(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 January 2009 (15.01.2009)

PCT

(10) International Publication Number
WO 2009/006670 A1

(51) International Patent Classification:
H04L 12/66 (2006.01) *G08B 29/16* (2006.01)

(21) International Application Number:
PCT/AU2008/000644

(22) International Filing Date: 11 May 2008 (11.05.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2007903654 6 July 2007 (06.07.2007) AU

(71) Applicant: **PARPHIPS PTY LTD** [AU/AU]; Level 1, 432 Parramatta Road, Petersham, New South Wales 2049 (AU).

(71) Applicant and
(72) Inventor: **PARDY, Nicholas Keith** [AU/AU]; PO Box 6, Cootamundra, New South Wales 2590 (AU).

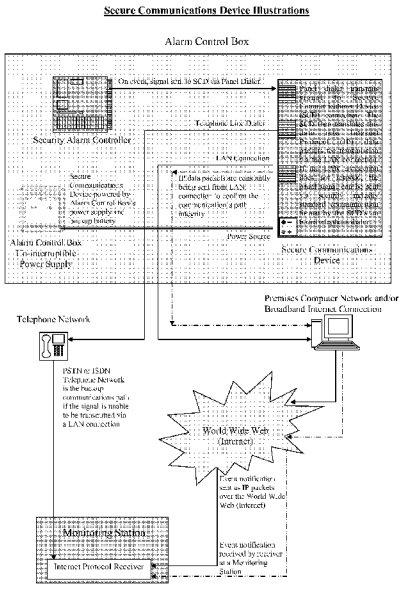
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to the identity of the inventor (Rule 4.17(i))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*
— *of inventorship (Rule 4.17(iv))*

Published:
— *with international search report*

(54) **Title:** SECURE COMMUNICATIONS DEVICE



(57) **Abstract:** The invention relates to a compact single device designed to be installed in conjunction with any existing industry standard security alarm system. The compact single device is designed to use the power supply of the existing standard security alarm system and controls communication to a security alarm system monitoring server via existing communications infrastructure consisting of Internet Protocol (IP) data packets as a primary communications path and by Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN) phone calls as a backup communications path.

WO 2009/006670 A1

SECURE COMMUNICATIONS DEVICE

The issue with traditional, common marketplace security alarm systems is that they rely on communications using the standard Public Switched Telephone Network (PSTN) which is flawed, in that it suffers a range of vulnerabilities. The alarm dialler that exists on the alarm panel's circuit board is the hardware responsible for sending a telephone communication, through a standard telephone call, to the monitoring station, server or alarm receiver (to be referred to henceforth as "monitoring server") to notify that an event has been triggered. In addition to this, the alarm dialler is capable (with the alarm being adequately programmed) of sending the monitoring server a test signal periodically that checks and verifies the communications path's integrity. This test signal confirms that the communications path from the alarm panel to the monitoring server is currently valid (but only *up until* the time of the test signal being sent and received). This creates alarm system vulnerability, where if the telephone line is severed on a system that uses a standard alarm dialler, the monitoring server is not notified of the severed line until the next expected signal is *not* received from the security alarm system. In addition, due to the cost of a phone call for each and every signal sent from the alarm dialler to the monitoring server (whether it be an alarm event or a test signal), many sites or premises decide to reduce the occurrence of test signals being sent in order to reduce on-going costs of their alarm system. By reducing the quantity of test signals being sent, and therefore increasing the intervals between each signal sent, the system's accuracy is compromised as more time passes before the monitoring server is aware of a fault. Therefore, if a system is set up to send test signals once a week, and the phone line is severed the day after the previous test signal was sent to the monitoring server, the monitoring server will not be notified of the severed communications path until the next test signal (due the following week) is *not* received. This creates a breach in security, as if an alarm is triggered sometime between the phone line being severed and the monitoring server receiving the following week's test signal, the monitoring server is not aware of the event, and hence no immediate action (eg. police attendance or security patrol) is taken.

Although there have been attempts to circumvent this issue of increasing an alarm system's communication integrity, none have been highly successful both in ability and cost effectiveness. Premises with high security risks in metropolitan areas have for many years used the Securitel Network, a system operated with the cooperation of telephone service providers and private security providers. Limited to use within restricted distances from a limited number of exchanges, the technology has always been expensive to operate with limited ability. Although Securitel monitors the integrity of the communications path by polling the PSTN phone line approximately twice a minute, it is limited to only transmitting a restricted amount of security system communication signals. Also, even though a security system monitoring server is notified (through the disappearance of the expected polling) of a severed communications path, the Securitel system is limited in the respect that once the communications path is severed, no further signals can be transmitted to the monitoring server until the communications path is restored. Again, this creates an alarm system vulnerability as a communications path may be severed, and an event triggered (eg. an alarm is activated), and the monitoring server is unaware. In addition, the ongoing cost of security system monitoring must be relatively low to be viable for the common marketplace, and although the cost of phone calls using the Securitel system is nil, the monitoring fee payable for the service provision is considered to be costly and therefore is not accessible by the general market.

SECURE COMMUNICATIONS DEVICE

Advancements in recent mobile phone communication technologies such as GSM (Global System for Mobile Communications) and GPRS (General Packet Radio Service) have brought forth new communication systems to the security industry and market. GSM offers the ability to transmit security system signals via the mobile phone network in the event of a PSTN phone line failure. Due to the expense of mobile phone calls, this system is usually only used as a backup device to the PSTN system. The GSM system is also inadequate in that it lacks the ability to constantly monitor the communications path for integrity, other than identifying if the PSTN phone line has dropped below the normal operating voltage. The GSM dialler is flawed for higher risk security system sites, in that there is no regular polling to confirm the integrity of the communications path. The offering of GPRS mobile phone technology has greatly increased the ability to both monitor the integrity of security system communications paths and to transmit signals to a monitoring server in the event of PSTN phone line failure by using constantly polled data packet communications over the wireless GPRS network. GPRS mobile phone security system communications rely on computer data packets being transmitted several times an hour to a network receiver, however, as with many wireless networks, data packet signals are often missed or lost, causing further security vulnerabilities. The ongoing expense associated with using the GPRS system is considered to be excessive by the general market, as constant wireless data transmissions incur high expense for connection and the actual data transmission itself. Overall, both GSM and GPRS as mobile phone technologies are plagued with issues concerning network coverage, signal quality and expense, making them more of a backup to the PSTN system, as opposed to being the alarm system's primary communications source.

The ability to use data packets over the Internet to send security system communications and constantly monitor communications path integrity is not a new idea, and with constant Broadband Internet now available to most premises, the use of such technology to increase security and reduce ongoing expense has never been greater. Although the security industry has been offered different devices in recent years for allowing communications via the Internet, none have been designed to work within the existing market place. All offerings to date have been designed to work primarily with only the manufacturer's latest security alarm panel or monitoring server, or to function as a complicated device that will not fit within the massive electronic security marketplace. The security system market consists of several different designs of security alarm systems that vary in technology design by nearly two decades, which has created an industry consisting of many older security systems that consumers will not update for many years, and in some cases decades, from now. Therefore, there is a large market sector of existing alarm installations that are unable to take advantage of the newer technologies that are proprietary and only available for new installations.

Many available systems are also not generally available to all security monitoring station's control room facilities. Systems such as the Fratech FE3000, Fratech Multi-Path and the Honeywell 7845i Internet Communicator are designed to work primarily with their own proprietary systems, and do not offer a solution to the general marketplace as they cannot be adapted or installed to all existing systems. An example of a system getting close to industry requirements is the ABN (Alarm Broadband Network) by NextAlarm.com in the United States of America. This system however is limited again to only working with NextAlarm.com's server

SECURE COMMUNICATIONS DEVICE

system and is limited in function and reliability, as it requires to be powered externally from the security system's power sources, using its own mains power supply. This means that the system's reliability can be compromised as it can be easily disabled by severing power to a premise, a blackout, or simply being unplugged. If this power interruption happens before the security system has time to send an alarm signal, the monitoring server is not notified. Therefore, in the event of a power outage, the system cannot communicate alarm events to a monitoring server at all. In addition, an Internet connection failure results in a communication termination as the device does not make use of any backup communication technologies, such as PSTN. Also, limitations with this system exist in its inability to allow reverse communications (communications from the monitoring server to the alarm panel), a function greatly used by alarm monitoring servers to remotely access security alarm systems for programming changes and to arm systems as required.

The invention development referred to here as the Secure Communications Device has been created to overcome the shortcomings of existing security alarm system communication devices claiming to transmit security alarm signals via the Internet. The invention is uniquely designed to function as an integrated hardware device with existing common marketplace security alarm systems, and is designed to be installed directly within the secure housing equipment enclosures of an existing security alarm system. The invention is designed to function using existing communications infrastructure and the power supply of the security alarm system, therefore utilising the security alarm system's incorporated battery backup supply. Overall, this means that the Secure Communications Device is backward compatible with existing alarm systems, is not proprietary and uses the existing communications networks and power backup.

By design, the Secure Communications Device is able to establish a virtual PSTN connection from the Secure Communications Device to a standard PSTN alarm dialler of any alarm system. When the alarm dialler requires communication with the monitoring server, it sends the signal to the Secure Communications Device along the virtual PSTN created by the Secure Communications Device. The Secure Communications Device then receives the alarm transmission from the alarm dialler and translates the signal into standard, encrypted Internet Protocol (IP) data packets and transmits these data packets via an Internet connection to a monitoring server. This allows communications to be sent from the alarm dialler to the monitoring server without requiring connection to the telephone network for normal condition alarm transmission purposes, and therefore not incurring call costs to notify of an event. Unlike Australian Patent Number 772360, this communications method does not use electronic mail, but rather encrypted packets of data, consisting of the raw alarm panel's industry-standard signals.

The Secure Communications Device's onboard processor is able to receive any industry standard alarm system's signal, acting as an alarm receiver, in any industry standard alarm system communication format (eg. Contact ID, 4+2, etc.) from the alarm system dialler, and then transmits this to the monitoring server. The primary communication method of transmitting data packets from the Secure Communications Device to the monitoring server is IP data packets, sent via the Internet. However, if the Internet connection is inoperative, the Secure Communications Device is able to communicate the alarm's event by transmitting via a telephone call using PSTN,

SECURE COMMUNICATIONS DEVICE

ISDN (Integrated Services Digital Network) or any backup communications technology associated to these. The Secure Communications Devices integrated ability to transmit the alarm system's data by either IP data packets, PSTN or ISDN is a critical design feature, as it allows the Secure Communications Device to transmit data by PSTN or ISDN in the event of an IP network failure, hence increasing its capability. Also, by the primary communications path being IP data packets, the Secure Communications Device does not use a phone call to transmit the alarm dialler's communication event unless the Internet connection is inoperative.

The Secure Communications Device incorporates by design the ability to listen to any answered incoming call that transmits through it on the supplied backup PSTN or ISDN phone line. The Secure Communications Device is listening for a specialised tone generated by a security alarm monitoring server, using remote access software, that is communicating to the Secure Communications Device. Once the Secure Communications Device has sensed the specialised tone, the Secure Communications Device is able to answer the call, hence allowing the monitoring server access to the Secure Communications Device for the purposes of modifying programming, for example.

The Secure Communications Device is designed to incorporate a polling feature via the IP network, constantly polling a control room monitoring server to confirm communications integrity. This feature allows the Secure Communications Device to replace existing Securitel technologies for communications path integrity monitoring. In the event of an IP network failure (determined by successive polling failures) the Secure Communications Device is able to transfer communications to the backup PSTN or ISDN phone system. This connection to the security alarm monitoring server via PSTN or ISDN signal will communicate that the network failure has occurred and that transmission via PSTN or ISDN is working successfully. This ensures that in the event of an Internet communication breakdown, the monitoring server is advised, whilst events are still able to be transmitted to the monitoring server through the backup PSTN or ISDN phone system.

The Secure Communications Device also incorporates in its design onboard storage identification known in the security industry as an Account Number or Client ID. This design feature enables the Secure Communications Device to be installed with any existing alarm design, without the requirement to reprogram the existing alarm system's onboard identification or account number. The Secure Communications Device is designed to ignore any account information transmitted by the alarm system dialler to the Secure Communications Device, and only transfers the alarm signal data to the monitoring server.

The invention may be better understood with reference to the specification illustrations.

SECURE COMMUNICATIONS DEVICE

The Claims defining the invention are as follows:

1. A compact single device invention designed to be installed in conjunction with any existing industry standard security alarm system, using the integrated power supply of the security alarm system, to control communications to a security alarm system monitoring server via the existing communications infrastructure, consisting of Internet Protocol (IP) data packets as a primary communications path and by Public Switched Telephone Network (PSTN) or ISDN (Integrated Services Digital Network) phone calls as a backup communications path.

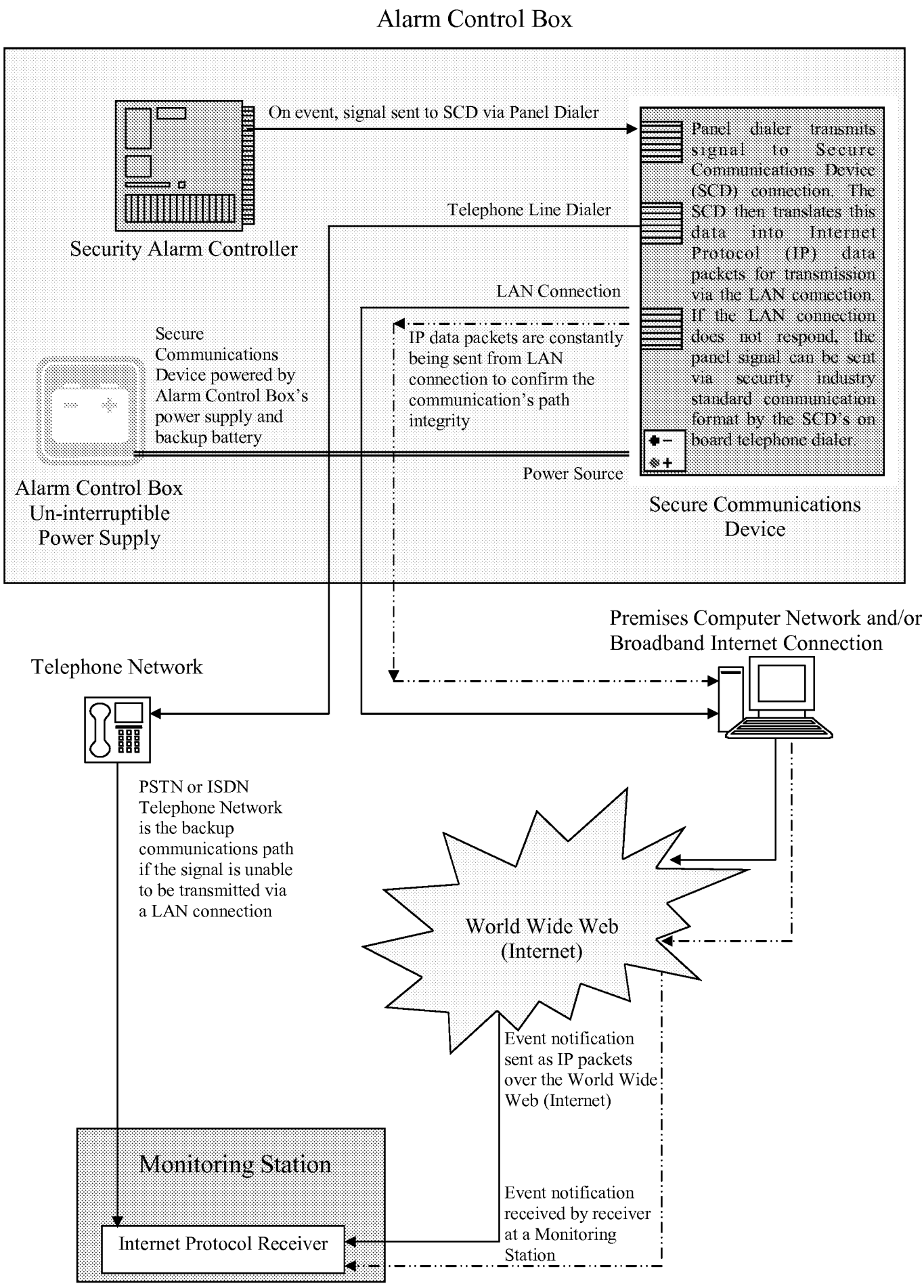
2. The compact single device invention of claim one designed to be small in size so as to be allowed to be installed inside existing security alarm system enclosures, powered by the said security alarm system's battery backup power supply, causing no loss of communications ability in the event of a mains power outage.

3. The compact single device invention of claim one, designed to manage communications from existing standard designed security alarm systems, ensuring by polled data packet on common computer IP network technology, a constantly verified communications path to a security alarm monitoring server.

4. The compact single device invention of claim one, able to receive communications from any existing security alarm system by method of closed telephone communications. The device creates a virtual PSTN phone line and dial tone to the security alarm system's onboard telephone dialler. The device intercepts any calls made by the said security alarm system, receives the call and all associated data from the security alarm system's onboard dialler, in any recognised format (eg. Contact ID, 4+2, etc). The device then acts the same as a security alarm monitoring receiver and acknowledges receipt of the call to the security alarm system's onboard dialler.

5. The compact single device invention of claim one, designed to store locally within its processor information pertaining to security alarm system identity via form of account number, without the requirement to process account data as stored in the connecting alarm system.

Secure Communications Device Illustrations



INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/000644

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 12/66 (2006.01) ***G08B 29/16*** (2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DWPI: security, alarm, Internet, PSTN, ISDN, phone, network and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2004/0186739 A1 (BOLLES et al.), 23 September 2004. Abstract, pages 1 – 3.	1, 2, 4, 5 3
X Y	AU 2004100187 A4 (CASUSCELLI et al.), 22 April 2004. Whole document.	1, 2, 4, 5 3
Y	US 2006/0067484 A1 (Elliot et al.), 30 March 2006. Abstract.	3

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 August 2008	28 AUG 2008
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **ANISH SINGH** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 2 6283 7915

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2008/000644

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6215404 B1 (MORALES), 10 April 2001. Whole document.	1 – 5
A	WO 2002/037443 A1 (GLOBALA TRYGGHETSBOLAGET AB), 10 May 2002. Whole document.	1 – 5
A	US 2005/0030174 A1 (HESS), 10 February 2005. Whole document.	1 – 5
A	US 7009510 B1 (DOUGLASS et al.), 7 March 2006. Whole document.	1 – 5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/AU2008/000644

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	20040186739						
AU	20040100187						
US	20060067484	US	7245703	US	20040047458	US	20050031091
		US	20050036588	US	20060239250	US	20070081634
		US	20080118039				
US	6215404						
WO	2002037443	AU	12885/02	AU	66525/01	SE	0003971
		SE	0003973	WO	2002001531		
US	20050030174	US	7327220	US	20080180241	WO	2005001785
US	7009510						

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX