

(19)



Octrooi Centrum
Nederland

(11) **2000632**

(12) **C OCTROOI**²⁰

(21) Aanvraag om octrooi: **2000632**

(51) Int.Cl.:
H04L29/06 (2006.01) **H04N7/18** (2006.01)
G08B25/00 (2006.01)

(22) Ingediend: **07.05.2007**

(41) Ingeschreven:
10.11.2008 I.E. 2009/01

(47) Dagtekening:
10.11.2008

(45) Uitgegeven:
05.01.2009 I.E. 2009/01

(73) Octrooihouder(s):
**Spectator Intellectual Properties B.V. te
Geertruidenberg.**

(72) Uitvinder(s):
**Marinus Adrianus Hendrikus Kloonen te
Oosterhout.
Rolf Martijn van den Hoek te Dordrecht.
Gerrit Gijsbert Ermstrang te Giessen.
Godefridus Johannes van de Water te
Nieuwkuijk.
Hubertus Franciscus Maria Hermes te
Sittard.**

(74) Gemachtigde:
**Ir. H.Th. van den Heuvel c.s. te 5200 BN
's-Hertogenbosch.**

(54) **Systeem en werkwijze voor het via, een ten minste gedeeltelijk publiek communicatienetwerk, uitwisselen van data tussen een eerste dataverwerkingssysteem en een tweede dataverwerkingssysteem.**

(57) Communicatiesysteem voor het via een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk uitwisselen van data tussen een eerste dataverwerkingssysteem en een tweede dataverwerkingssysteem, omvattende een eerste dataverwerkingssysteem, ingericht om te communiceren volgens een communicatieprotocol, waarbij het eerste dataverwerkingssysteem via een eerste koppeling verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk en een tweede dataverwerkingssysteem, omvattende ten minste één dataverwerkingssysteem, ingericht om te communiceren volgens het communicatieprotocol, waarbij het tweede dataverwerkingssysteem via een tweede koppeling verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk met het kenmerk dat ten minste één van de koppelingen een voor dataverkeer volgens het communicatieprotocol onoverbrugbare verbinding omvat.

NL C 2000632

De inhoud van dit octrooi komt overeen met de oorspronkelijk ingediende beschrijving met conclusie(s) en eventuele tekening(en).

Octrooi Centrum Nederland is een agentschap van het ministerie van Economische Zaken

Systeem en werkwijze voor het via, een ten minste gedeeltelijk publiek communicatienetwerk, uitwisselen van data tussen een eerste dataverwerkingssysteem en een tweede dataverwerkingssysteem

- 5 De onderhavige uitvinding heeft betrekking op een inrichting en werkwijze voor het via een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk uitwisselen van data tussen een eerste dataverwerkingssysteem en een tweede dataverwerkingssysteem. In het bijzonder heeft de onderhavige uitvinding betrekking op een systeem voor het bewaken van een eerste locatie vanaf een tweede locatie,
10 gebruikmakend van een dergelijke inrichting.

- Bij het via een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk verzenden van data van een eerste dataverwerkingssysteem, naar een tweede dataverwerkingssysteem, via een ten minste gedeeltelijk voor het publiek
15 toegankelijk communicatienetwerk, zoals het internet, wordt gebruik gemaakt van communicatieprotocollen, veelal het internetprotocol of een vergelijkbaar protocol. Naast verscheidene voordelen hebben deze protocollen het nadeel, dat kwaadwillenden, die toegang hebben tot het betreffende ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk, zich via een dergelijk communicatieprotocol
20 relatief eenvoudig toegang kunnen verschaffen (ook wel “hacken” genoemd) tot met het communicatienetwerk verbonden dataverwerkingssystemen, wanneer zij ergens op het communicatienetwerk kans zien zich als “trusted party” voor te doen. Vaak doordat ze handig gebruikmaken van fouten in de software, gebruikersfouten en/of instellingsfouten van bijvoorbeeld firewalls, routers of toepassingen die verbonden zijn
25 met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk.

- Bekende beveiligingstechnieken, zoals firewalls, die doorgaans als softwareoplossing geïmplementeerd zijn, zijn nog steeds te omzeilen en vormen zodoende een veiligheidsrisico. Het functioneren van de met het ten minste gedeeltelijk voor het
30 publiek toegankelijke communicatienetwerk verbonden dataverwerkingssystemen, en de via die systemen gekoppelde andere systemen zijn dus benaderbaar. De dataveiligheid valt aldus niet te garanderen.

Een tweetal toepassingsgebieden waarin dit in het bijzonder als bezwaarlijk wordt, zijn die van beveiligings- en zorgsystemen, voor ondermeer het op afstand bewaken van een locatie of object, of het communiceren met die locatie of dat object.

- 5 In geval van een beveiligingssysteem kunnen dergelijke systemen de noodzaak van de aanwezigheid van een fysiek persoon op de te bewaken locatie opheffen, de hoeveelheid aanwezig bewakingspersoneel reduceren, het veiligheidsgevoel van aanwezig bewakingspersoneel verhogen, en ontstaat de mogelijkheid de bestaande bewaking te controleren door middelen te verschaffen voor het op afstand kunnen bewaken van die
- 10 locatie, vaak een (bedrijfs-)pand, zoals een bank of een winkelpand, bijvoorbeeld dat van een juwelier.

- Een beveiligingssysteem omvat bijvoorbeeld een sensor zoals een deurcontact of een bewegingsmelder op een eerste locatie, voor het opwekken van een alarmsignaal, dat
- 15 naar een tweede locatie wordt gezonden. Dat gebeurt veelal via een al dan niet speciaal toegewezen infrastructuur, bijvoorbeeld PSTN of ISDN.

- Op de tweede locatie - een meldpunt, alarmcentrale of waarnemingsstation - wordt het signaal omgezet in een voor een bewaker waarneembaar signaal, zoals een zichtbaar,
- 20 hoorbaar of voelbaar signaal. De bewaker op de tweede locatie kan vervolgens beslissen welke opvolging hieraan dient te worden gegeven. In sommige gevallen wordt een alarmsignaal ook doorgegeven aan hulpdiensten zoals de politie of een particuliere bewakingsdienst.

- 25 Een probleem van een systeem zoals hierboven beschreven is echter is dat een groot deel van de door deze systemen gegenereerde alarmsignalen niet opgewekt wordt door de aanwezigheid van een inbreker op de te bewaken locatie, maar door dieren, weersomstandigheden (zoals onweer), verkeerd afgestelde of bediende apparatuur, onvoldoende technisch onderhoud of andere redenen, zodat een vals alarm wordt
- 30 gegenereerd.

Een gevolg daarvan is dat hulpdiensten niet meer in actie komen op basis van een alarmsignaal en dat een particuliere bewakingsdienst moet worden ingeschakeld of dat een eigenaar of beheerder van de locatie zelf op inspectie moet gaan.

Het wordt daarom steeds meer gebruikelijk om in middelen te voorzien voor het verifiëren van het alarmsignaal, die een operator in het waarnemingsstation waar het alarmsignaal binnenkomt in staat stellen om de juistheid van het alarmsignaal te kunnen vaststellen. Ook kan het zo zijn dat een bewaker in een waarnemingsstation los van enige alarmmelding op eigen initiatief – bijvoorbeeld op gezette tijden – een inspectie dient uit te voeren, of juist bekend is met de komst van bijvoorbeeld een toeleverancier op een tijdstip dat de locatie onbemand danwel onbewaakt is. Om op dat moment in staat te zijn de locatie te bewaken, worden naast eventuele sensoren zoals contacten en bewegingsmelders audiovisuele registratiemiddelen zoals camera's geplaatst, waarmee een operator na het ontvangen van een alarmmelding zich een gedetailleerder beeld kan vormen van de eerste locatie.

De genoemde audiovisuele registratiemiddelen voor het verifiëren van het alarmsignaal kunnen deel uitmaken van een gesloten televisiesysteem, dat veelal geïmplementeerd is met behulp een eerste dataverwerkingssysteem, dat ingericht is om te communiceren via een communicatieprotocol, zoals het internetprotocol. Om gegevens uit te wisselen tussen de eerste locatie en de tweede locatie, en eventueel ook locaties van hulpdiensten, kan het dataverwerkingssysteem op de eerste locatie via een communicatieverbinding in verbinding staan met een dataverwerkingssysteem op de tweede locatie dat eveneens is ingericht om te communiceren via het betreffende communicatieprotocol, zoals het internetprotocol. Gebruikelijkerwijs zijn het eerste dataverwerkingssysteem en het tweede dataverwerkingssysteem via een ten minste gedeeltelijk publiek netwerk verbonden, waarop om redenen van eenvoud van communicatie een communicatieprotocol wordt bedreven, bijvoorbeeld het internetprotocol. Het is verder gebruikelijk dat het alarmsignaal zelf via een andere verbinding, zoals de hierboven genoemde toegewijde telefoonverbinding wordt verzonden.

Aldus worden data, bijvoorbeeld beeldmateriaal, geregistreerd op een te bewaken locatie, vanaf een eerste dataverwerkingssysteem op de te bewaken locatie verzonden naar een tweede dataverwerkingssysteem op het waarnemingsstation, en worden opdrachtdata, bijvoorbeeld voor het bedienen van registratiemiddelen voor het opwekken van het beeldmateriaal, verzonden van het tweede dataverwerkingssysteem

op het waarnemingsstation naar het eerste dataverwerkingssysteem op de eerste locatie. Het gevaar dat deze dataverwerkingssystemen gehackt worden maakt echter dat het gebruik van een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk, zonder verdere bescherming tegen dit hacken, minder aantrekkelijk is. In dat geval kan er oneigenlijke data-uitwisseling plaatsvinden met het dataverwerkingssysteem en andere systemen die met het dataverwerkingssysteem zijn verbonden.

Immers kan een kwaadwillende zich toegang verschaffen tot alle met het communicatienetwerk verbonden locaties en inrichtingen, zodra hij zich toegang heeft weten te verschaffen tot één van de locaties, door middel van inbreken (“hacken”) op het bij die locatie behorende dataverwerkingssysteem. Door zich vervolgens voor te doen als reguliere gebruiker van het dataverwerkingssysteem of het communicatienetwerk waarop is ingebroken wordt hij op andere met het dataverwerkingssysteem verbonden communicatienetwerken beschouwd als een vertrouwde partij, en kan hij zich ook hiertoe relatief eenvoudig toegang verschaffen.

Met een dataverwerkingssysteem kunnen immers niet alleen data zoals audio-, video-, en besturingsinformatie worden uitgewisseld maar eveneens computervirussen, (spam)e-mail en gegevens van kwaadwillenden die op het communicatienetwerk proberen in te breken. Deze worden alle zonder onderscheid getransporteerd over eenzelfde communicatieverbinding. Bij de bekende beveiligingssystemen wordt de beveiliging tegen ongewenste data uitwisseling afgehandeld door, bijvoorbeeld een firewall of encryptie van gegevens. Wanneer dergelijke oplossingen op software gebaseerd zijn valt de beveiliging te omzeilen door het achterhalen van een wachtwoord, een encryptiesleutel of door gebruik te maken van fouten in de software.

Het is daarom een doel van de onderhavige uitvinding om een werkwijze en systeem voor het via een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk uitwisselen van data tussen een eerste dataverwerkingssysteem en een tweede dataverwerkingssysteem te verschaffen, dat de bovengenoemde nadelen althans gedeeltelijk opheft..

Het is een verder doel van de onderhavige uitvinding om een systeem te verschaffen voor het bewaken van een eerste locatie vanaf een tweede locatie waarbij de eerste en de tweede locatie een dataverwerkingssysteem omvatten dat is ingericht om te communiceren volgens een communicatieprotocol, gebruikmakend van de

5 bovengenoemde werkwijze.

De uitvinding verschaft daartoe een communicatiesysteem voor het, via een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk, uitwisselen van data tussen een eerste dataverwerkingssysteem, met ten minste één dataverwerkingssysteem,

10 bijvoorbeeld een computer of een beveiligingscamera, en een tweede communicatienetwerk met ten minste één dataverwerkingssysteem waarbij de beide dataverwerkingssystemen zijn ingericht om te communiceren volgens een communicatieprotocol, waarbij het eerste dataverwerkingssysteem via een eerste koppeling verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke

15 communicatienetwerk en het tweede dataverwerkingssysteem via een tweede koppeling verbonden met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk, waarbij de uitvinding daardoor gekenmerkt is dat ten minste één van de koppelingen een voor dataverkeer volgens het communicatieprotocol onoverbrugbare dataverbinding omvat.

20 Onder een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk volgens de onderhavige uitvinding dient ook een privaat communicatienetwerk of een private communicatieverbinding te worden verstaan welke om enigerlei reden publiek toegankelijk is of op enigerlei wijze gevoelig kan zijn voor hackers, zoals een IP

25 gebaseerd vast communicatienetwerk, zoals het internet, intranet, extranet, LAN, WAN, VPN, HFC, kabel of X-DSL, een IP gebaseerd draadloos communicatienetwerk, waaronder GPRS, W-LAN, WIMAX, EDGE, UMTS of een satellietnetwerk, een GSM, GSMdata, HSCSD, ISDN of PSTN netwerk.

30 Een dataverwerkingssysteem kan een computer omvatten, maar ook digitale beveiligingscamera's of andere systemen die zijn ingericht voor het opwekken van, via een internetprotocol of aanverwant protocol, transporteerbare gegevens, of die zijn ingericht voor het communiceren via een dergelijk protocol. Dergelijke systemen kunnen met een analoge of digitale interface verbonden zijn met het ten minste

gedeeltelijk voor het publiek toegankelijke communicatienetwerk, waarbij het communicatieprotocol een netwerkcommunicatieprotocol kan omvatten, en in het bijzonder een protocol kan omvatten uit de groep van het internetprotocol (IP), V.110, of X.75.

5

Door de via het gebruikte communicatieprotocol onoverbrugbare koppeling is het voor kwaadwillenden niet mogelijk om zich vanaf het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk, zoals een IP gebaseerd vast of draadloos communicatienetwerk, een ISDN, of een PSTN communicatienetwerk door middel van
10 het gebruikte communicatieprotocol toegang te verschaffen tot het dataverwerkingssysteem, dat verbonden is met de via het gebruikte communicatieprotocol onoverbrugbare koppeling.

Om communicatie via de voor het gebruikte communicatieprotocol onoverbrugbare
15 koppeling mogelijk te maken dienen de data volgens het gebruikte communicatieprotocol geconverteerd te worden naar een zodanig dataformaat dat de koppeling wel overbrugbaar is. De koppeling die de voor het gebruikte communicatieprotocol onoverbrugbaar is wordt daartoe in een uitvoeringsvorm van de onderhavige uitvinding voorzien van een protocolconvector, voor het convertoren van data volgens het
20 gebruikte communicatieprotocol naar data geschikt voor transport via, de voor het gebruikte communicatieprotocol, onoverbrugbare koppeling, die bijvoorbeeld een videoverbinding, een audioverbinding of een dataverbinding volgens het RS232 protocol kan omvatten. Deze verbindingen kunnen daarbij zowel analoog als digitaal uitgevoerd zijn.

25

In een verdere uitvoeringsvorm verschaft de onderhavige uitvinding een communicatiesysteem voor het bewaken van een eerste locatie, zoals een (bedrijfs)pand, vanaf een tweede locatie, met audiovisuele registratiemiddelen, zoals videocamera's of microfoons die zich bevinden op de eerste locatie. Deze
30 registratiemiddelen staan daarbij in verbinding met een eerste dataverwerkingssysteem dat zich bevindt op de eerste locatie, en wordt bedreven volgens een bepaald communicatieprotocol. Voorts omvat het systeem volgens de onderhavige uitvinding een waarnemingsstation, dat zich bevindt op de tweede locatie, voor het weergeven van

de meetgegevens aan een waarnemer, bijvoorbeeld via een waarschuwingssignaal zoals een licht of een geluid, of een indicatie op een monitor.

De meetgegevens kunnen zijn opgewekt door een videoregistratie- of weergave systeem, zoals een camera, een DVS (digitale video streamer), een DVR (digitale video recorder), of een CCTV systeem, door een audioregistratie- of weergave systeem, zoals een microfoon, of een luidspreker, door een dataregistratie- of weergave systeem, zoals een beweging- of contact sensor, een breukmelder, een schakelaar, een brandmelder, een kentekenteken- of een gezichtsherkenningsysteem, of een video-motion-detector.

10

Tussen het eerste en het tweede dataverwerkingssysteem is er een communicatieverbinding aanwezig, ten minste voor het uitwisselen van door de registratiemiddelen opgewekte registratiedata. In een uitvoeringsvorm van de onderhavige uitvinding wordt ook het alarmsignaal van de sensor via de communicatieverbinding uitgewisseld. De communicatieverbinding omvat ten minste een voor dataverkeer volgens het gebruikte communicatieprotocol onoverbrugbare koppeling .

15

Het systeem volgens de onderhavige uitvinding kan dankzij het gebruik van een volgens het gebruikte communicatieprotocol onoverbrugbare koppeling geen onbedoelde gegevens uitwisselen, zoals computervirussen, (spam)e-mail en gegevens van kwaadwillenden overbrengen vanuit het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk naar het eerste of het tweede dataverwerkingssysteem, of van het eerste dataverwerkingssysteem naar het tweede dataverwerkingssysteem of vice versa, anders dan gedefinieerd voor deze onoverbrugbare koppeling.

20

25

Het communicatiesysteem volgens de onderhavige uitvinding kan daartoe zodanig zijn ingericht dat het eerste dataverwerkingssysteem is gekoppeld met registratiemiddelen voor het verschaffen van registratiedata van een eerste locatie, bijvoorbeeld een videocamera of een microfoon, en het eerste dataverwerkingssysteem is ingericht voor het via het communicatienetwerk naar het tweede dataverwerkingssysteem volgens het internetprotocol verzenden van de registratiedata, terwijl het tweede dataverwerkingssysteem is ingericht voor het aan een waarnemer op een tweede locatie

30

- weergeven van de registratiedata. Hierbij kan zowel de eerste koppeling tussen het eerste dataverwerkingssysteem en het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk via bijvoorbeeld het internet protocol ontoegankelijk zijn, als de tweede koppeling tussen het tweede dataverwerkingssysteem en het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk via bijvoorbeeld het internetprotocol ontoegankelijk zijn, waarbij zowel het eerste als het tweede dataverwerkingssysteem één of meerdere dataverwerkingssystemen kan omvatten.
- 5
- 10 Het tweede dataverwerkingssysteem kan verder zijn ingericht voor het in ontvangst nemen van opdrachten van de waarnemer, en het in opdrachtdata volgens het internetprotocol omzetten van de ontvangen opdrachten. Het tweede dataverwerkingssysteem is daarbij dan ingericht voor het versturen van opdrachtdata volgens het internetprotocol naar het eerste dataverwerkingssysteem, dat is ingericht
- 15 voor het ontvangen van de opdrachtdata en het doorsturen van de opdrachtdata naar een met het eerste dataverwerkingssysteem gekoppelde inrichting die is ingericht voor het uitvoeren van de opdrachtdata, welke voorts een geluidsignaal, een gesproken bericht, een videosignaal, een voice-respons systeem, een DTMF systeem, een bedieningssignaal voor een inrichting, zoals verlichting, een PTZ camera, een
- 20 vergrendelingsinrichting of een productiemachine kan omvatten.

Op deze manier kan de inrichting worden ingezet voor het door een operator op het waarnemingsstation toespreken van een aanwezige persoon op de eerste locatie, of bijvoorbeeld het openen van een toegang tot een deel van de eerste locatie voor een

25 toeleverancier die een nachtlevering komt doen, het aan of uitschakelen van verlichting in een dergelijke situatie, of bij vermeend onraad, of bijvoorbeeld het bedienen van een machine wanneer al dan niet op afstand is bepaald dat bijsturing of in- of uitschakelen noodzakelijk is.

- 30 Naast het bewaken van objecten kan het communicatiesysteem volgens de onderhavige uitvinding worden gebruikt voor het bewaken van personen, bijvoorbeeld ouderen of patiënten die zorg behoeven. In een dergelijk geval wordt het waarnemingsstation bemand door verzorgers, of verschaft het waarnemingsstation toegang tot verzorgers. Naast personen of locaties is het verder mogelijk om gegevens die zich op een van de

dataverwerkingssystemen bevinden, zoals patientendossiers of soortgelijke
persoonsgevoelige informatie te beveiligen met behulp van de onderhavige uitvinding.

5 In alle toepassingen van de onderhavige uitvinding geldt dat in tegenstelling tot een
verbinding tussen meerdere dataverwerkingssystemen die gebaseerd is op het
communicatieprotocol, dat dataverkeer, over de via het communicatieprotocol niet
toegankelijke verbinding, door fysieke instellingen van de via het
communicatieprotocol onoverbrugbare koppeling mogelijk wordt gemaakt. Hierdoor is
het voor een kwaadwillende niet mogelijk vanaf het ten minste gedeeltelijk publieke
10 communicatienetwerk naar het eerste of tweede dataverwerkingssysteem door te
dringen noch om, vanuit of eenmaal doorgedrongen tot het eerste
dataverwerkingssysteem, door te dringen tot het tweede dataverwerkingssysteem, of
andersom: vanuit of eenmaal doorgedrongen tot het tweede dataverwerkingssysteem,
door te dringen tot het eerste dataverwerkingssysteem, omdat onbedoelde data-
15 uitwisseling via de koppeling niet mogelijk is. In het bijzonder is onbedoelde
datauitwisseling niet mogelijk door misbruik te maken, zoals misbruik van fouten in de
software, misbruik van softwarematige instellingen, zoals gebruikersinstellingen.

In een uitvoeringsvorm van de onderhavige uitvinding wekken registratiemiddelen op
20 de eerste locatie een breedbandig audiovisueel signaal op dat naar het
waarnemingsstation gevoerd dient te worden. Het waarnemingsstation is daarbij
ingericht om een operator in staat te stellen om verscheidene in de te bewaken ruimte
opgestelde camera's te selecteren om de door deze camera's opgewekte beelden te
kunnen volgen. Voorts zijn er bedieningsmiddelen aanwezig voor het bedienen van
25 beweegbare camera's, of voor het op afstand bedienen van licht- of andere inrichtingen,
zoals productiemachines. Daarnaast kan de operator vanaf de tweede locatie een
persoon die aanwezig is op de eerste locatie, zoals een chauffeur die een levering komt
brengen, vanaf afstand toespreken, door middel van een tweeweg-
communicatieverbinding. De registratiemiddelen zijn daarbij verbonden met een eerste
30 dataverwerkingssysteem dat wordt bedreven volgens het internetprotocol. Het eerste
dataverwerkingssysteem is via het internet verbonden met het tweede
dataverwerkingssysteem dat zich in het waarnemingsstation bevindt. Tussen het eerste
dataverwerkingssysteem en het tweede dataverwerkingssysteem, bevinden zich één of
meerdere protocolconvertors die de registratiegegevens volgens het internetprotocol,

omzet in een in een veilig formaat dat niet toestaat onbedoelde gegevens te bevatten.

Een voorbeeld van een geschikt gebleken signaal is daarbij een (analoog) videosignaal, een (analoog) audiosignaal, of een RS-232 interface met een zeer specifiek, vooraf gedefinieerd dataprotocol. De protocolconverteer wordt daarbij gevormd door een eerste
 5 deelinrichting die een videosignaal volgens het internetprotocol (een zogenaamd streaming videosignaal) omzet in een analoog videosignaal. Een daartoe geschikt gebleken inrichting is een videostreamer. Het aldus opgewekte videosignaal wordt toegevoerd aan een tweede deelinrichting die er weer een via het internetprotocol
 10 transporteerbaar signaal van maakt, dat via het gebruikte communicatienetwerk wordt toegevoerd aan het tweede dataverwerkingssysteem, op het waarnemingsstation. De tweede deelinrichting kan eveneens gevormd worden door een videostreamer-inrichting. In een uitvoeringsvorm van de onderhavige uitvinding omvat de tweede koppeling een tweede protocolconverteer, welke identiek kan zijn aan de eerste, voor het verder
 verhogen van het beveiligingsniveau.

15

In een verdere uitvoeringsvorm kan de operator vanuit de tweede locatie een verbinding met de eerste locatie maken voor het uitvoeren van een preventieve controle of voor het doen van een virtuele rondgang of om additionele diensten voor klanten te verrichten, zoals bijvoorbeeld het assisteren van op afstand gecontroleerde nachtleveringen of de
 20 controle en bediening van installaties en machines.

De uitvinding zal nu worden toegelicht aan de hand van de volgende figuren, waarin:

- Figuur 1 een eerste uitvoeringsvorm toont van een systeem voor het uitwisselen van data volgens de onderhavige uitvinding;
- 25 - Figuur 2 een tweede uitvoeringsvorm toont van een systeem voor het uitwisselen van data volgens de onderhavige uitvinding;
- Figuur 3 een derde uitvoeringsvorm toont van een systeem voor het uitwisselen van data volgens de onderhavige uitvinding;
- Figuur 4 een vierde uitvoeringsvorm toont van een systeem voor het uitwisselen
 30 van data volgens de onderhavige uitvinding;
- Figuur 5 een vijfde uitvoeringsvorm toont van een systeem voor het uitwisselen van data volgens de onderhavige uitvinding.

Figuur 1 toont een volgende uitvoeringsvorm van de onderhavige uitvinding waarbij er op de eerste locatie 105 een aantal sensoren uit de groep van alarmgevers, audio- en video-registratiemiddelen en weergave apparatuur is gekoppeld met een dataverwerkingssysteem, gevormd door het gesloten televisiesysteem (CCTV) 100. Het gesloten televisiesysteem 100 staat in datacommunicerende verbinding met een eerste protocolconvector 200. Via de verbinding kunnen videogegevens 115, audiogegevens 125 of besturingsgegevens 135 of combinaties daarvan aan de protocolconvector 200 worden toegevoerd, om door de protocolconvector 200 te worden omgezet in gegevens 405 volgens het internetprotocol of soortgelijk netwerkcommunicatieprotocol. Deze gegevens 405 worden door de protocolconvector 200 verzonden naar het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk 400. Via het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk 400 worden de gegevens 405 volgens het internetprotocol doorgevoerd naar een eerste waarnemingsstation 300, dat via een tweede protocolconvector 310 verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk 400. De tweede protocolconvector zet de gegevens 405 volgens het internetprotocol om in videogegevens 115', audiogegevens 125' en besturingsgegevens 135' welke doorgevoerd worden naar het eerste waarnemingsstation 300.

Figuur 2 toont een volgende uitvoeringsvorm van de onderhavige uitvinding waarbij er op eerste locatie 106 een aantal sensoren uit de groep van alarmgevers, audio- en video-registratiemiddelen en weergave apparatuur is gekoppeld met een dataverwerkingssysteem, gevormd door het gesloten televisiesysteem 100. Het gesloten televisiesysteem 100 staat in datacommunicerende verbinding met een eerste protocolconvector 206. Via de verbinding kunnen audiogegevens 126 of besturingsgegevens 136 of combinaties daarvan aan de protocolconvector 206 worden toegevoerd. Op de protocolconvector 200 is voorts videocamera 103 aangesloten welke videogegevens 116 aan de protocolconvector 206 verschaft. De protocolconvector 206 converteert de videogegevens 116, audiogegevens 126 en besturingsgegevens 136 in gegevens 406 volgens het internetprotocol. Deze gegevens 406 volgens het internetprotocol worden door de protocolconvector 206 verzonden naar het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk 400. Via het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk 400 worden de gegevens 406 volgens het internetprotocol doorgevoerd naar het eerste

waarnemingsstation 300, dat via een tweede protocolconvector 310 verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk 400. De tweede protocolconvector zet de gegevens 405 volgens het internetprotocol om in videogegevens 115', audiogegevens 125' en besturingsgegevens 135' welke
 5 doorgevoerd worden naar het eerste waarnemingsstation 300.

De in figuur 2 getoonde uitvoeringsvorm heeft het voordeel dat de protocolconvector 206 voorzien is van op zich bekende middelen voor het communiceren met de videocamera 103. De protocolconvector 206 kan daarbij bijvoorbeeld gevormd worden
 10 door een videostreamer, welke in staat is om de videocamera 103 via bijvoorbeeld Pan Tilt Zoom (PTZ) signalen te bedienen. Deze uitvoeringsvorm is dientengevolge bijzonder voordelig toepasbaar in situaties waar een bestaand gesloten televisiesysteem aanwezig is op een locatie, welk bestaand systeem niet verwijderd of vervangen mag worden. Redenen hiervoor kunnen reeds verleende goedkeuringen of
 15 beveiligingscertificaten zijn, of recente gepleegde investeringen voor een dergelijk gesloten televisiesysteem. De onderhavige uitvinding maakt het mogelijk op basis van een reeds bestaand systeem een beveiligingssysteem te verschaffen met een geringere kans dat een dataverwerkingssysteem gehackt wordt, waarbij er voorts, door direct bestaande camera 103 met protocol convector 206 te verbinden, een verbeterde
 20 beeldkwaliteit of beelddoorvoersnelheid bereikt kan worden.

Figuur 3 toont een derde uitvoeringsvorm van de onderhavige uitvinding, waarbij zowel de op de eerste locatie 105 uit figuur 1 als de op de eerste locatie 106 uit figuur 2 opgestelde gesloten televisiesystemen 100, 105, 106 via de respectievelijke
 25 protocolconvector 200 en 206 verbonden zijn met het ten minste gedeeltelijk voor het publiek toegankelijk toegankelijke communicatienetwerk 400. Een dergelijke uitvoeringsvorm kan in het bijzonder worden toegepast wanneer er vanaf één waarnemingsstation meerdere locaties bewaakt dienen te worden. Tussen de te bewaken locaties kan er op generlei wijze dataverkeer via het internetprotocol plaatsvinden, daar
 30 elk van de locaties via een, voor het internetprotocol, onoverbrugbare protocolconvector gekoppeld is met het ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk 400.

Figuur 4 toont een vierde uitvoeringsvorm van de onderhavige uitvinding, waarbij een tweede waarnemingsstation 320 via een derde protocolconvector 330 verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk 400, zodat de gegevens 405 volgens het internetprotocol worden doorgestuurd naar het

5 tweede waarnemingsstation 320 dat via een derde protocolconvector 330 verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk 400.

Daarbij kan gelijktijdig een verbinding met twee waarnemingsstations 300, 320 worden

10 gelegd. De tweede protocolconvector 310 zet de gegevens 405 volgens het internetprotocol om in videogegevens 115', audiogegevens 125' of besturingsgegevens 135' die naar het eerste waarnemingsstation 300 worden verzonden. De derde protocolconvector 330 zet de gegevens 405 volgens het internetprotocol om in videogegevens 115'', audiogegevens 125'' of besturingsgegevens 135'' die naar het

15 tweede waarnemingsstation 320 worden verzonden.

Een dergelijke uitvoeringsvorm biedt het voordeel dat er naast meerdere te beveiligen locaties ook meerdere waarnemingsstations aanwezig zijn, waarbij het mogelijk is om een bestaande communicatieverbinding door te schakelen van een eerste

20 waarnemingsstation naar een tweede waarnemingsstation. Een dergelijke uitvoeringsvorm kan bijvoorbeeld voorzien in een backupvoorziening voor het eerste waarnemingsstation. Ook kan deze gebruikt worden wanneer verschillende waarnemingsstations verschillende bevoegdheden hebben. Een eerste waarnemingsstation kan daarbij bevoegd zijn om bankovervallen waar te nemen en te

25 behandelen, terwijl een tweede waarnemingsstation bijvoorbeeld bevoegd kan zijn om gijzelingen te behandelen.

Figuur 5 toont weer een volgende uitvoeringsvorm van de onderhavige uitvinding. Deze uitvoeringsvorm omvat de uitvoeringsvorm uit figuur 4, welke gekoppeld is met een

30 soortgelijke uitvoeringsvorm 500. Een dergelijke koppeling biedt het voordeel dat bijvoorbeeld een videosignaal dat is opgewekt door het gesloten televisiesysteem 100 en ontvangen is door een eerste waarnemingsstation 300, kan worden doorgezonden naar een verder waarnemingsstation 520, verbonden via een protocolconverter 510 aan het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk 400, dat in

de tekening voor de overzichtelijkheid tweemaal is weergegeven. Het eerste waarnemingsstation 300 kan daarbij een waarnemingsstation van een particuliere beveiligingsinstantie zijn, terwijl het tweede waarnemingsstation 520 dat van een officiële instantie zoals de politie kan zijn. Op deze manier wordt in de functionaliteit van “extern doorschakelen” voorzien en wordt onbedoelde data-uitwisseling via deze onoverbrugbare koppelingen verder bemoeilijkt.

Naast de getoonde uitvoeringsvormen kent de onderhavige uitvinding nog vele variaties welke allen door de navolgende conclusies worden omvat.

Conclusies

1. Communicatiesysteem voor het via een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk uitwisselen van data tussen een eerste
 - 5 dataverwerkingssysteem en een tweede dataverwerkingssysteem, omvattende:
 - een eerste dataverwerkingssysteem, ingericht om te communiceren volgens een communicatieprotocol, waarbij het eerste dataverwerkingssysteem via een eerste koppeling verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk;
 - 10 - een tweede dataverwerkingssysteem, omvattende ten minste één dataverwerkingssysteem, ingericht om te communiceren volgens het communicatieprotocol, waarbij het tweede dataverwerkingssysteem via een tweede koppeling verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk;
 - 15 **met het kenmerk**
 - dat ten minste één van de koppelingen een voor dataverkeer volgens het communicatieprotocol onoverbrugbare verbinding omvat.
2. Communicatiesysteem volgens conclusie 1, **met het kenmerk** dat het ten minste
 - 20 gedeeltelijk voor het publiek toegankelijke communicatienetwerk een communicatienetwerk is uit de groep van:
 - een IP gebaseerd vast communicatienetwerk, zoals het internet, intranet, extranet, LAN, WAN, VPN, HFC, kabel of X-DSL;
 - een IP gebaseerd draadloos communicatienetwerk, waaronder GPRS, W-LAN,
 - 25 WIMAX, EDGE, UMTS of satelliet;
 - een GSM, GSMdata, HSCSD;
 - een ISDN;
 - een PSTN.
3. Communicatiesysteem volgens conclusie 2, **met het kenmerk dat** ten minste één
 - 30 van de koppelingen een protocolconvertoir omvat, voor het converteren van data volgens het gebruikte communicatieprotocol van het communicatienetwerk naar data geschikt voor transport via één uit de groep van:
 - een videoverbinding;

- een audioverbinding;
 - een dataverbinding volgens een RS232, RS485, RS422 of vergelijkbare interface.
- 5 4. Communicatiesysteem volgens conclusie 2, **met het kenmerk dat** ten minste één van de koppelingen een protocolconvector omvat, voor het converteren van data geschikt voor transport via één uit de groep van:
- een videoverbinding;
 - een audioverbinding;
- 10 - een dataverbinding volgens het RS232, RS485, RS422 of vergelijkbare interface;
- naar data volgens het gebruikte communicatieprotocol.
5. Communicatiesysteem volgens één van de voorgaande conclusies, **met het kenmerk**
- 15 dat de voor dataverkeer volgens het gebruikte communicatieprotocol onoverbrugbare koppeling tenminste een dataverbinding omvat uit de groep van:
- een analoge dataverbinding;
 - een digitale dataverbinding.
- 20 6. Communicatiesysteem volgens één van de voorgaande conclusies, **met het kenmerk dat**:
- het eerste dataverwerkingssysteem is gekoppeld met registratiemiddelen voor het verschaffen van registratiedata van een eerste locatie;
 - het eerste dataverwerkingssysteem is ingericht voor het, via het
- 25 communicatienetwerk, naar het tweede dataverwerkingssysteem volgens het gebruikte communicatieprotocol, verzenden van de registratiedata;
- het tweede dataverwerkingssysteem ten minste is ingericht voor het aan een waarnemer op een tweede locatie weergeven van de registratiedata;
- 30 7. Communicatiesysteem volgens conclusie 6, **met het kenmerk dat** de registratiemiddelen voor het verschaffen van registratiedata middelen omvatten uit de groep van:
- een videoregistratie- of weergave systeem, zoals een camera, een DVS (digitale video streamer), een DVR (digitale video recorder), of een CCTV systeem;

- een audioregistratie- of weergave systeem, zoals een microfoon, of een luidspreker;
- een dataregistratie- of weergave systeem, zoals een beweging- of contact sensor, een breukmelder, een schakelaar, een brandmelder, een kentekenteken- of een gezichtsherkenningssysteem, of een video-motion-detector.

5

8. Communicatiesysteem volgens conclusie 6 of 7, waarbij:

- het tweede dataverwerkingssysteem is ingericht voor het in ontvangst nemen van opdrachten van de waarnemer;
- 10 - het tweede dataverwerkingssysteem is ingericht voor het in data omzetten van ontvangen opdrachten naar dataformaten die geschikt zijn volgens het gebruikte communicatieprotocol,
- het tweede dataverwerkingssysteem is ingericht voor het versturen van opdrachtdata volgens het gebruikte communicatieprotocol, naar het eerste dataverwerkingssysteem;
- 15 - het eerste dataverwerkingssysteem is ingericht voor het ontvangen van de opdrachtdata;
- het eerste dataverwerkingssysteem is ingericht voor het doorsturen van de opdrachtdata naar een met het eerste dataverwerkingssysteem gekoppelde inrichting die is ingericht voor het uitvoeren van de opdrachtdata.
- 20

9. Communicatiesysteem volgens conclusie 8, waarbij de opdrachtdata gekozen zijn uit de groep van:

- een geluidsignaal;
- 25 - een gesproken bericht;
- een videosignaal;
- een voice-respons systeem
- een DTMF systeem
- een bedieningssignaal voor een inrichting, zoals verlichting, een PTZ camera,
- 30 een vergrendelingsinrichting of een productiemachine.

10. Werkwijze voor het via een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk uitwisselen van data tussen een eerste dataverwerkingssysteem en een tweede dataverwerkingssysteem, omvattende:

- 5 - het inrichten van een eerste dataverwerkingssysteem voor het communiceren volgens een communicatieprotocol;
- het koppelen van het eerste dataverwerkingssysteem met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk;
- het inrichten van een tweede dataverwerkingssysteem voor het communiceren volgens het communicatieprotocol;
- 10 - het koppelen van het tweede dataverwerkingssysteem met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk;

gekenmerkt door:

- het voor dataverkeer volgens het communicatieprotocol, met een onoverbrugbare koppeling verbinden van ten minste het eerste of het tweede
- 15 dataverwerkingssysteem met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk.

11. Werkwijze volgens conclusie 10, **gekenmerkt door:**

- 20 - het ter hoogte van een koppeling van het eerste of het tweede dataverwerkingssysteem met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk converteren van data volgens het communicatieprotocol, naar data geschikt voor transport via één uit de groep van:
- 25 - een videoverbinding;
- een audioverbinding;
- een dataverbinding volgens de RS232, RS485, RS422 of vergelijkbare interface.

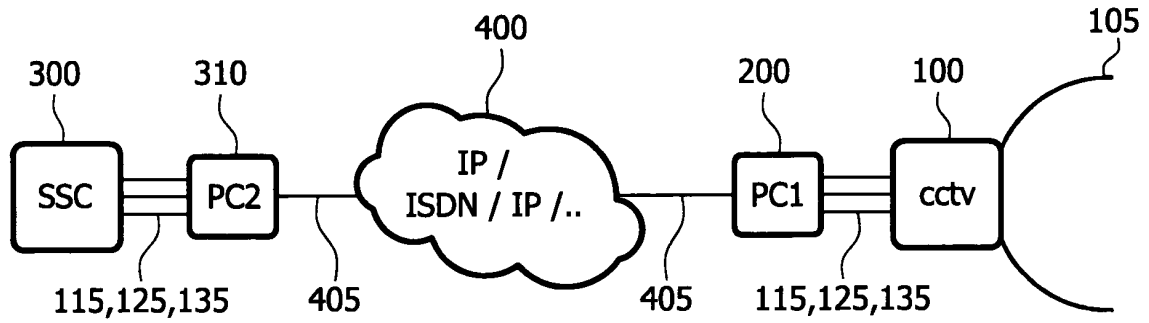


FIG. 1

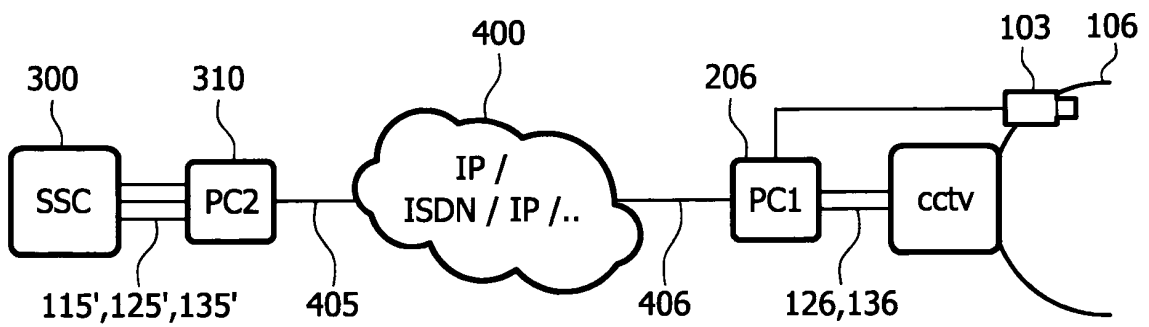


FIG. 2

2/3

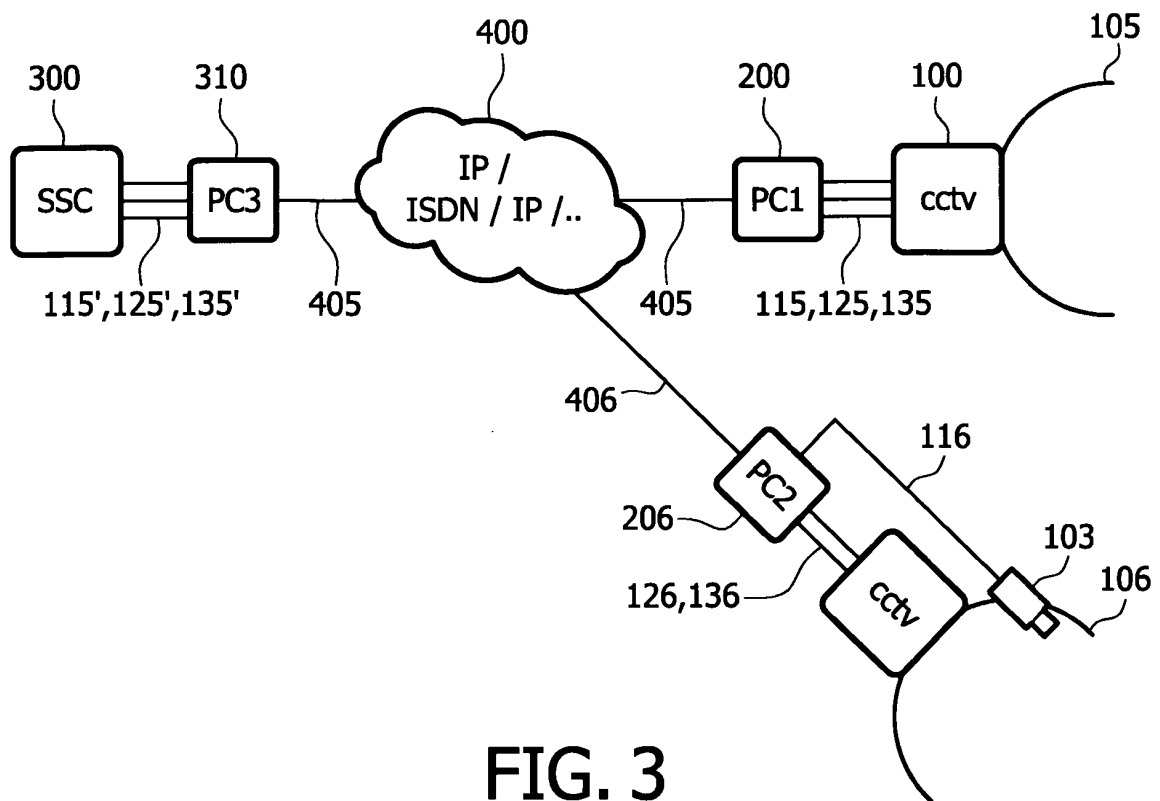


FIG. 3

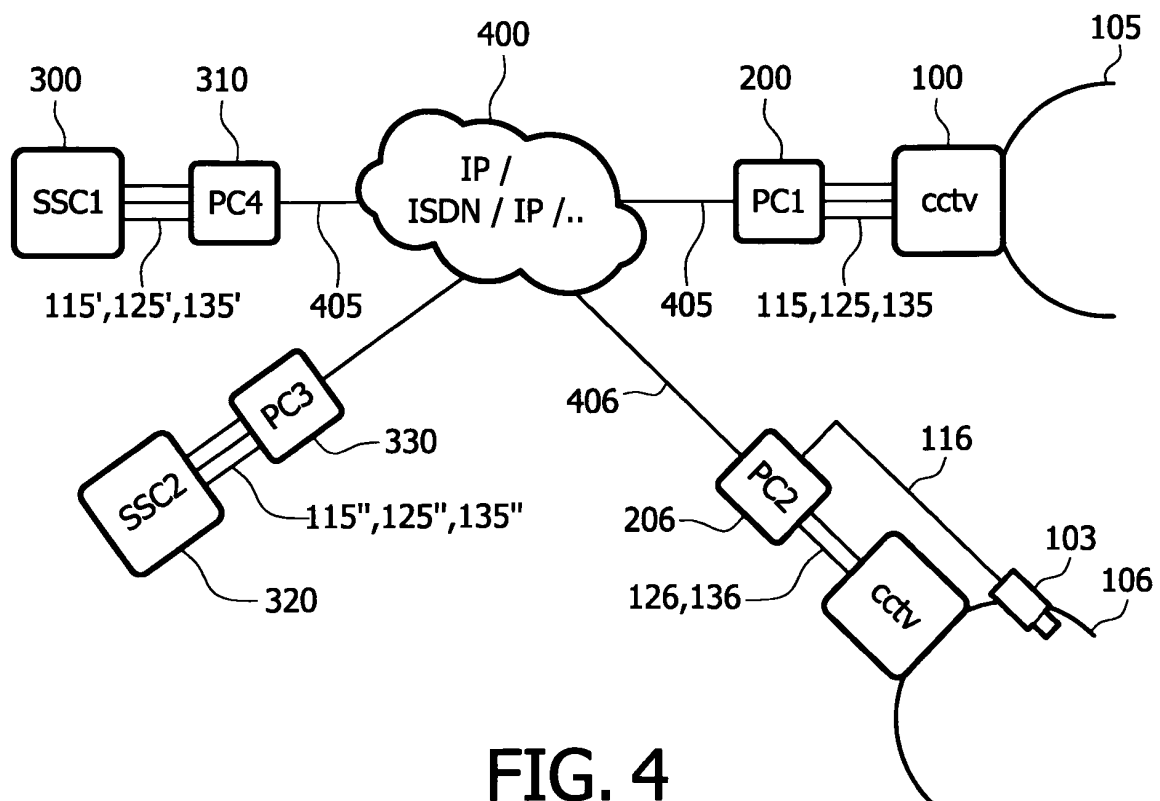


FIG. 4

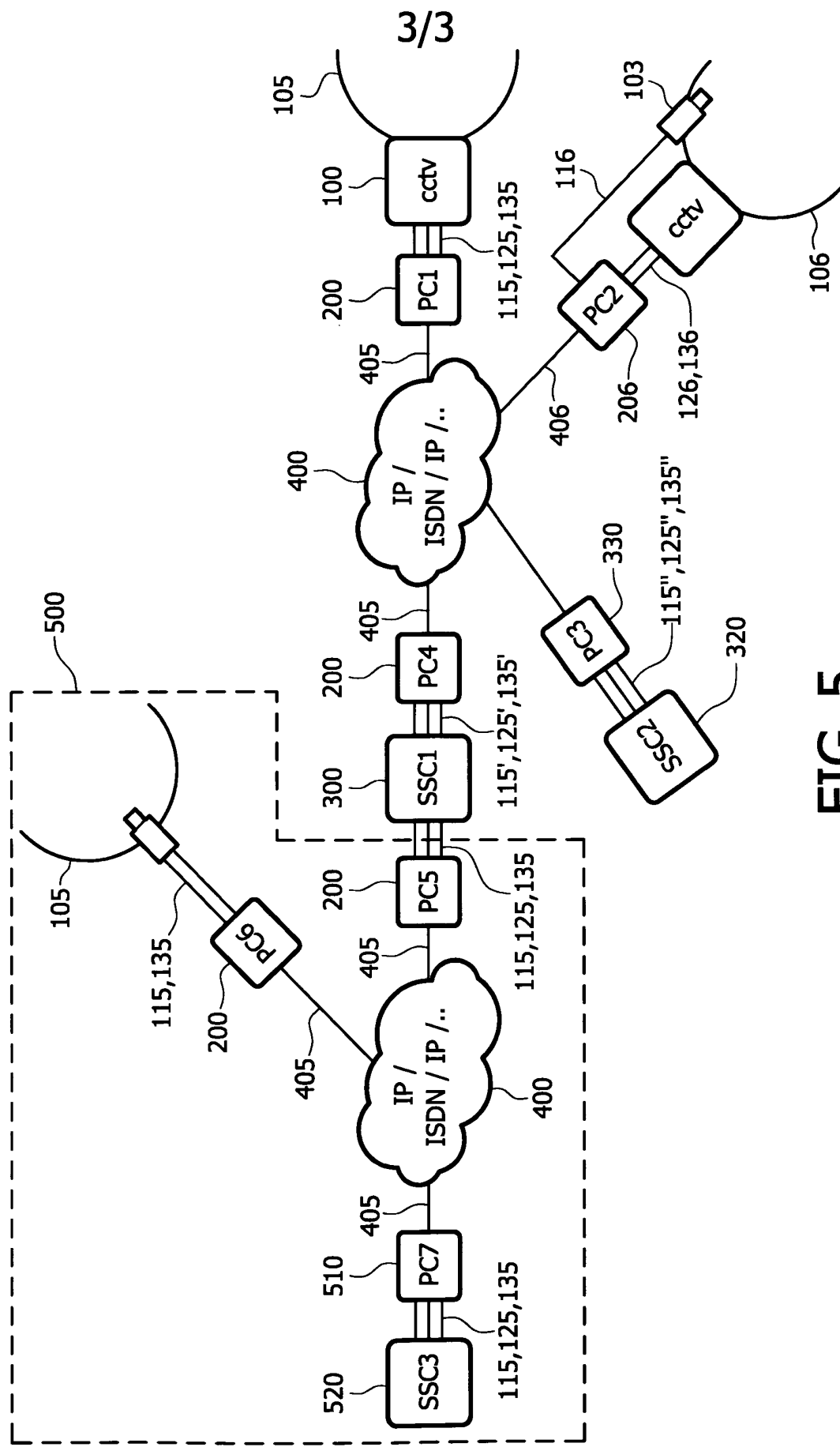


FIG. 5

SAMENWERKINGSVERDRAG (PCT)

RAPPORT BETREFFENDE NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

IDENTIFICATIE VAN DE NATIONALE AANVRAGE		KENMERK VAN DE AANVRAGER OF VAN DE GEMACHTIGDE	
		1.491.001 NL	
Nederlands aanvraag nr. 2000632		Indieningsdatum 07-05-2007	
		Ingeroepen voorrangsdatum	
Aanvrager (Naam) Spectator Intellectual Properties B.V.i.o.			
Datum van het verzoek voor een onderzoek van internationaal type 26-07-2007		Door de Instantie voor Internationaal Onderzoek aan het verzoek voor een onderzoek van internationaal type toegekend nr. SN 48879	
I. CLASSIFICATIE VAN HET ONDERWERP (bij toepassing van verschillende classificaties, alle classificatiesymbolen opgeven)			
Volgens de internationale classificatie (IPC) H04L29/06 H04N7/18 G08B25/00			
II. ONDERZOChte GEBIEDEN VAN DE TECHNIEK			
Onderzochte minimumdocumentatie			
Classificatiesysteem		Classificatiesymbolen	
IPC8	H04L H04N G08B		
Onderzochte andere documentatie dan de minimum documentatie, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen			
III.	☐	GEEN ONDERZOEK MOGELIJK VOOR BEPAALDE CONCLUSIES (opmerkingen op aanvullingsblad)	
IV.	☐	GEBREK AAN EENHEID VAN UITVINDING (opmerkingen op aanvullingsblad)	

**ONDERZOEKSRAPPORT BETREFFENDE HET
RESULTAAT VAN HET ONDERZOEK NAAR DE STAND
VAN DE TECHNIEK VAN HET INTERNATIONALE TYPE**

Nummer van het verzoek om een onderzoek naar
de stand van de techniek
NL 2000632

A. CLASSIFICATIE VAN HET ONDERWERP
INV. H04L29/06 H04N7/18 G08B25/00

Volgens de Internationale Classificatie van octroolen (IPC) of zowel volgens de nationale classificatie als volgens de IPC.

B. ONDERZOCHE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie (classificatie gevolgd door classificatiesymbolen)
H04L H04N G08B

Onderzochte andere documentatie dan de minimum documentatie, voor dergelijke documenten, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

Tijdens het onderzoek geraadpleegde elektronische gegevensbestanden (naam van de gegevensbestanden en, waar uitvoerbaar, gebruikte trefwoorden)

EPO-Internal, WPI Data, INSPEC, COMPENDEX

C. VAN BELANG GEACHTE DOCUMENTEN

Categorie °	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
X	TECTON LIMITED: "High Performance IP solutions - Network Toolkit"[Online] 10 mei 2006 (2006-05-10), bladzijden 1-2, XP002466655 Gevonden op het Internet: URL: http://tecton-cctv.com/pdfs/Network%20Toolkit%20CCTV.pdf [gevonden op 2008-01-28] het gehele document	1-11
X	US 2006/139162 A1 (FLYNN DANIEL J [US]) 29 juni 2006 (2006-06-29) alineas [0024] - [0027]; figuren 1,2	1-11
A	GB 2 416 897 A (VISIBLE VIGILANCE LTD [GB]) 8 februari 2006 (2006-02-08) het gehele document	1-11
	----- -/--	

☒ Verdere documenten worden vermeld in het vervolg van vak C. ☒ Leden van dezelfde octroofamilie zijn vermeld in een bijlage

° Speciale categorieën van aangehaalde documenten

A niet tot de categorie X of Y behorende literatuur die de stand van de techniek beschrijft

D in de octrooiaanvraag vermeld

E eerdere octrooi(aanvraag), gepubliceerd op of na de indieningsdatum, waarin dezelfde uitvinding wordt beschreven

L om andere redenen vermelde literatuur

O niet-schriftelijke stand van de techniek

P tussen de voorrangsdatum en de indieningsdatum gepubliceerde literatuur

T na de indieningsdatum of de voorrangsdatum gepubliceerde literatuur die niet bezwarend is voor de octrooiaanvraag, maar wordt vermeld ter verheldering van de theorie of het principe dat ten grondslag ligt aan de uitvinding

X de conclusie wordt als niet nieuw of niet inventief beschouwd ten opzichte van deze literatuur

Y de conclusie wordt als niet inventief beschouwd ten opzichte van de combinatie van deze literatuur met andere geciteerde literatuur van dezelfde categorie, waarbij de combinatie voor de vakman voor de hand liggend wordt geacht

Z lid van dezelfde octroofamilie of overeenkomstige octroolpublicatie

Datum waarop het onderzoek naar de stand van de techniek van internationaal type werd voltooid

29 Januari 2008

Verzenddatum van het rapport van het onderzoek naar de stand van de techniek van internationaal type

Naam en adres van de instantie

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

De bevoegde ambtenaar

Mannekens, Jan

**ONDERZOEKSRAPPORT BETREFFENDE HET
RESULTAAT VAN HET ONDERZOEK NAAR DE STAND
VAN DE TECHNIEK VAN HET INTERNATIONALE TYPE**

Nummer van het verzoek om een onderzoek naar
de stand van de techniek

NL 2000632

C.(Vervolg). VAN BELANG GEACHTE DOCUMENTEN

Categorie *	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
A	US 2006/031934 A1 (KRIEGEL KEVIN [US]) 9 februari 2006 (2006-02-09) het gehele document -----	1-11
A	WO 98/51080 A (ACOSTA EDWARD [US]; KAO FRANK [US]) 12 november 1998 (1998-11-12) het gehele document -----	1-11
A	US 2003/061325 A1 (MONROE DAVID A [US]) 27 maart 2003 (2003-03-27) het gehele document -----	1-11

**ONDERZOEKSRAPPORT BETREFFENDE HET
RESULTAAT VAN HET ONDERZOEK NAAR DE STAND
VAN DE TECHNIEK VAN HET INTERNATIONALE TYPE**

Informatie over leden van dezelfde octrooifamilie

Nummer van het verzoek om een onderzoek naar
de stand van de techniek

NL 2000632

In het rapport genoemd octrooigeschrift	Datum van publicatie	Overeenkomend(e) geschrift(en)	Datum van publicatie
US 2006139162	A1	29-06-2006	GEEN
GB 2416897	A	08-02-2006	GEEN
US 2006031934	A1	09-02-2006	EP 1784732 A2 16-05-2007 WO 2006017678 A2 16-02-2006
WO 9851080	A	12-11-1998	AU 7293098 A 27-11-1998 EP 1010327 A1 21-06-2000 JP 2002507336 T 05-03-2002 US 6166729 A 26-12-2000
US 2003061325	A1	27-03-2003	GEEN



OCTROOICENTRUM NEDERLAND

WRITTEN OPINION

File No. SN48879	Filing date (day/month/year) 07.05.2007	Priority date (day/month/year)	Application No. NL2000632
International Patent Classification (IPC) INV. H04L29/06 H04N7/18 G08B25/00			
Applicant Spectator Intellectual Properties B.V. i.o. te Gee			

This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the application
- ☐ Box No. VIII Certain observations on the application

	Examiner Mannekens, Jan
--	----------------------------

WRITTEN OPINION

Application number

NL2000632

Box No. I Basis of this opinion

1. This opinion has been established on the basis of the latest set of claims filed before the start of the search.
2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the application and necessary to the claimed invention, this opinion has been established on the basis of:
 - a. type of material:
 - ☐ a sequence listing
 - ☐ table(s) related to the sequence listing
 - b. format of material:
 - ☐ on paper
 - ☐ in electronic form
 - c. time of filing/furnishing:
 - ☐ contained in the application as filed.
 - ☐ filed together with the application in electronic form.
 - ☐ furnished subsequently for the purposes of search.
3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
4. Additional comments:

Box No. V Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty	Yes: Claims	
	No: Claims	1-11
Inventive step	Yes: Claims	
	No: Claims	1-11
Industrial applicability	Yes: Claims	1-11
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item V

**Reasoned statement with regard to novelty, inventive step or industrial applicability;
citations and explanations supporting such statement**

- 1 The following documents have been cited in the search report; the numbering will be adhered to in the rest of the procedure:
 - D1: TECTON LIMITED: "High Performance IP solutions - Network Toolkit"[Online] 10 mei 2006 (2006-05-10), bladzijden 1-2, XP002466655
Gevonden op het Internet: URL:<http://tecton-cctv.com/pdfs/Network%20Toolkit%20CCTV.pdf>> [gevonden op 2008-01-28]
 - D2: US 2006/139162 A1 (FLYNN DANIEL J [US]) 29 juni 2006 (2006-06-29)
 - D3: GB-A-2 416 897 (VISIBLE VIGILANCE LTD [GB]) 8 februari 2006 (2006-02-08)
 - D4: US 2006/031934 A1 (KRIEGEL KEVIN [US]) 9 februari 2006 (2006-02-09)
 - D5: WO 98/51080 A (ACOSTA EDWARD [US]; KAO FRANK [US]) 12 november 1998 (1998-11-12)
 - D6: US 2003/061325 A1 (MONROE DAVID A [US]) 27 maart 2003 (2003-03-27)
- 2 The present application does not meet the criteria of patentability, because the subject-matter of independent claims 1 and 10 is not new.
- 2.1 Claim 1: The document D1 discloses (the references in parentheses applying to this document):

A system used for a security installation (D1, page 2, Technical Notes) allowing "uitwisselen van data tussen een eerste dataverwerkingssysteem en een tweede dataverwerkingssysteem" (D1, page 2, Technical Notes, "For example alarms for a building can be transmitted over a secure network to a monitoring centre") over "een ten minste gedeeltelijk voor het publiek toegankelijk communicatienetwerk" (D1, page 1, Figure - Internet; page 2, Technical Notes, "Alarm inputs and outputs can be sent over the network of internet") comprising:
"een eerste dataverwerkingssysteem, ingericht om te communiceren volgens een communicatieprotocol, waarbij het eerste dataverwerkingsprotocol via een eerste koppeling verbonden is met het ten minste gedeeltelijk voor het publiek toegankelijke communicatienetwerk" (D1, page 1, Figure - Keyboard RS485 over

Internet via Network Toolkit);

"een tweede dataverwerkingssysteem, ingericht om te communiceren volgens het communicatieprotocol, waarbij het tweede dataverwerkingssysteem via een tweede koppeling verbonden is met het communicatienetwerk" (D1, page 1,

Figure - RS485 controlled camera over Internet via second Network Toolkit);

"met het kenmerk dat ten minste één van de koppelingen een voor dataverkeer volgens het communicatieprotocol onoverbrugbare verbinding bevat" (D1, page 1, Figure 1, RS485 over IP Network via Network Toolkit).

Note: Alternatively to document D1, document D2 can be used in the reasoning.
 The relevant passages in D2 are paragraphs 24-27 and Figures 1-2

2.2 Claim 10: The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent claim 10 which therefore is also considered not new.

3 Dependent claims 2-9, 11 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of novelty and/or inventive step, see documents D1-D6 and the corresponding passages cited in the search report.