC. Voor de bekabeling naar het paneel volgt hieronder de aansluitingen.

De Pin aansluitingen tussen NX 8 en de IPC:

### IPC (aansluitklem) === Paneel NX8 (xx)

- Tx === Rx (Pin 3)
- Rx === Tx (Pin 2)
- GND === GND (Pin 5)

Het NX-8 paneel kan geprogrammeerd worden door het programmeren van bepaalde adressen. (raadpleeg de NX-8 handleiding als u wilt weten hoe u het NX-8 paneel kunt programmeren).

Om de instellingen van het NX8 paneel te configureren dient u het volgende te doen:

Druk op \* 8, gevolgd door de programmeercode "9713". Voor de instellingen op het centrale paneel drukt u " 0 # ". Nu bent u in de programmeermode.

Er zijn een aantal adressen die geen invloed hebben op de manier waarop alarmen gegenereerd worden door de IPC. Deze adressen zijn:

0 t/m 22: deze worden gebruikt voor het configureren en kiezen van (het gebruik van) telefoon nummers; 88, 89, 92, 95, 98, 101, 104, 107

Deze worden gebruikt voor `account' codes. De account code van het paneel moet ook in de IPC worden geprogrammeerd.

### Configureren van de NX-584 module:

De NX-584 kan ook geprogrammeerd worden door de adressen van de module te programmeren. De module ID is 72.

De volgende adressen moeten geprogrammeerd worden:

Address 0:



Bit 1 (binary/ASCII conversie mode) kan aan- of uitgezet worden. Aangezien binary mode" sneller is en daardoor meer geschikt voor gebruik, geniet deze instelling de voorkeur (bit uitzetten)

• Address 1- 4:

Bepaalt de parameters van de seriepoort: 9600 baudrate;

Address 2
 Segment 1: 0.

Segment 2: 0. (bepaalt de mogelijkheid van het doorsturen van bepaalde events; moet uitgezet worden!);

- Address 3
- Segment 1: 0.

Segment 2: bit 1 and 3 (System Status request en Log event request) moeten aan staan. Segment 3: bit 1 (Program Data Request) moet aan staan. Segment 4: bit 4 en bit 7 moeten aan staan.

# 5.3.4 DSC PANELEN (DVACS MODULE)

De Pin aansluitingen tussen DSC PC5400 en de IPC:

### IPC (aansluitklem) === Paneel PC5400 (RJ45)

- Tx === Rx (Pin 7)
- Rx === Tx (Pin 2)
- GND === GND (Pin 5)

**A)** POWER SERIES: T.b.v. aansluiten en programmeren **PC5400 DVACS** module op IPC. Aansluiten:

- 1. Keybus aansluiting ,RED , BLACK , YELLOW en GREEN.
- 2. Tussen T1 en T2 een draadbrug aanbrengen (module sabotage ingang).
- 3. Modulaire kabel tussen DVAC's mod. en IPC aanbrengen.
- 4. 8 polige Modulaire connector op DVAC,s module.(DVAC's uitgang) en aansluitklemmen.

<u>PC50XX:</u>

### Programmeren van DVAC's module v2.X:

- Voer in \* 8 installateur code 801
- Lok. 06 indicatie 1 deselecteren, # #
- Lok. 803
- Lok. 36 programmeren volgens lok. 001. (groepen definities 1 t/m 8).
- Lok. 37 programmeren volgens lok. 002. (groepen definities 9 t/m 16 ).
- Lok. 38 programmeren volgens lok. 003. (groepen definities 17 t/m 24 ).
- Lok. 39 programmeren volgens lok. 004. (groepen definities 25 t/m 32).
- Lok **40** Hexadecimale DVAC,s ID (Hexadecimale waarde aansluitnummer)
- Afsluiten met **#** toets.

### Programmeren van DVAC's module v3.X:

- Voer in \* 8 installateur code 801
- Lok. 06 indicatie 1 deselecteren, # #
- Lok. 803
- Lok. 31 programmeren zone typen (groepen definities 1 t/m 16 ).
- Lok. 32 programmeren zone typen (groepen definities 17 t/m 32 ).
- Lok. 33 programmeren zone typen (groepen definities 33 t/m 48).
- Lok. 34 programmeren zone typen (groepen definities 49 t/m 64 ).
- Lok 40 Hexadecimale DVAC,s ID (Hexadecimale waarde aansluitnummer)
- Afsluiten met # # toets.

### Supervisie (Bewaking):

Activeer door 902 in te voeren in het DSC Systeem en na 1 minuut 903 in te voeren. Op het display verschijnt de tekst : ingelezen module LINKS MODULE.

Dvac's module terug brengen naar de fabrieksinstellingen:

- Voer in \* 8 installateur code 803
- Lok. 06 indicatie 1 selecteren.
- Ga uit locatie 803 (dit maakt van de DVAC'S een printer module).
- Wacht een minuut zodat de module is ingelezen.
- Voer in 997 installateurcode 997 (brengt de module naar de fabrieksinstelling PC5400).

**B)** MAXSYS  $\rightarrow$  T.b.v. aansluiten en programmeren **PC4400 DVACS** module op IPC.

Aansluiten:

- 1. Keybus aansluiting , RED , BLACK , YELLOW en GREEN.
- 2. Tussen T1 en T2 een draadbrug aanbrengen (module sabotage ingang).
- 3. Modulaire kabel tussen DVAC's mod. en IPC aanbrengen.
- 4. 8 polige Modulaire connector op DVACS module.(DVAC's uitgang) en aansluitklemmen.

### PC4401 V1.1:

- Inlezen module:
- Toets \* 8 installateur code;
- Toets 02, 00, 01
- Maak een module sabotage (T1 en T2)
- Toets \*
- Toets \*, DVAC's inschakelen (Y)
- Programmeren:
- Toets \* 8 installateur code

Toets **00**, **08**, **00**, **XX**, **00** waar XX de module ID is (hexadecimale waarde aansluitnummer) voor instellen Module Function. Toets **0x voor de functie** "DVAC". Ook de Baudrate wordt nu automatisch ingesteld . PC40XX V2.X:

- Inlezen module:
- Toets \* 8 installateur code
- Toets 2, 0, 1
- Maak een module sabotage (T1 en T2)
- Toets \*
- Toets \*, DVAC's inschakelen (Y)
- Programmeren:
- Toets \* 8 installateur code

Toets **0**, **08**, **2**, **0**, **01** DVAC ID (hexadecimale waarde aansluitnummer) <u>PC40XX V3.X:</u>

- Inlezen module:
- Toets \* 8 installateur code;
- Toets 02, 00, 01
- Maak een module sabotage (T1 en T2)
- Toets \*
- Toets \*, DVAC's inschakelen (Y)
- Programmeren:
- Toets \* 8 installateur code

Toets 00, 08, 01, 00, 01 DVAC ID (hexadecimale waarde aansluitnummer)

# 5.3.5 ATS3000, 4000, 4500 (Vanaf V04.06.44)

De Pin aansluitingen tussen ATS en de IPC:

IPC (aansluitklem) === Paneel ATS (aansluitklem)

- Tx === Rx (Computer Port)
- Rx === Tx (Computer Port)



• GND === GND (Computer Port)

### 12VDC (ATS paneel) === CTS

Het CTS aansluitpunt (aan ATS1801 zijde) dient te worden verbonden met de 12VDC van het ATS paneel

### Paneel instellingen:

Het ATS paneel kan terug naar de fabrieksinstellingen met de "Kill" jumper LK10. Om de jumper kort te sluiten dient u de voeding en accu van het paneel te ontkoppelen. Wacht 30 seconden voordat u de jumper eraf haalt. Koppel vervolgens de voeding en de accu terug aan het paneel. Schakel het paneel uit met code "1122" en druk op toest "OFF" en kies vervolgens "0" voor alle zones. Alle LED's zullen nu uitgaan.

### Serial settings

Na het indrukken van de "menu" toets, komt men door het opgeven van de code "1278", via menu 19 in het installateur menu. In het installateurmenu 19 dienen minimaal de volgende instellingen geprogrammeerd te worden, uitgaande van de default instellingen van het ATS controlepaneel:

### Menu 9, Menu 17 PAC instellingen, PAC 1:

- Menu 17/1 Protocol = 5, SIA <u>of</u> 7, XSIA.
- Menu 17/4 Systeemklantnummer tbv systeemmeldingen = 0001.
- Menu 17/5 Gebiedsklantnummer tbv gebiedsmeldingen en alarmen = 0001.
- Menu 17/14 Verbindingstype, Universele Interface = Type 4.
- Menu 18 Sia Area modifier op "JA" instellen.

### Menu 29, Computerverbinding:

- Menu 29/6 Meld alarmgebeurtenissen naar computer = Ja.
- Menu 29/7 Meld toegangscontrolegebeurtenissen naar computer = Ja.
- Menu 29/11 Computeradres = 0001
- Menu 29/12 Beveiligingswachtwoord = 0000000000. (Deze moet overeenkomen met Security password in de alarm interface web/pagina van de IPC)

# **OPMERKING:** Indien het computeradres/beveiligingswachtwoord wordt gewijzigd dient de IPC opnieuw te worden opgestart.

### 5.4 Antenne

- Bandbreedte: 80 MHz in EGSM, 150 MHz if GSM 850, 170 MHz in DCS, 140 MHz PCS band
- Versterking: 1.5dBi ≤ versterking < 3dBi (referenced to I/2 dipole)
- Impedantie: 50 ohm
- Ingangs vermogen: > 2 W piekvermogen
- VSWR maximaal: ⇐ 10:1
- VSWR aanbevolen: ⇐ 2:1

Afbeelding: GSM/GPRS modem aansluiting





OPMERKING: Neem de nodige voorzichtigheid in acht bij het aansluiten van de antenne.

OPMERKING: Bij gebruik van GPRS kunnen er mogelijk problemen zijn met het bereik, bijv. als je in de kelder staat. Dit heeft impact op de dienstverlening. Mobiel geeft geen garanties op netwerken en heeft ook geen beschikbaarheidgegevens. Advies is bij installatie van de GPRS converter met je (KPN) mobiel de bereikbaarheid te testen (aantal bereikbaarheidsstreepjes of GPRS data verkeer).

# 6 KORTE INLEIDING IP

# 6.1 Inleiding

In de volgende hoofdstukken wordt de basis van de IP technologie behandeld. Hoe werkt IP en wat kun je er mee doen? Wij willen u adviseren om de standaard kennis voor netwerken eigen te maken. Dit kan bij verschillende instellingen o.a. bij Van Dusseldorp Training & Advies, Kenteq. De verschillende ROC's en andere opleidingsinstituten hebben een goede basisopleiding hiervoor opgezet. Netwerkkennis is onontbeerlijk voor nu en in de toekomst.

De basis van het Internet wordt gevormd door Transmission Control Protocol / Internet Protocol (TCP/IP). In dit hoofdstuk komen de volgende onderwerpen aan de orde:

- Het OSI Model
- De lagen 1 en 2
- · IP-adressering en netwerkklassen
- · Switches, Routers en Hubs
- Routering
- DNS
- Protocollen / Poortnummers

Met deze informatie zult u wellicht bij inbedrijfstelling van de IP-Converter een beter idee krijgen over waarom iets wel of niet werkt.

## 6.2 Het OSI-model

Het OSI-model is een verzameling afspraken over de manieren van communiceren tussen twee of meerdere computersystemen van eventueel verschillende merken.

Dit model deelt de communicatie in zeven lagen op. Daarom wordt dit ook wel het Zeven lagenmodel genoemd. Het OSI-model

- laag 7 Applicatie laag
- · laag 6 Presentatie laag
- · laag 5 Sessie laag
- laag 4 Transport laag
- · laag 3 Netwerk laag
- laag 2 Datalink laag
- laag 1 Fysieke laag

Laag 1: het laagste niveau kunnen we ons het best voorstellen als de fysieke hardware met de elektrische signalen. Deze zorgen ervoor dat we hardware aan elkaar kunnen knopen.

Laag 2: Datalink laag ofwel Media Access Controllaag zorgt ervoor dat een PC via een netwerkkaart met andere stations op het netwerk kan praten. In deze laag vindt foutcorrectie en flow control plaats.

Laag 3: Hier vinden we het IP-protocol. Deze laag zorgt voor adressering en routering.

Laag 4: Hier vinden we de subset TCP tegen (hierover later meer).

Overige lagen deze laten we hier buiten beschouwing.

Afbeelding: schematische weergave communicatie





# 6.3 De lagen 1 en 2

Zoals we in het OSI-model hebben kunnen zien, hebben we eerst een stukje "fysieke" hardware nodig om te kunnen communiceren. Dit kan een modem of een ethernetkaart interface zijn.

Voor de verdere uitleg gaan we uit van een ethernet omdat dit een soort netwerk- verbinding is die zeer veel gebruikt wordt en omdat we hierop de problematiek van het IP-protocol goed kunnen laten zien.

### Afbeelding: schematische weergave versturen data over ethernet



We gaan er vanuit dat station A met de server C wil communiceren. Het eerste wat er gebeurt is dat de stations op de tekening van een netwerkkaart en de benodigde driver software zijn voorzien.

Wat gebeurt er nu als station A met de server C op IP-niveau wil communiceren?

Op ethernet niveau heeft de driver software, waar de pakketjes als eerste doorheen moeten, geen notie van IPadressen. Hier worden MAC-adressen gebruikt. MAC-adressen zijn adressen die op ethernet bestaan uit 6 bytes, MAC-adressen worden hexadecimaal uitgeschreven. Bijvoorbeeld: 00.0f.12.34.aa.bb, deze adressen zijn gecodeerd in de hardware en in principe wereldwijd uniek.

Stations zijn hierdoor op een eenduidige wijze te identificeren. Wil station A nu pakketjes gaan sturen naar de server C dan moet hij zien te achterhalen wat het MAC-adres is van server C. Dit doen ze met het zgn. ARP (Address Resolution Protocol) protocol. Station A zal hiertoe een pakketje sturen met een speciaal bestemmming(=Destination) MAC-adres "ff.ff.ff.ff.ff" en als source (zijn eigen) MAC-adres het eigen adapter adres. Tevens wordt het gezochte IP-adres meegestuurd. Alle stations dienen dergelijke requests te bekijken en te vergelijken met het eigen IP-adres. Server C zal dit adres herkennen en een zgn. ARP-response frame sturen met zijn eigen MAC-adres en IP-adres. Station A zal deze data lokaal in zijn eigen ARP-tabel opslaan zodat hij die informatie in het vervolg niet meer hoeft op te zoeken. Vervolgens kan station A data naar server C gaan sturen. Normaal gesproken beschikt C reeds over een ARP-entry in de ARP-tabel en kan deze een response direct adresseren.

# 6.4 IP, Adressering en netwerkklassen

Het IP(v4)-adres is opgebouwd uit een viertal bytes (= 32 bits) en wordt dotted (= met puntjes tussen de bytes (= 8 bits)) decimaal uitgeschreven. Voorbeelden van IP adressen zijn: 10.1.1.1 en 145.82.5.254. Willen we iets meer van deze adressen weten dan zullen we op bit niveau verder moeten denken. Bij de uitgifte van adressen is de basis gelegd van een drietal typen netwerken, de zgn. klasse A-, B- en C- netwerken (type D en E worden bijna niet gebruikt).

### De netwerktypen uitgeschreven op bit niveau

```
1
                                 3
                                          Δ
                       2
          12345678 90123456 78901234 56789012
Bits
Klasse A Onnnnnn hhhhhhhh hhhhhhh hhhhhhh
Klasse B 10nnnnn nnnnnnn hhhhhhhh hhhhhhh
Klasse C 110nnnnn nnnnnnn nnnnnnn hhhhhhh
Klasse D 1110xxxx xxxxxxx xxxxxxx xxxxxxx
Klasse E 11110yyy yyyyyyy yyyyyyy yyyyyyy
nnn = het toegewezen netwerk deel van het nummer
hhh = het vrij te gebruiken host deel
xxx = speciale adressen t.b.v. multicasting
yyy = gereserveerde experimentele adressen
Een paar voorbeelden van IP adressen
010.001.001.001 00001010 00000001 00000001 00000001 = Klasse A
145.082.005.254 10010001 01010010 00000101 11111110 = Klasse B
Uit het bovenstaande schema kun je aflezen dat het adres 010.001.001.001 een klasse A adres is, immers het
begint binair met een nul. Adres 145.82.5.254 is een klasse B-adres omdat het met 10 begint. Het kennen van
deze adres ranges is belangrijk omdat Routers (hierover later meer) met deze grenzen rekening houden in hun
routetabellen.
```

### IPv6

Een structurele oplossing voor de schaarste in adresruimte van IPv4 is te vinden in de opvolger hiervan: IPv6. In IPv6 zijn er 128 bits beschikbaar voor een IP-adres, en is de theoretische bovengrens dus  $2^{128}$  =

2340.282.366.920.938.463.463.374.607.431.768.211.456 IP-adressen. Net als bij IPv4 geldt dat in de praktijk weer adressen gebruikt worden als netwerkadres en broadcastadres maar evengoed is het aantal te alloceren IP-adressen hiermee astronomisch. De IP-Converter ondersteund op dit moment alleen Ipv4.

### Hoe komen we aan een IP-adres?

Als we onze werkstation of onze server aan willen sluiten op een bestaand netwerk, dan is het eenvoudig. We kunnen dan een adres vragen aan de beheerder van het netwerk waarop we willen aansluiten.

Tegenwoordig worden dergelijke adressen veelal automatisch toegewezen (DHCP). Sluiten we onze PC of adapter bijvoorbeeld via een provider aan op het Internet dan zorgt het PPP protocol er bij het inloggen op het provider netwerk voor dat we automatisch een adres toegewezen krijgen.

Willen we zelf een netwerk bouwen dan hebben we een tweetal opties:

- We willen een nummerplan gebruiken waarmee we direct het internet opkunnen en/of in de toekomst kunnen communiceren met andere netwerken. We hebben dan een officieel geregistreerd netwerkadres nodig. Binnen de huidige policy dienen dergelijke adressen bij je ISP (Internet Service Provider) aangevraagd te worden.
- 2. Willen we niet direct koppelen aan het internet of kunnen we niet voldoende adressen krijgen, dan kunnen we gebruik maken van zogenaamde private adressen. Dit zijn adressen die gereserveerd zijn voor gebruik binnen het eigen netwerk. We kunnen hiermee niet naar buiten communiceren, maar we voorkomen in ieder geval dat we eventueel conflicten krijgen doordat we naar een extern adres willen, dat we intern gebruiken. Hiervoor zijn de volgende adressen ter beschikking gesteld:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

Ook met dergelijke adressen zijn er oplossingen te vinden uiteindelijk te communiceren met het internet. Ze bieden in bepaalde gevallen zelfs voordelen op beveiligingsniveau.

### DHCP

DHCP staat voor "Dynamic Host Configuration Protocol"

DHCP is een netwerkprotocol om dynamisch IP-adressen aan computers of netwerk apparatuur toe te kennen.

Elk apparaat binnen het netwerk dat geen vast IP-adres heeft ingesteld kan door middel van DHCP een IP-adres toegekend krijgen. Het grote voordeel is dat deze niet handmatig hoeven te worden ingesteld.

OPMERKING: De aangesloten apparatuur moet DHCP ondersteunen. De IP-Converter ondersteund DHCP.

### 6.5 Switches, routers en hubs

### Hub / Switch

Een Hub is net als een Switch een apparaat in de infrastructuur van een netwerk. \\In tegenstelling tot een switch is een Hub een 'dom' (laag 1 van het OSI-model, of bitniveau) apparaat en stuurt het een binnengekomen datapakketje simpelweg door naar alle poorten op het netwerk. Dit is meteen ook het nadeel van de Hub omdat op deze manier al het netwerkverkeer op alle aangesloten segmenten komt waardoor zogenaamde 'collisions' of botsingen van datapakketjes zich voordoen. Hierdoor daalt de algehele snelheid van het netwerk. Bovendien kunnen eventuele hackers die erin slagen een verbinding te maken met de Hub alle netwerkverkeer bekijken, ook verkeer dat niet voor hen bestemd is.



#### Afbeelding: een voorbeeld van een zgn. collision domain



Heden ten dage worden Hubs amper nog ingezet in nieuw opgebouwde netwerken, aangezien het prijsverschil met een goedkope switch quasi nihil is, en met deze laatste micro-segmentatie mogelijk is. Hierdoor krijgt elk apparaat zijn eigen netwerkpoort en netwerksegment, waardoor het niet gestoord wordt door datapakketten die niet voor dat segment zijn bedoeld (buiten broadcast en multicast verkeer). Aangezien een Hub niets meer is dan een multiport repeater, stuurt het evenwel alle elektrische signalen (waar datapakketten uiteindelijk worden uit opgebouwd) door naar alle aangesloten segmenten. Een switch opereert op laag 2 van het OSI-model, en kan zogenaamde frames herkennen in de elektrische signalen, en beslissen voor welk aangesloten segment zo'n frame bestemd is, en dan uitsluitend langs de poort van dat netwerksegment het frame versturen.

Een Switch is net als een Hub, een apparaat in de infrastructuur van een computernetwerk. In tegenstelling tot een Hub is een switch in staat om te schakelen tussen verschillende netwerksnelheden (meestal 10 Mbit en 100 Mbit) en stuurt een switch een datapakketje alleen maar door naar de poort waar de eindbestemming zich bevindt. Een switch zorgt op deze manier voor minder verkeer op het netwerk dan een hub.

### Werking

Een switch kan Ethernet, Token ring, Fibre Channel of andere types pakketgeschakelde netwerksegmenten verbinden tot één homogeen netwerk op het niveau van de OSI-datalinklaag.

Switches zijn zelflerend. Een netwerkpakketje met een nieuw adres komt langs een inkomende poort de switch binnen en wordt in eerste instantie via alle andere poorten het netwerk in gestuurd. Indien op een specifieke poort een antwoordpakketje komt weet de switch door het afzenderadres wie daar aangesloten is. De switch slaat dit adres en de poort op in zijn MAC-adressentabel en zal in het vervolg pakketjes met hetzelfde adres alleen nog naar die ene poort sturen. Regelmatig probeert de switch de andere poorten ook weer. Het kan immers zijn dat iemand een andere computer aangesloten heeft of een computer naar een andere poort verplaatst heeft.

Bij een hub kan het hele netwerk één collision domain zijn. Door het gebruik van een switch wordt dit opgesplitst naar elk verbonden netwerksegment. Enkel NIC's die rechtstreeks op een switchpoort verbonden zijn door een point-to-pointlink of direct verbonden hubs zullen dan een collision domain vormen. Op deze manier kunnen fullduplex point-to-point-verbindingen met een switch mogelijk gemaakt worden waar collisions uitgesloten worden.

In complexe netwerken waar redundante links liggen of waar men storingen wil opvangen kan het Spanning Tree Protocol gebruikt worden om lussen in het netwerk te vermijden.

Er bestaan managed switches en unmanaged switches. Zoals de naam het laat vermoeden kan je een managed switch beheren: QoS (quality of service: sommige soorten netwerkverkeer voorrang geven), VLAN's (virtuele LANs: de switch opsplitsen in verscheidene virtuele switches) of poorten reserveren voor specifieke computers.

### Router

Een Router is een apparaat of software op een computer die twee of meer verschillende computernetwerken aan elkaar verbindt Bijvoorbeeld internet en een bedrijfsnetwerk. Een Router is een soort schakelapparaat voor datapakketten die actief is op OSI-laag 3.

Om de juiste uitgaande poort te kiezen zoekt de Router het bestemmingsadres van het te routeren pakket op in de routeringstabel. Deze bestaat uit een tabel met IP-adressen of gegroepeerde IP-adressen (subnet), en het bijbehorende volgende knooppunt (next-hop). Het volgende knooppunt is doorgaans een buur-Router die gekoppeld is via een van de poorten van de Router.

Wanneer het bestemmingsadres routeerbaar is en dus in de Routeringstabel staat, zal de Router het bijbehorende volgende knooppunt gebruiken om de uitgaande poort te bepalen. Het binnenkomende IP-pakket wordt naar de uitgaande poort gestuurd.

De Router bouwt een routeringstabel op door route-informatie uit te wisselen met buur-routers. Zo ontstaat een volledig beeld van alle routes in het IP-netwerk. De Router zal op basis van het Kortste Pad Algoritme (Edsger Dijkstra) een routeringstabel opbouwen waarbij het kortste pad wordt gekozen naar de eindbestemming. Met

andere woorden: Het knooppunt dat gekozen wordt maakt deel uit van het kortste pad (shortest path)...

Een datapakket mag normaal maar door een bepaald aantal Routers heen gaan voor hij op zijn eindbestemming aankomt, bepaalt door de TTL (Time to Live) waarde van het pakketje. Een Router staat vaak in connectie met een gateway of functioneert zelf als dusdanig.

## 6.6 Routering

Als afstanden of het aantal stations te groot worden is het beter een Router in het netwerk te plaatsen. Een Router is een apparaat of software op een computer die twee of meerdere verschillende computernetwerken aan elkaar verbindt Een bijvoorbeeld is de koppeling van internet en een bedrijfsnetwerk. Een Router kan gezien worden als een schakelapparaat voor datapakketten die actief is op OSI-laag 3.

Om de juiste uitgaande poort te kiezen zoekt de Router het bestemmingsadres van het te routeren pakket op in de routeringstabel. Een routeringstabel bestaat uit een tabel met IP-adressen of gegroepeerde IP-adressen (subnet) en het bijbehorende volgende knooppunt (next-hop). Het volgende knooppunt is doorgaans een buur-router die gekoppeld is via een van de poorten van de router.

#### Hoe kan een station een server vinden die zich achter een router bevindt?

Om deze vraag te beantwoorden moeten we begrijpen hoe het samenspel tussen routers en werkstations en servers verloopt. Een van de functies van een router is er voor zorgen dat de broadcasts (o.a. voor ARP requests) zich niet door het hele netwerk kunnen verspreiden. Je kunt je voorstellen dat je PC geen tijd meer over zou houden voor normale zaken indien hij de ARP requests van alle stations op het hele internet (miljoenen pc's dus) voor zijn kiezen zou krijgen. Zo werkt het gelukkig ook niet bij een routeerbaar protocol.

Bij een routeerbaar protocol als IP hoeft een station slechts het MAC-adres van zijn lokale partners (op zijn eigen stukje ethernet = segment) op te zoeken en te onthouden. Bevind degene die hij zoekt zich achter een router dan hoeft het lokale station zijn data slechts af te leveren bij zijn "lokale" default gateway. Hij zal dus nog wel 1 ARP query uit moeten voeren om zijn default gateway te vinden. Dit samenspel vindt je schematisch terug in de volgende tekening.

Afbeelding: schematische weergave routering tussen 2 ethernet segmenten



Je begrijpt nu waarom je een default gateway nodig hebt om bijvoorbeeld op een externe server te kunnen komen. Hoe weet een station nu of zijn partner zich lokaal op zijn segment bevindt?

Hiervoor dient er op het station naast zijn IP-adres een netwerkmasker (subnet mask) geconfigureerd te worden. Hoe werkt dit nu?

Stel we hebben te maken met werkstation 145.82.13.254, die opzoek is naar server 145.82.15.23. Bevinden deze zich op het zelfde segment?

145	082	013	254
145	082	015	023
?	?	?	?

De adressen lijken vrij aardig op elkaar, dus het zou kunnen.

Toch kun je hier nog geen antwoord op geven want je kent het subnet masker niet die op de werkstations gedefinieerd is. Stel het masker is voor beide stations 255.255.255.0, bevinden ze zich dan op het zelfde subnet? Ook het subnet masker bestaat net als het IP-adres uit een reeks binaire enen en nullen. De positie (hoeveelheid) van de enen bepalen het netwerkdeel van het adres en het stuk van het IP-adres dat nog overblijft. De nullen laten zien welke ruimte er voor host (=stations) beschikbaar is op dat deel van het netwerk, verder subnet genoemd. Nu gaan we bepalen of de bovengenoemde adressen zich op hetzelfde subnet bevinden. Hiertoe dienen we de adressen en het masker binair uit te schrijven (de IP-stack vergelijkt dit immers ook op bit niveau).

Subnet mask 255.255.255.0 11111111 1111111 1111111 00000000 De IP adressen Station A 145.82.13.254 10010001 01010010 00001101 1111110 Station B 145.82.15.23 10010001 01010010 00001111 00010111 Het bepalen van de subnetten waarop de stations zich bevinden:



Station A 145.82.13.254 10010001 01010010 00001101 00000000 Station B 145.82.15.23 10010001 01010010 00001111 00000000 Terug gerekend naar een decimale notering

### IP-adres netwerk subnet

Station A 145.82.13.254 145.82.0.0 145.82.13.0 Station B 145.82.15.23 145.82.0.0 145.82.15.0 We zien dus dat de beide stations zich wel op hetzelfde (klasse B) netwerk bevinden maar ook dat de beide stations zich op verschillende subnetten bevinden. Station A moet dus verkeer via zijn default gateway naar station B sturen.

Het bovenstaande voorbeeld was op het blote oog ook nog wel te herleiden aangezien het hostdeel precies op de punt begon.

Stel dat het masker 255.255.248.0 zou zijn? Liggen de beide stations dan op het zelfde subnet. We gaan de zaak weer uitschrijven.

### Subnet mask

255.255.248.0 11111111 11111111 11111000 00000000

De IP adressen

Station A 145.82.13.254 10010001 01010010 00001101 1111110 Station B 145.82.15.23 10010001 01010010 00001111 00010111 Het bepalen van de subnetten waarop de stations zich bevinden:

Station A 145.82.13.254 10010001 01010010 00001000 00000000 Station B 145.82.15.23 10010001 01010010 00001000 00000000 Het bepalen van het laatste adres, het zgn. local broadcast adres:

Station A 145.82.13.254 10010001 01010010 00001111 1111111 Station B 145.82.15.23 10010001 01010010 00001111 1111111

Terug gerekend naar een decimale notering:

IP-adres netwerk subnet broadcast adres

Station A 145.82.13.254 145.82.0.0 145.82.8.0 145.82.15.255

Station B 145.82.15.23 145.82.0.0 145.82.8.0 145.82.15.255

Nu liggen de beide werkstations wel op hetzelfde subnet. Je ziet nu ook duidelijker het nut van het binair uitschrijven van adressen om bijvoorbeeld het netwerk te bepalen en het laatste adres in dat netwerk, het broadcast adres.

Het broadcast adres wordt gebruikt om bijvoorbeeld testframes, zogenaamde ping pakketjes, naar alle stations op dat subnet te sturen. Voor werkstations kunnen de adressen 145.82.8.1 tot en met 145.82.15.254 gebruikt worden, ruim 2000 adressen. Het volgende subnet (als we hetzelfde masker zouden gebruiken) loopt van 145.82.16.0 tot en met 145.82.31.255.

### **Default Gateway**

Hoe weet de default gateway (de Router) nu waar hij de pakketjes van station A voor station B naar toe moet sturen?

In tegenstelling tot de overige IP-stations beschikt een Router over tabellen (de Route tabellen), waar per (sub)netwerk staat opgenomen waar hij de data voor dat specifieke (sub)netwerk naar toe moet sturen (naar welk IP-adres). We gaan in het volgende voorbeeld weer uit van het eerst gekozen subnetmask 255.255.255.0.

De Router zal hierbij de volgende stappen doorlopen:

- 1. Is het pakketje voor mij bestemd? Ook een Router heeft IP-adressen en je kunt bijvoorbeeld SNMP-berichten naar een Router sturen om bepaalde beheers informatie op te vragen. Hij kent zijn eigen interface adressen en kan dus bepalen of het pakketje voor hem zelf bestemd is. Is dit niet het geval dan gaat hij verder met de volgende stap.
- 2. Ken ik het netwerk lokaal? Is dit het geval dan zal de router kijken of hij een ARP entry heeft voor station B in zijn ARP tabel. Is dit niet het geval dan zal er een ARP request verstuurd worden voor het MAC-adres van station B. Hierna zal na een reply de data verstuurd worden richting station B. Wat station B verder met de data doet (en of de data aankomt), dat weet de Router niet. Hij levert slechts een zgn. best-effort dienst. Kent de Router het netwerk echter niet lokaal, dan gaat hij verder met de volgende stap.
- 3. Heb ik een route naar het betreffende netwerk? In het eenvoudigste geval is in de configuratie van Router A ingebracht (met een "route add ……" commando o.i.d.) dat het netwerk 145.82.15.0 zich ergens achter IP-node 2.1 bevindt. Kent hij het netwerk en heeft hij de laag 2 (MAC) info al dan kan hij het pakketje direct doorsturen. In het geval van een seriële verbinding is de laag 2 verbinding in principe reeds bij het opzetten van de verbinding gemaakt.
- 4. Indien en geen specifieke route aanwezig is, is er wellicht een default route aanwezig. Deze route wordt

gebruikt voor alle bestemmingen waarvoor op een andere manier geen route te vinden is.

5. Lukt ook dit niet, dan zal de Router naar het werkstation een zgn. ICMP- pakketje sturen met de informatie "network unreachable", wat zoveel betekend, ik kan het netwerk niet vinden en heb het pakketje in de bittenbak gegooid.

Vervolgens worden deze stappen ook door de opvolgende Routers doorlopen totdat het netwerk gevonden is waarop station B zich bevindt.

### Her-routering en de opbouw van route tabellen.

Stel nu dat de verbinding tussen Router B en D uitvalt. Indien routes met de hand gedefinieerd zouden zijn, ziet Router B dat hij het pakketje niet verder kan sturen richting D. Hij weet echter niet dat er een alternatieve verbinding bestaat via Router C. Dat is hem immers nooit verteld.

Dit probleem is op te lossen door de Routers "dynamisch" route informatie te laten uitwisselen d.m.v. een routing protocol. Dit heeft als bijkomend voordeel dat op het moment dat er een netwerk (lees interface met een IP-adres en masker) aan een Router wordt toegevoegd, dit niet meer op alle individuele Routers gedefinieerd hoeft te worden. Afhankelijk van het gebruikte protocol kunnen vaste (overal de zelfde (bijv. RIP)) of variabele met (per subnet) verschillende hoeveelheden hosts (bijv. OSPF)) gedefinieerd worden.

# 6.7 DNS

In het bovenstaande voorbeeld zijn we er steeds vanuit gegaan dat station A wist welk IP-adres station B heeft. Dit werkt als je slechts een beperkte hoeveelheid stations hebt die naar station B hoeven. Immers wil je station B verplaatsen naar een ander subnet, dan zul je alle stations die naar station B willen hiervan op de hoogte moeten stellen en zo nodig moeten herconfigureren.

Stel station B zou in werkelijkheid de <u>www.asb.nl</u> server zijn. Wij hebben geen idee wie er allemaal een bookmark naar onze site gemaakt hebben, dus kunnen we ze ook niet informeren.

Om dit probleem te voorkomen is het Domain Name System (= DNS) opgezet waarbij een vertaalslag gemaakt wordt van namen naar IP-adressen.

# 6.8 **Protocollen / Poortnummers**

We introduceren hier weer even het oude concept van server en werkstation. De server is de gene die de service aanbiedt, het werkstation de gene die de service wil afnemen. Dit is even tamelijk zwart-wit gesteld. In de praktijk is de scheidslijn lang niet altijd zo duidelijk te trekken. Stel je wil een webserver en FTP-server beschikbaar stellen (zodat men bij je kan surfen en files downloaden). Hoe kan de "server" nu bepalen of iemand iets wil downloaden via FTP of komt browsen via WWW?

### Protocolnummers

Kijken we naar het IP-protocol dan komen we een aantal lagen tegen. Het eerste wat je tegen komt is een source en destination IP-adres. Het destination adres wordt gebruikt om het pakket te routeren. Het source adres wordt door de andere partij gebruikt om het pakket weer terug te kunnen sturen. Vervolgens komen we het protocolnummer tegen.

Binnen het IP-protocol zijn een aantal specifieke protocollen gedefinieerd waarvan de protocollen TCP(6), UDP(17) en ICMP(1) de bekendste zijn.

De verschillende protocollen hebben zo hun eigen eigenschappen. Zo is het ICMP protocol een puur lowlevel protocol bedoeld voor het storing zoeken en opvragen van netwerk parameters. TCP en UDP zijn de protocollen waar we hier iets dieper op in zullen gaan.

### UDP

Dit is het eenvoudigste protocol omdat het een zogenaamde connectionless service levert. Connectionless wil zeggen dat het protocol geen idee heeft of het eerste dan wel het laatste pakketje van een sessie verstuurd wordt. Er wordt ook niet bijgehouden of alle pakketjes wel goed bij de ontvangende kant aangekomen zijn. Dit laat het protocol allemaal over aan de hoger liggende lagen (denk nog eens terug aan het OSI-model). Willen applicaties dus zeker weten of alle pakketjes netjes aangekomen zijn dan moeten ze dit zelf controleren (vragen aan de partner aan de andere kant). Typisch toepassingen voor dit protocol zijn het uploaden van configuratie files naar devices die mogelijk onvoldoende resources hebben voor een TCP- implementatie. Het sturen van systeemberichten (TCP zou in dergelijke gevallen te traag dan wel teveel overhead opleveren als er slechts 1 pakketje verstuurt hoeft te worden) en een nieuwe toepassing is het gebruik bij telefonie over IP (hier heeft hertransmissie immers geen zin, dan maar een kraakje).

### ТСР

TCP biedt een zogenaamde "connection oriented" verbinding. Dit wil zeggen dat het protocol voor de verbinding zorgt en daardoor garanties kan bieden zolang er een verbinding bestaat. TCP zorgt dan ook voor de nodige hertransmissie doordat de andere zijde zgn. ACK (acknowledgement) pakketjes stuurt.

#### www.asb.nl



Daarnaast kent TCP een zgn. flowcontrol mechanisme waardoor het kan anticiperen op de beschikbare bandbreedte. Als verbindingen namelijk overbelast raken zullen er op de tussenliggende netwerken vertragingen optreden of zelfs pakketten weggegooid worden. Als bepaalde pakketten trager dan wel helemaal niet aankomen kan de zendende kant gas terug nemen. Hierdoor hebben de tussenliggende netwerken minder belasting. Als alle stations zich hier netjes aan houden, houdt de congestie (het verstopt raken van het netwerk) vanzelf op en kan er daarna langzaam weer meer data verstuurd worden.

### Poortnummers

Vervolgens worden binnen de protocollen poortnummers toegepast om de verschillende services adresseerbaar te maken. Deze poortnummers (ook wel sockets genoemd) worden gebruikt door de protocolstack om te bepalen naar welk programma de data gerouteerd moet worden.

Programma's die luisteren op dergelijke poorten (Deamons) moeten aan de TCP stack vertellen dat de data die op bijvoorbeeld poort 80 (= www) binnen komt doorgestuurd moet worden naar de webserver.

Poort 21 daarentegen is in principe gereserveerd voor FTP-verkeer. Deze poorten kun je in principe als beheerder vrij kiezen, echter voor de meeste protocollen zijn poorten gereserveerd. De cliëntapplicaties zullen deze poorten gebruiken als er verder niets anders opgegeven wordt.

Met de hulp van de IP-adressen, protocolnummers en poortnummers zullen per sessie unieke combinaties ontstaan waardoor het gelijktijdig starten van eventueel meerdere sessies naar verschillende services mogelijk is.

- Een aantal poortnummers en hun toepassingsprotocol zijn:
  - 20 FTP (data)
  - 21 FTP (besturing)
  - 22 SSH
  - 23 Telnet
  - 25 SMTP
  - 53 DNS
  - 69 TFTP
  - 80 World Wide Web HTTP
  - 88 Kerberos
  - 110 POP3
  - 123 NTP server
  - 137 Netbios Name Service
  - 389 LDAP
  - 443 HTTPS
  - 4433 IP-Converter Remote Management Server
  - 5060 IP-Converter SIP
  - 7000 IP-Converter RTP
  - 31000 IP-Converter
  - 31001 IP-Converter

# 7 Algemene informatie

### WAARSCHUWING

Om het gevaar van brand of een elektrische schok te voorkomen adviseren wij de IPC niet bloot te stellen aan regen of vocht en het apparaat niet onder spanning te openen. Voorkom blootstelling van de IP-Converter aan fel zonlicht, hoge temperaturen en stof. Probeer in geen geval het apparaat zelf te repareren want dan vervalt uw recht op garantie. Laat reparaties aan de **erkende vakman** over.

#### **GARANTIE BEPALING**

De garantie van de IP-Converter komt direct te vervallen wanneer de IP-Converter in mechanische of elektronische zin wordt gewijzigd. Dit is ook van toepassing wanneer de montagegaten worden beschadigd (opgeboorde gaten kunnen de multiple layer print intern beschadigen). **Reparatiezendingen dienen retour te worden gestuurd in de originele antistatische verpakking**.



### SESD VOORKOMEN

Schade door ontlading van statische elektriciteit (ESD) komt voor als printplaten of componenten verkeerd behandeld worden. Dit kan volledige uitval of terugkerende fouten tot gevolgen hebben. Let op de volgende richtlijnen voordat u het systeem installeert of onderhoud pleegt:

- Draag altijd een pols- of enkelband om ESD te voorkomen als u met elektronische onderdelen werkt. Verbind een einde van de band met een ESD-stekker of met een ongeverfd metalen onderdeel op het systeem (aardpunt);
- Pak printen alleen bij de hoeken van de printplaat vast. Vermijd het aanraken van de componenten op de printplaat;
- Vermijd contact tussen de printen en kleding. De polsband beschermt de print alleen tegen ESD-voltages op het lichaam; ESD-voltages op kleding kunnen nog steeds schade veroorzaken.

# 

De **IP-Converter** voldoet aan de eisen van de van toepassing zijnde Nieuwe Aanpakrichtlijnen, die gesteld zijn volgens de CE. Dit label bevindt zich op de onderzijde van het product.

Dit product leent zich alleen voor de in deze handleiding aanbevolen installatie en installatiewijze, gebruikt met de apparatuur en hulpmiddelen in de juiste omgeving zoals omschreven. De leverancier wijst elke verantwoording van de hand voor elke buiten de omschrijving gebruikte applicatie en hulpmiddelen of andere dan omschreven omgeving.

#### REINIGEN

Maak indien nodig de buitenzijde van de IP-Converter schoon met een zachte doek, eventueel licht bevochtigd met wat afwasmiddel. Gebruik geen reinigingsmiddelen zoals alcohol, ammoniak of wasbenzine om het apparaat te reinigen. Dit zou het kunnen aantasten.



### NIET WEGGOOIEN !

Bij beëindiging van de levensduur van dit apparaat moet u het niet weggooien, maar kunt u het weer inleveren bij uw dealer of fabrikant. Gooi de IP-Converter nooit bij het gewone huis- en tuin- en keukenafval.



# 8 BIJLAGE A Geteste panelen

In onderstaande lijsten staan de panelen waarvan bij ASB-Security BV bekend (getest) zijn dat deze communiceren met de IP-Converter. Zover bekend hebben we de software versie vermeld. Indien panelen niet in onderstaande lijsten vermeld zijn, hoeft dit niet te betekenen dat deze niet kunnen communiceren met de IP-Converter. Ze zijn alleen niet getest door ASB-Security BV.

### TABEL Geteste protocollen / systemen analoog

Ţ	So	Kia	X	Å ℃	(de CII	Mu	CII	Mu	Fa	Fa	ЧU
pe	ftw	9zei	AIS	SIA	D 12 9fau	lti \	1		st F	st F	/Do
cc	are	r ve		Int	400 11t)	Acc	<u>300</u>	S00	orn	orn	MU
	Ver	rsie	Ë	Ë	Hz/	Õur	Hz/	Dun Hz	nat	nat	loa
	sie		10	10	230	<b>#</b>	210	210 1t	140	160	9
			ω	S S	РОН		Ĥ	P	)0 H	о т	
				ulti	N		N	N	z	z	
LaSmo Security Solutions											
DSC PC5010	V1.03		V								
DSC EC6360 v3.2			V		V						
DSC EC6400 v3.0			V		V						
DSC NT 9005 V1.0EU			V		V						
DSC PC1864			V		V						
Lobeco											
Nx-8			V		V						
GE-Security											
CD3401 / RD6201			V		V				V	V	
CD15001			V		V						
ATS V04.07.10			V		V						
ATS 3001			V		V						
ATS 1000A	008.008.31		V								
CS275 S1			V		V						
ADI		•									
Galaxy Dimension	V6.70		V								V
Galaxy 8	V4.31	V2.00	V				V				
		V4.01									
Galaxy G2-20+	V1.5		V								V
Galaxy G2-40+	V1.5		V								V
Galaxy G3	V4.31				V						
Galaxy 16+			V								
Galaxy 60	V4.32		V		V						
Galaxy XL	V2.18	V5.05	V								V
Vista 25					V						
Vista 120NL	V2.5				V						
Lynx					V						
Powermax					V						
Alphatronics											
Alphavision 96	V3.6		V								
Honeywell											
OMNI 624EU	Rev 2.5				V						
OMNI 848EU	Rev 2.5				V						
Safe Box					V						

Div.							
Eurotec freelink				V			
Bosch Easy Serie				V			
Jablotron				V			
Texecom Premier 816	V10.6	V					
Scantronics 8136i		V					
Paradox NE96		V		V			
FBI XL3				V			
Rokonet ProSys 40	V1.20e	V		V			
Guardall RX16i	V4.21c	V		V			
Satel Integra 32		(X)SIA SATEL	(X)SIA SATEL	(			
Scantronic K9752				V			

# TABEL Geteste systemen serieel

Type CCS	versie	Interface	Interface Versie
Aritech CD3401 V1.4	V6.0 (101298-4)	MPI-232V2	2.30
Aritech CD150.01	6.22	MPI-232V2	2.30
Galaxy 8		Externe RS232 interface Rev 1.1	V2.01, CS: 047D
Galaxy 8		Externe RS232 interface Rev 1.1	V1.20
NX-8		NX-584	V.01F0 1.06
DSC Power Series		DVACS	PC50XX V2.X
DSC Power Series		DVACS	V3.X
DSC MAXSYS		DVACS	PC4401 V1.1
DSC MAXSYS		DVACS	PC40XX V2.X
DSC MAXSYS		DVACS	PC40XX V3.X
ATS3000, 4000, 4500	Vanaf versie V04.06.44	ATS1801	

# 9 BIJLAGE B Frequently Asked Questions

- Vraag: Waarom kan ik niet meer inloggen na een update?
  - Antwoord: Als de tijdelijke internet-bestanden verwijderd worden kan er weer ingelogd worden.
- Vraag: Waarom geeft de IP-Converter een E13?
  - Antwoord: Als het paneel geen data stuurt, geeft de IP-Converter een E13. NB: het gebruikte paneel is een Galaxy 60. Het paneel werkt goed. Het paneel gaat offline waardoor er een E13 verschijnt.
- Vraag: Waarom gaat het puntje in het display van de IP-Converter knipperen in plaats van constant branden?
  Antwoord: Eén van de verbinding (Primary of Backup) staat in Failed To Connect.
- Vraag: Waarom komt er een "A" in het display van de IP-Converter te staan?
  - Antwoord: Bij doorsturen van een alarmmelding komt in het display van de IPC even een "A" te staan.
- Vraag: Hoe kan ik controleren of de juiste poorten openstaan?
  - Antwoord: AoIP portscanner: www.asb.nl/portscanner
- Vraag: Waarom heb ik geen lokale lijnspanning op de IP-Converter?
  - Antwoord: Als de LAN stekker eruit is en als de GPRS in FTC staat dan wordt de lokale lijnspanning uitgeschakeld. Als er geen GPRS is geconfigureerd dan alleen als de LAN stekker eruit is (link down).
- Vraag: Waarom heeft mijn IP-Converter GPRS wel lokale lijnspanning terwijl er geen Ethernet link is?
  - Antwoord: Bij een IP-Converter GPRS gaat de lijnspanning pas uit als de Ethernet link er niet is EN de GPRS het ook niet doet.
- Vraag: Hoe groot zijn de berichten die via de GPRS verstuurd worden
  - Antwoord: Een melding is ongeveer 512bytes en een controle of de GPRS verbinding actief is ongeveer 256bytes.
- Vraag: Hoe groot zijn de berichten die via de vaste IP verbinding verstuurd worden (netwerkbelasting)
  - Antwoord Een poll bericht is ongeveer 150bytes, een controle van de verbinding is ongeveer 20 bytes en een melding is ongeveer 150bytes.
- Vraag: Kan de IPC geupdate worden via GPRS in plaats van via de vaste ethernet verbinding.
  - Antwoord: Dit is niet mogelijk. Dit komt onder andere dat er meteen een download plaats vindt waarbij de datalimiet kan worden bereikt omdat de software update ongeveer 3MB groot is. Verder is de functionaliteit niet aanwezig om dit te ondersteunen.
- Vraag: Welke verbindingen worden er gebruikt om VoP data te versturen?
  - Antwoord: Alleen de primaire (vaste) IP verbinding wordt gebruikt om VoP data te versturen.
- Vraag: Bij vervanging van de IP-Converter, moet er dan iets aangepast worden in de ontvanger van de meldkamer
  - Antwoord: De ontvanger heeft als unieke sleutel klant nummer + MAC adres van de IP-Converter. Hierdoor dient wanneer een IP-Converter vervangen wordt de entry uit de ontvanger verwijderd te worden. Wanneer op locatie de nieuwe IP-Converter aangesloten wordt dan accepteert de ontvanger weer de nieuwe combinatie klant nummer + MAC adres. Let wel op, wanneer je de IP-Converter laat verwijderen uit de ontvanger moet je zeker weten dat deze niet meer aan de lijn hangt, anders meldt deze IP-Converter zich natuurlijk bij de volgende poll weer aan.

# 10 BIJLAGE C Poorten Overzicht

Hieronder is een overzicht welke poorten er gebruikt worden door de IP-Converter.

Functie	Soort	Poort Nummer	Protocol	Richting
Alarm		31000	UDP	Uitgaand
		31001	UDP	Uitgaand
Verification of Performance	VoP	32000	UDP	Uitgaand
Remote Management Server	RMS	4433	TCP	Uitgaand
Update Server	TFTP	69	UDP	Uitgaand
Network Time Protocol	NTP	123	UDP	Uitgaand
VoIP	SIP	5060	UDP	Ingaand*/Uitgaand
	RTP	7000	UDP	Ingaand*/Uitgaand
	STUN	3478	UDP	Uitgaand
Help Page	HTTP	80	TCP	Uitgaand

\* Deze poort dient geforward te worden naar het IP-adres van de IP-Converter

Voor up/downloading is er minimaal 150Kbps (voor zowel upload als download) vrije bandbreedte vereist.

# 11 BIJLAGE D Inbedrijfstelling

Deze procedure stelt u in staat de Alarm IP-Converter te programmeren en te installeren.

- 1. Sluit de netwerkkabel aan;
- 2. Koppel het alarmpaneel aan de IP-Converter (Tip en Ring of serieel);
- 3. Breng de IP-Converter op *spanning* door klemmen: '+13V' en 'GND' aan te sluiten; Op het display zal een 'U' zichtbaar zijn. Hierna wordt het versie nummer van de IP-Converter weergegeven;
- 4. Controleer of de laatste *software versie* actief is; Is de software in de IP-Converter niet de laatste, voer dan een update uit. Zie 'Remote software update';
- 5. Stel in het paneel het IP-adres van de *ontvanger*, uitgevuld met **nullen**, in. (Voorbeeld: 080112203003)
- 6. Optioneel
  - 1. Druk één maal op de drukknop. Het *IP-adres* wordt getoond. Open een Internet Explorer en type het IPadres in de adresbalk.
    - Login op de IP-Converter;
  - 2. Stel in het paneel of in de IP-Converter het klantnummer en Receiver IP-adres in. (RCT parameters);
- 7. Seriële koppeling
  - Druk één maal op de drukknop. Het *IP-adres* wordt getoond. Open een Internet Explorer en type het IPadres in de adresbalk. *Login* op de IP-Converter;
  - Stel in het paneel en in de IP-Converter het juiste protocol in. (Configuratie→ Alarm Interface);
- 8. Maak een melding controleer of deze bij het beheercentrum en bij de meldkamer binnenkomt;
- 9. Indien de meldingen binnenkomen is de IP-Converter opgeleverd.

# **12 BIJLAGE E Flowchart Inbedrijfstelling**





# 13 BIJLAGE E ATS 1 t/m 6 configuratie

In onderstaand tabel zijn de instelling opgenomen voor de Europese ATS 1 t/m 6 richtlijnen volgens de NEN-EN 50131-1:2006. Deze instellingen dienen in de *Web Interface Configuratie – RCT parameters* ingevuld te worden. Zie paragraaf 13.1.1 voor meer informatie.

### Alleen via een primaire verbinding

Verbindingstype	ATS Configuration	RCT 1 reporting time
ATS 1	Single Path 2	
ATS 2	Single Path 2	
ATS 3	Single Path 2	
ATS 4	Custom	300 Minutes
ATS 5	Single Path 4	
ATS 6	Single Path 6	

### Alleen via een GPRS verbinding

Verbindingstype	ATS Configuration	Connection type	Reporting time when RCT1 is active	Reporting time when RCT 1 is deactive
ATS 1	Custom	GPRS	24 hours	24 hours
ATS 2	Custom	GPRS	24 hours	24 hours
ATS 3	Custom	GPRS	24 hours	24 hours
ATS 4	Custom	GPRS	24 hours	300 minutes
ATS 5	Custom	GPRS	24 hours	3 minutes
ATS 6	Custom	GPRS	24 hours	20 seconds

### Configureer RCT1 als volgt:

RCT1			
Replace account code	Actief		
Account code	< Zelfde account code als bij RCT 2>		
Receiver IP address via DTMF	Niet actief		
Receiver IP address	127.0.0.1		
Reporting time	24 hours		