(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 605 222 A1

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
14.12.2005 Patentblatt 2005/50

(51) Int Cl.[7]: **F41A 17/06**

(21) Anmeldenummer: **04102570.1**

(22) Anmeldetag: **07.06.2004**

(84) Benannte Vertragsstaaten:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PL PT RO SE SI SK TR
Benannte Erstreckungsstaaten:
AL HR LT LV MK

(71) Anmelder: **Swisscom Mobile AG**
3050 Bern (CH)

(72) Erfinder: **Ritter, Rudolf**
3052, Zollikofen (CH)

(74) Vertreter: **P&TS**
Patents & Technology Surveys SA
Terreaux 7
P.O.Box 2848
2001 Neuchâtel (CH)

(54) Vorrichtung zum Fernkontrollieren der Benutzung einer persönlichen Waffe und persönliche Waffe mit einer solchen Vorrichtung

(57) Kontrollvorrichtung (2) zum Fernkontrollieren der Benutzung einer persönlichen Waffe (1), mit:

einer drahtlosen Schnittstelle (3) zur Kommunikation in einem Mobilfunktelekommunikationsnetzwerk (7),
einem Detektor (4) zur Ermittlung von einem Ereignis aus der persönlichen Waffe (1),
Datenverarbeitungsmitteln (5) zur Bearbeitung eines Signals aus dem besagten Detektors, zur Vorbereitung einer Datenmeldung mit im Signal enthaltenen Informationen und zum Senden der Meldung über die drahtlose Schnittstelle (3).

Persönliche Waffe (1) mit einer solchen Vorrichtung, Datenbank zur Speicherung der in den Datenmeldungen enthaltenen Informationen und Verfahren zum Fernkontrollieren der Benutzung einer persönlichen Waffe (1) mit einer solchen Kontrollvorrichtung.

Dank der Kontrollvorrichtung (2) der Erfindung kann die Benutzung einer bestimmten persönlichen Waffe (1) zum Beispiel aus einer weit entfernten Zentrale (8) überwacht werden. In einer Variante der Erfindung können auch Befehle zur temporären und/oder endgültigen Sperre der Waffe (1) aus der Überwachungszentrale gesendet werden.

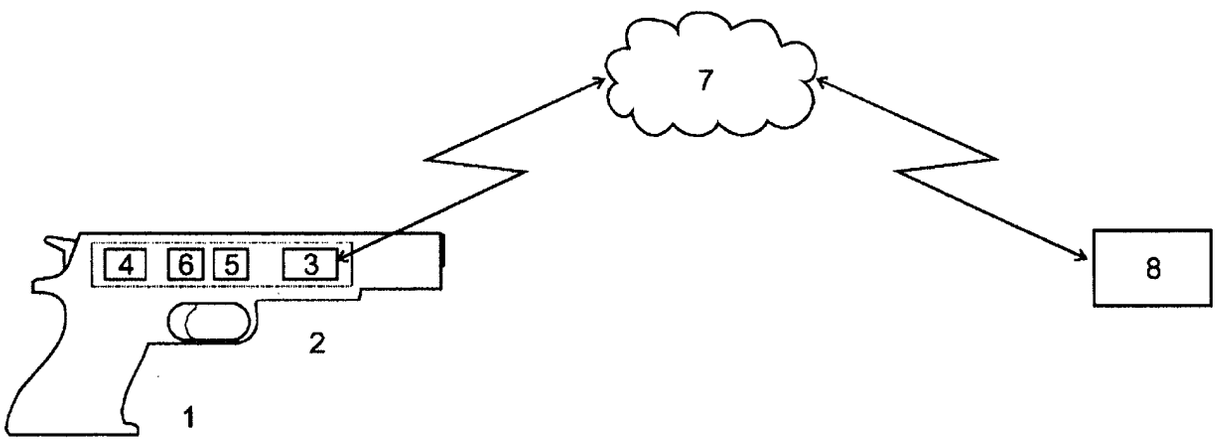

Fig.1

EP 1 605 222 A1

Beschreibung

[0001] Die vorliegende Erfindung betrifft eine Vorrichtung zum Fernkontrollieren der Benutzung einer persönlichen Waffe und eine persönliche Waffe, die eine solche Kontrollvorrichtung umfasst. Die vorliegende Erfindung betrifft insbesondere eine Kontrollvorrichtung zur Detektion von durch eine persönliche Waffe gefeuerten Schüsse und/oder zur Sperre dieser persönlichen Waffe.

[0002] In gewissen Fällen kann es wünschenswert sein, wissen zu können, wann, wo und durch wen ein Schuss von einer bestimmten persönlichen Waffe abgefeuert wurde. Dies ist beispielsweise der Fall, wenn die Verantwortung für gewisse Schüsse, die während einer Übung oder eines bestimmten Einsatzes abgefeuert wurden, bestimmt werden muss. Im Stande der Technik werden üblicherweise solche Informationen mit Hilfe von Waffen externer Elemente wie zum Beispiel Zeugen, Überwachungskameras, externe Detektoren und/oder dem Schützen selber bestimmt.

[0003] Ausserdem ist es auch manchmal wünschenswert, eine persönliche Waffe auf Distanz sperren und/oder auslösen zu können, um zum Beispiel vor einem Einsatz zu vermeiden, dass ein Schütze ohne Befehl schiesst, oder um eine verlorene Waffe zu deaktivieren.

[0004] US2002/0149468 beschreibt ein System und ein Verfahren zum Fernkontrollieren der Benutzung von Objekten, zum Beispiel Waffen, mit Hilfe von RFID. Die RFID können Signale zur temporären oder endgültigen Ausser- oder Inbetriebsetzung des entsprechenden Objektes empfangen und interpretieren. Ein Nachteil dieses Systems ist die kurze Reichweite der Signale, die nur einige hundert Meter beträgt. Dieses System kann also nur Objekte in einem räumlich begrenzten Bereich kontrollieren. Ausserdem sind die RFID passive Elemente, die nicht zum spontanen Senden von Daten geeignet sind. Selbst wenn sie lokal gespeist werden, emittieren RFID nur dann, wenn sie durch einen angepassten Leser gelesen werden.

[0005] Ein Ziel der Erfindung ist also, eine Kontrollvorrichtung zum Fernkontrollieren der Benutzung einer persönlichen Waffe und eine persönliche Waffe vorzuschlagen, welche Nachteile der Kontrollvorrichtungen und der Waffen des Standes der Technik nicht aufweisen.

[0006] Dieses Ziel wird mit einer Kontrollvorrichtung und einer persönlichen Waffe erreicht, welche die Merkmale des entsprechenden unabhängigen Anspruches aufweist. Vorteilhafte Ausführungsformen werden ausserdem durch die abhängigen Ansprüche gegeben.

[0007] Erreicht wird dieses Ziel insbesondere mit einer Kontrollvorrichtung zum Fernkontrollieren der Benutzung einer persönlichen Waffe, mit:

einer drahtlosen Schnittstelle zur Kommunikation in einem Mobilfunktelekommunikationsnetzwerk,
einem Detektor zur Ermittlung von einem Ereignis aus der persönlichen Waffe,

[0008] Datenverarbeitungsmitteln zur Bearbeitung eines Signals aus dem Detektor, zur Vorbereitung einer Datenmeldung mit im besagten Signal enthaltenen Informationen und zum Senden der Datenmeldung über die drahtlose Schnittstelle.

[0009] Erreicht wird dieses Ziel insbesondere auch mit einer persönlichen Waffe mit einer solchen Vorrichtung, mit einer Datenbank zur Speicherung der in den Datenmeldungen enthaltenen Informationen und mit einem Verfahren zum Fernkontrollieren der Benutzung einer persönlichen Waffe mit einer solchen Kontrollvorrichtung.

[0010] Dank der Kontrollvorrichtung der Erfindung kann die Benutzung einer bestimmten persönlichen Waffe zum Beispiel aus einer weit entfernten Zentrale überwacht werden. In einer Variante der Erfindung können auch Befehle zur temporären und/oder endgültigen Sperre oder dem Auslösen der Waffe aus einer entfernten Überwachungszentrale gesendet werden. Die Datenbank der Erfindung erlaubt ausserdem die Speicherung der aus verschiedenen Kontrollvorrichtungen empfangenen Informationen.

[0011] Eine bevorzugte Ausführungsform der vorliegenden Erfindung wird im Folgenden anhand der einzigen Figur näher beschrieben. Sie zeigt:

Fig. 1 eine schematische Darstellung der Kontrollvorrichtung gemäss einer bevorzugten Ausführungsform der Erfindung.

[0012] In einer bevorzugten Ausführungsform ist die Kontrollvorrichtung 2 der Erfindung in einer persönlichen Waffe 1 integriert. Die persönliche Waffe 1 ist zum Beispiel eine Feuerwaffe wie eine Pistole, eine Selbstladewaffe, usw. Sie kann aber auch eine elektrische Waffe, eine Warnwaffe, eine blanke Waffe, usw., sein. Die Kontrollvorrichtung 2 wird vorzugsweise bei der Herstellung der Waffe 1 eingebaut. In einer anderen Ausführungsform wird mindestens ein Teil der Kontrollvorrichtung 2 der Erfindung an eine bestehende Waffe angebracht. Die Waffe weist dann vorzugsweise Befestigungselemente, die zur sicheren Befestigung der Kontrollvorrichtung 2 auf der Waffe angepasst sind, auf.

[0013] Die Kontrollvorrichtung 2 der Erfindung umfasst eine drahtlose Schnittstelle 3, um über ein mobiles Telekommunikationsnetzwerk 7 vorzugsweise bidirektional kommunizieren zu können. In einer bevorzugten Ausführungsform der Erfindung ist die Schnittstelle 3 eine Funkschnittstelle zur Kommunikation in einem zellularen Netzwerk 7 wie zum Beispiel einem GSM, UMTS, CDMA oder GPRS Netzwerk oder in einem Wireless LAN (WLAN). Die Schnittstelle 3 besteht möglicherweise aus einem integrierten Modul oder aus einem in der Waffe 1 einschiebbaren Modul im PC-Card Format oder in einem anderen geeigneten Format.

[0014] In einer anderen nicht dargestellten Ausfüh-

rungsform der Erfindung umfasst die Waffe 1 eine lokale drahtlose Schnittstelle wie zum Beispiel eine Bluetooth, Home-RF, IrdA, WLAN oder proprietäre Schnittstelle, die zur Kommunikation mit einem externen vorzugsweise tragbaren Mobilgerät, zum Beispiel mit einem Mobiltelefon, vorgesehen ist, wobei das externe Mobilgerät eine drahtlose Schnittstelle zur Kommunikation im Netzwerk 7 umfasst. Der Benutzer der Waffe 1 trägt dann vorzugsweise auch das Mobilgerät mit sich, damit die Waffe 1 über dem Netzwerk 7 durch das Mobilgerät kommunizieren kann. Um die Vertraulichkeit der Kommunikationen zwischen der Waffe 1 und dem Mobilgerät zu gewährleisten, werden sie vorzugsweise gesichert, indem sie zum Beispiel verschlüsselt werden.

[0015] Die Kontrollvorrichtung 2 der Erfindung umfasst vorzugsweise ein Identifizierungsmodul 6, beispielsweise eine herausnehmbare Chip-Karte, zur Identifizierung des Benutzers der Waffe 1 im Netzwerk 7. Das Identifizierungsmodul 6 erlaubt zumindest eine Datenübertragung über das Netzwerk 7. Die Datenübertragung erfolgt zum Beispiel über SMS, USSD und/oder MMS Meldungen und/oder über IP-Pakete. Obwohl eine Sprachverbindung über das Netzwerk 7 möglich wäre, ist sie für diese Anwendung nicht notwendig. Wie später erläutert, kann aber im Rahmen der Erfindung die Möglichkeit, eine solche Verbindung mit der Kontrollvorrichtung 2 der Waffe 1 aufstellen zu können, vorgesehen werden.

[0016] Die Kontrollvorrichtung 2 umfasst einen Detektor 4 zur Ermittlung von Ereignissen aus der Waffe 1. Die ermittelten Ereignisse umfassen zum Beispiel jedem durch die Waffe 1 abgefeuerten Schuss.

[0017] In einer bevorzugten Ausführungsform wird in der Waffe 1 bei jedem abgefeuerten Schuss ein elektrisches Signal, zum Beispiel ein elektrischer Impuls erzeugt. Die Waffe 1 umfasst dann zum Beispiel eine nicht dargestellte Vorrichtung zur Umwandlung der durch die Schüsse erzeugten mechanischen Impulse in elektrische Signale. Andere Systeme zur Erzeugung des elektrischen Signals in der Waffe 1 sind im Rahmen der Erfindung auch möglich. Es kann beispielsweise ein elektrischer Kontakt bei jedem Schuss mechanisch geöffnet oder geschlossen werden, was zum Beispiel zur Auslösung eines elektrischen Signals durch einen nicht dargestellten Kontroller in der Waffe 1 führt. Das ausgelöste elektrische Signal ist zum Beispiel ein einfacher elektrischer Impuls oder ein komplexeres zum Beispiel digitales Signal. Gemäss dieser Ausführungsform der Erfindung umfasst vorzugsweise der Detektor 4 eine elektrische Leitung, mit welcher die durch die Waffe 1 erzeugten elektrischen Signale empfangen und weitergeleitet werden können.

[0018] In einer weiteren Ausführungsform ermittelt die Kontrollvorrichtung 2 direkt den mechanischen Stoss, welcher beim Schuss erzeugt wird und sich in der mechanischen Struktur der Waffe 1 verbreitet. Der Detektor 4 umfasst dann vorzugsweise einen Sensor, welcher zum Beispiel jedes Mal wenn er einen mechanischen Impuls einer gewissen Stärke fühlt einen elektrischen Impuls erzeugt. In einer Ausführungsform der Erfindung wird der Detektor 4 mindestens teilweise als MEMS (micro electromechanical system) realisiert.

[0019] In einer noch weiteren Ausführungsform werden die Ereignisse, zum Beispiel die gefeuerten Schüsse, mit Hilfe von einem Lärm, zum Beispiel dem Knallen, ermittelt. Der Detektor 4 umfasst dann zum Beispiel einen akustischen Sensor oder einen Drucksensor, zum Beispiel ein Mikrophon, welches ein elektrisches Signal bei jedem Knallen erzeugt.

[0020] In noch weiteren Ausführungsformen der Erfindung werden noch andere Typen von überwachten Ereignissen wie zum Beispiel Kombinationen von Druck-, Gas- und/oder Temperaturvariationen vom Detektor 4 ermittelt.

[0021] Bei jedem durch die Waffe 1 abgefeuerten Schuss empfängt vorzugsweise die Kontrollvorrichtung 2 der Erfindung ein Signal aus dem Detektor 4. Für jedes empfangene Signal erzeugen Datenverarbeitungsmittel, zum Beispiel ein Prozessor 5, in der Kontrollvorrichtung 2 eine digitale Datenmeldung, die Informationen über den gefeuerten Schuss enthält. Wie später erläutert können die in der Meldung enthaltenen Informationen zum Beispiel die Uhrzeit und das Datum des gefeuerten Schusses, die Identität des Benutzers der Waffe 1, den Standort der Waffe 1 als der Schuss gefeuert wurde, usw., umfassen.

[0022] In einer Ausführungsform der Erfindung werden die Uhrzeit und das Datum durch eine Uhr ermittelt, die sich in der Waffe 1, beispielsweise in der Kontrollvorrichtung 2, befindet. Ein Nachteil dieser Ausführungsform ist, dass diese Uhr zum Beispiel durch den Benutzer der Waffe 1 verstellt werden kann. Es können also die Daten über die Uhrzeit und das Datum des Schusses verfälscht werden. Um eine solche Verfälschung zu vermeiden werden in einer bevorzugten Ausführungsform der Erfindung die Uhrzeit und das Datum aus dem Netzwerk 7 entnommen. Es werden zum Beispiel die Uhrzeit und das Datum des Netzwerks 7 benutzt. Es können auch Daten aus einem nicht dargestellten am Netzwerk 7 angeschlossenen Server oder aus einem sattelitären Standortbestimmungssignal, zum Beispiel aus einem GPS oder Galileo Signal, entnommen werden. In diesem letzten Fall umfasst vorzugsweise die Kontrollvorrichtung 2 eine Schnittstelle zum Empfang der Standortbestimmungssignale wie zum Beispiel eine GPS oder eine Galileo Schnittstelle. Um eine spätere Verfälschung dieser Daten nach der Aufbereitung der Meldung zu vermeiden wird die Meldung vorzugsweise signiert und mit einem Zeitstempel markiert.

[0023] Die Identität des Benutzers der Waffe 1 wird vorzugsweise durch das Identifizierungsmodul 6 ermittelt. In einer Ausführungsform der Erfindung enthält das Identifizierungsmodul 6 eine eindeutige Identifizierung, zum Beispiel eine Identifizierungsnummer wie eine IMSI oder eine MSISDN Nummer, die auch zu ihrer Identifi-

zierung im Netzwerk 7 dient. Diese Identifizierung wird in der Meldung einbezogen, damit die Personalien des Benutzers zum Beispiel sein Name, Adresse, usw., beispielsweise aus einer Datenbank ermittelt werden können. Die Datenbank wird zum Beispiel durch den Betreiber des Netzwerks 7 verwaltet und die Personalien der Benutzer werden dem Empfänger durch diesen Vertreiber mitgeteilt. Vorzugsweise verwaltet aber der Empfänger seine eigene Datenbank, damit er eine gewisse Kontrolle über diese Daten ausüben kann und sie vorzugsweise vertraulich bleiben. Die Identifizierung des Benutzers der Waffe 1 kann also vorzugsweise ohne Eingriff des Betreibers des Netzwerks 7 erfolgen. In einer Variante der Erfindung enthält das Identifizierungsmodul 6 die vollständigen Personalien des Benutzers, die dann als solche in die Meldung einbezogen werden. Die Identität des Benutzers umfasst zum Beispiel sein Name, Adresse, Funktion, seinen Rang, usw. Die Meldung wird dann vorzugsweise verschlüsselt, damit diese Daten durch unbefugte Empfänger nicht gelesen werden können. In einer Ausführungsvariante der Erfindung basiert die Authentifizierung des Benutzers auf einem biometrischen Sensor oder auf Daten in einem RFID-Tag.

[0024] Der Standort der Waffe 1 wird beispielsweise im Netzwerk 7 durch Triangulation oder durch einen nicht dargestellten in der Waffe 1 integrierten GPS-Empfänger ermittelt. Ist die Waffe 1 mit GPS und/oder Galileo Mitteln bestückt, kann zusätzlich zur Position ebenfalls Azimut und Elevation der Waffe 1 ermittelt werden.

[0025] Um die Authentifizierung der Meldung zu erlauben, wird sie vorzugsweise durch das Identifizierungsmodul 6 signiert. Die Meldung kann auch vom Identifizierungsmodul 6 verschlüsselt werden, damit sie nur durch befugte Empfänger gelesen werden kann. Es können auch asymmetrische Schlüssel in der Kontrollvorrichtung 2 verwendet werden, um die Meldung zu signieren und zu verschlüsseln. Der dazu verwendete Zertifikat kann vom Betreiber des Netzwerks 7 oder vorzugsweise vom Betreiber einer Zentrale 8 oder von einer Behörde ausgestellt werden.

[0026] Die Datenmeldung wird dann zum Beispiel durch die drahtlose Schnittstelle 3 über das Netzwerk 7 an einen Empfänger, zum Beispiel einer entfernten Zentrale 8, gesendet, oder in einem nicht dargestellten Speicherbereich der Kontrollvorrichtung 2 oder des Identifizierungsmoduls 6 in der Erwartung eines späteren Sendens dieser Meldung gespeichert. Die Meldung ist vorzugsweise zur Übertragung über das Telekommunikationsnetzwerk 7 angepasst. Ist das Netzwerk 7 beispielsweise ein GSM-Netzwerk, dann ist die Meldung zum Beispiel eine SMS-, eine USSD- oder eine MMS-Meldung. Im Falle eines GPRS- oder UMTS-Netzwerks kann die Meldung zum Beispiel als E-Mail oder anderes IP-Pakete gesendet werden.

[0027] Die Zeitpunkte zu welchen die Meldungen gesendet werden, können vorzugsweise mit Hilfe von einem oder mehreren Parametern bestimmt werden. Diese Parameter umfassen zum Beispiel die Anzahl gefeuerte Schüsse seit der letzten Meldung, das Zeitintervall seit der letzten Meldung, der momentane Einsatz der Waffe 1, das Vorhandensein des Telekommunikationsnetzwerks 7, der Standort der Waffe 1, usw. In einer Ausführungsform der Erfindung wird zum Beispiel eine Meldung automatisch unmittelbar nach jedem Schuss gesendet. Somit wird insbesondere vermieden, dass die Meldungen in der Kontrollvorrichtung 2 gespeichert werden, was auch zum Beispiel eine Verfälschung der Daten während dieser Speicherzeit verhindert.

[0028] In anderen Ausführungsformen werden die Meldungen zum Beispiel nach einer gewissen Anzahl Schüsse und/oder nach einem gewissen Zeitintervall seit der letzten Meldung gesendet. In diesen Fällen beinhaltet eine ausgesandte Meldung Daten über mehrere Schüsse oder es werden mehrere Meldungen gleichzeitig gesendet. Die Aussendung der gespeicherten Meldungen kann auch getriggert werden, wenn die Waffe 1 sich in einem bestimmten Standort befindet, zum Beispiel wenn sie in einem gewissen Gebäude, zum Beispiel einer Kaserne, einer Polizeistation, usw., ist, was üblicherweise mit dem Ende eines Einsatzes übereinstimmt.

[0029] Umfasst die Waffe 1 eine lokale drahtlose Schnittstelle, die zur Kommunikation mit einem tragbaren Mobilgerät vorgesehen ist, wobei das Mobilgerät eine drahtlose Schnittstelle zur Kommunikation im Netzwerk 7 umfasst, kann das Senden der Datenmeldung durch die Aktivierung dieser lokalen Schnittstelle getriggert werden. Vorzugsweise kann das Senden der Meldung auch manuell durch den Benutzer zum Beispiel am Ende eines Einsatzes getriggert werden.

[0030] Die Parameter zur Bestimmung des Zeitintervalls zwischen zwei gesendeten Meldungen können vorzugsweise angepasst werden, zum Beispiel durch Betätigung einer nicht dargestellten Benutzerschnittstelle der Kontrollvorrichtung 2 und/oder durch Befehle in Meldungen, die der Waffe 1 über das Telekommunikationsnetzwerk 7 gesendet werden.

[0031] Falls am für die Aussendung vorgesehenen Zeitpunkt keine Meldung gesendet werden kann, weil zum Beispiel keine Verbindung mit dem Netzwerk 7 aufgebaut werden kann, wird vorzugsweise das Senden wiederholt, bis es erfolgreich durchgeführt wird. Das Zeitintervall zwischen zwei aufeinanderfolgenden Wiederholungen wird vorzugsweise immer länger mit der Anzahl der Versuche. In einer Variante der Erfindung wird nach einer gewissen Anzahl Versuche das Senden unterbrochen. Der Benutzer wird dann vorzugsweise mit Hilfe einer Warnlampe, eines Tonsignals und/oder einer Meldung auf einer nicht dargestellten Anzeige der Kontrollvorrichtung 2 davor gewarnt und gebeten, das Senden manuell zu triggern, wenn die Verbindung wieder herstellbar ist.

[0032] Die Meldungen mit den Informationen über die von der Waffe 1 abgefeuerten Schüsse werden einem Empfänger, zum Beispiel einer Zentrale 8, beispielswei-

se einer Polizeizentrale, gesendet, welche für das Kontrollieren der Waffe und deren Einsatz verantwortlich ist. Im Falle von Polizeiwaffen werden zum Beispiel die Meldungen aus allen in einem gewissen geographischen Bereich eingesetzten Waffen zu einer gewissen Polizeizentrale gesendet. Die in den Meldungen enthaltenen Informationen werden dort zum Beispiel analysiert und/oder gespeichert. Die Informationen wie die Identität des Benutzers, die Uhrzeit und das Datum der abgefeuerten Schüsse, der Standort der Waffe 1 bei jedem Schuss, usw., werden vorzugsweise in einer zentralen Datenbank gespeichert, um im Falle einer Klage gegen die Benutzung einer bestimmten Waffe 1 den aktuellen Einsatz der entsprechenden Waffe 1 beweisen zu können. Die zentrale Datenbank wird vorzugsweise durch den Betreiber der Zentrale 8 verwaltet, um die Vertraulichkeit der Informationen gewährleisten zu können. Beim Empfang werden die Meldungen vorzugsweise ebenfalls mit einem Zeitstempel markiert, damit die Empfangszeit und -datum auch in einer sicheren und unwiderruflichen Weise gespeichert werden.

[0033] In einer Variante der Erfindung wird die Waffe 1 durch einen Verein zum Beispiel einen Schiessverein verwaltet, welcher Wettbewerbe und/oder Spiele mit harmlosen Waffen organisiert. Die Daten über die Benutzung der Waffe 1 werden dann zum Beispiel dazu gebraucht, um die Benutzung der Waffe 1 dem entsprechenden Spieler zu verrechnen, und/oder um entsprechende Einsätze zu analysieren.

[0034] In einer Variante der Erfindung umfasst die Waffe 1 und/oder die Kontrollvorrichtung 2 nicht dargestellte Mittel zur Identifizierung und/oder Authentisierung des Benutzers der Waffe 1 mit Hilfe von biometrischen Parametern. Diese Mittel umfassen zum Beispiel Sensoren auf dem Kolben der Waffe 1 zur Erkennung der Fingerabdrücke des Benutzers, die dann in einem Vektor gewandelt werden. Zur Authentisierung des Benutzers wird zum Beispiel der erzeugte Vektor mit einem Referenzvektor verglichen, welcher den Fingerabdrükken des Benutzers des Identifizierungsmoduls 6 entspricht. Wenn beide Vektoren nicht übereinstimmen, das heisst wenn der Benutzer nicht authentifiziert wird, kann zum Beispiel die Kontrollvorrichtung 2 die Benutzung der Waffe 1 temporär oder endgültig sperren. In einer Variante kann der nicht authentifizierte Benutzer aufgefordert werden, seine Identität mit Hilfe einer Benutzerschnittstelle der Kontrollvorrichtung 2 anzugeben, bevor ihm die Benutzung der Waffe 1 erlaubt wird.

[0035] In einer Variante der Erfindung wird der Benutzer der Waffe 1 mit Hilfe seiner biometrischen Parametern identifiziert, indem der Vektor mit einer gewissen Anzahl Referenzvektoren verglichen wird, wobei jeder Referenzvektor den Fingerabdrücken eines befugten Benutzers der Waffe 1 entspricht. Vorzugsweise wird die Benutzung der Waffe 1 durch die Kontrollvorrichtung 2 nur dann erlaubt, wenn der aktuelle Benutzer einer der erlaubten Benutzern ist.

[0036] Vorzugsweise werden der Referenzvektor oder die Referenzvektoren in der Kontrollvorrichtung 2 beispielsweise im Identifizierungsmodul 6 gespeichert.

[0037] In einer weiteren Ausführungsform werden die biometrischen Parameter in einer Meldung dem Empfänger 8 gesendet, welcher die Authentifizierung und/oder Identifizierung des Benutzers anhand von vor oder nach dem Schuss ermittelten Referenzvektoren durchführen wird.

[0038] Vorzugsweise werden die biometrischen Parameter des Benutzers in jeder Meldung zusammen mit den anderen Informationen über die abgefeuerten Schüsse gesendet, insbesondere wenn mehrere Benutzer die gleiche Waffe 1 benutzen können oder wenn der Benutzer nicht authentifiziert wurde.

[0039] Andere Identifizierungs- und/oder Authentifizierungsmittel sind im Rahmen der Erfindung auch möglich. Der Benutzer kann zum Beispiel aufgefordert werden, ein vorzugsweise nur ihm bekanntes Geheimnis mit Hilfe einer Benutzerschnittstelle der Kontrollvorrichtung 2 einzugeben, um die Benutzung der Waffe 1 zu ermöglichen.

[0040] Gemäss einer bevorzugten Ausführungsform der Erfindung können Befehlssignale durch die Kontrollvorrichtung 2 an die Waffe 1 gesendet werden. Die Befehlssignale dienen zum Beispiel zur temporären oder endgültigen Sperrung und/oder Auslösung der Waffe 1, zum Beispiel um ihren Einsatz vor einem gewissen Zeitpunkt zu vermeiden, oder um die Waffe 1 endgültig ausser Betrieb zu setzen, zum Beispiel nachdem die Waffe 1 verloren oder gestohlen wurde.

[0041] Die drahtlose Schnittstelle 3 der Kontrollvorrichtung 2 kann also vorzugsweise auch Meldungen über das Telekommunikationsnetzwerk 7 empfangen. Wie bei der Aussendung von Meldungen sind die empfangenen Meldungen dem Typ des Netzwerks 7 angepasst. Die Meldungen sind somit zum Beispiel SMS- und/oder MMS-Meldungen im Falle eines GSM-Netzwerks 7, E-Mail Nachrichten und/oder andere IP-Pakete im Falle eines UMTS- oder GPRS Netzwerks 7, usw.

[0042] Eine durch die Kontrollvorrichtung 2 empfangene Meldung umfasst zum Beispiel bestimmte Zeichen oder Zeichenfolgen, die durch die Kontrollvorrichtung 2 interpretiert werden und zum Senden der entsprechenden Befehle an die Waffe 1 führen. Vorzugsweise wird die Meldung durch die Zentrale 8 mit ihrer Signatur signiert, damit die Waffe 1 den Ursprung der Befehle überprüfen kann. Die Meldung wird ausserdem vorzugsweise noch mit der öffentlichen Signatur der Waffe 1, die zum Beispiel im Identifizierungsmodul 6 gespeichert ist, verschlüsselt, damit nur diese bestimmte Waffe 1 die Meldung lesen kann und die Befehle ausführen wird.

[0043] Die durch die Kontrollvorrichtung 2 der Waffe 1 gesandten Befehlssignale sind zum Beispiel digitale elektrische Signale, die zum Beispiel durch einen nicht dargestellten Kontroller der Waffe 1 empfangen und interpretiert werden. Der Kontroller steuert dann zum Beispiel ein nicht dargestelltes mechanisches und/oder elektronisches Sperrmittel innerhalb der Waffe 1 zu ihrer

temporären oder endgültigen Sperre. Diese Sperrmittel umfassen beispielsweise einen elektromagnetischen Aktuator, welcher den Drücker der Waffe 1 blockieren kann. Zur endgültigen Sperre der Waffe 1 wird vorzugsweise ein mechanisches und/oder elektrisches Element innerhalb der Waffe 1 zerstört, damit sie nicht mehr benutzt werden kann.

[0044] In einer anderen Ausführungsform der Erfindung betätigt die Kontrollvorrichtung 2 direkt die elektronischen und/oder mechanischen Sperrmittel der Waffe 1. Somit wird die über die erste Schnittstelle 3 empfangene Meldung in der Kontrollvorrichtung 2 interpretiert und direkt zur entsprechenden Betätigung der Sperrmittel gelangen.

[0045] In bestimmten Fällen können die Befehlssignale durch die Kontrollvorrichtung 2 selber generiert werden, zum Beispiel um die Waffe 1 nach einer gewissen Ruhezeit oder wenn der Benutzer nicht authentifiziert werden kann, usw., automatisch zu sperren. Vorzugsweise werden aber die Befehle von der Kontrollvorrichtung 2 an die Waffe 1 durch über das Telekommunikationsnetzwerk 7 empfangenen Meldungen getriggert.

[0046] In einer Variante der Erfindung kann die Kontrollvorrichtung 2 der Erfindung Signale zum Abfeuern von Schüssen durch die Waffe 1 senden und/oder durchführen. In diesem Fall können zum Beispiel die Sperrmittel der Waffe 1 Schüsse auch abfeuern, indem beispielsweise der elektromagnetische Aktuator zur Blockierung des Drückers ihn auch betätigen kann. Die Signale zum Abfeuern von Schüssen können vorzugsweise auch mit Hilfe von über das Netzwerk 7 empfangene Meldungen getriggert werden. Somit kann also das Abfeuern von Schüssen durch die Waffe 1 ferngesteuert werden.

[0047] Wenn die Waffe 1 keine Meldung aus der Zentrale 8 bekommen kann, zum Beispiel weil sie sich in einem Gebiet befindet, wo kein Empfang vom Netzwerk 7 vorhanden ist, kann sie vorzugsweise völlig manuell eingesetzt werden. Sie kann zum Beispiel manuell gesperrt und/oder ausgelöst werden, nachdem ein Sicherheitscode über mechanische oder elektromechanische Eingabemittel eingegeben wurden. Andere Verhalten der Waffe 1 sind im Rahmen der Erfindung auch möglich. Die Waffe 1 kann zum Beispiel ihren letzten Status, gesperrt oder ausgelöst, behalten, bis eine Verbindung mit der Zentrale 8 wieder möglich ist. Sie kann auch gesperrt werden, sobald keine Verbindung vorhanden ist, zum Beispiel um einen Missbrauch während einem Wettbewerb oder einem Spiel zu vermeiden.

[0048] In einer Ausführungsform der Erfindung wird die Waffe 1 nur dann ausgelöst, wenn ihre interne Uhr durch eine externe Zeitangabe kalibriert werden konnte und/oder wenn die Uhrzeit und das Datum aus dem Netzwerk 7 oder aus einem entfernten Server ermittelt werden konnte.

[0049] Vorzugsweise umfasst die Waffe 1 zum Beispiel auf der Kontrollvorrichtung eine Anzeige und/oder Warnlampe um den Zustand der Waffe 1 dem Benutzer mitteilen zu können. Eine Warndiode wird zum Beispiel aktiviert, wenn die Waffe ferngesteuert und/oder fernüberwacht wird. Eine weitere Diode wird zum Beispiel aktiviert, wenn die Waffe gesperrt ist, usw.

[0050] Die Kontrollvorrichtung wird vorzugsweise durch Batterien in der Waffe 1 gespeist. Die Batterien sind vorzugsweise wiederaufladbare Batterien, die zum Beispiel aus der Waffe 1 herausgenommen werden können, um auf einem adaptierten Ladegerät geladen zu werden. In einer anderen Ausführungsform können die Batterien auch direkt in der Waffe 1 aufgeladen werden, indem zum Beispiel die Waffe für eine bestimmte Zeit an eine elektrische Stromquelle angeschlossen wird. Falls die Batterie leer ist, und die Kontrollvorrichtung 2 nicht mehr gespeist werden kann, kann vorzugsweise die Waffe 1 mindestens für eine gewisse Zeit weiter benutzt werden. Die Waffe 1 sperrt sich dann möglicherweise automatisch, um einen unerlaubten Einsatz zu vermeiden. Andere Verhalten der Waffe 1 sind bei niedriger Speisung der Kontrollvorrichtung 2 im Rahmen der Erfindung auch möglich. In einer Ausführungsform, wird zum Beispiel die Waffe 1 gesperrt sobald die Kontrollvorrichtung 2 eine niedrige Speisung detektiert. In einer anderen Ausführungsform schaltet die Kontrollvorrichtung 2 die Schnittstelle 3 aus, sobald die vorhandene Energie unter einer gewissen Schwelle ist. Sie funktioniert aber weiter, um die Daten über die Benutzung der Waffe zum Beispiel in einem Logfile zu speichern. Nach einer tieferen Energieschwelle wird möglicherweise die Waffe 1 temporär und/oder endgültig gesperrt. Weitere Kombinationen dieser verschiedenen Verhalten sind im Rahmen der Erfindung auch möglich. Die Schnittstelle 3 kann auch separat vom Rest der Kontrollvorrichtung 2 gespeist werden, damit Meldungen auch bei leeren Waffenbatterie gesendet und/oder empfangen werden können.

[0051] Die Datenmeldungen, die durch die Waffe 1 gesendet und/oder empfangen werden, werden vorzugsweise signiert und/oder verschlüsselt, um ihre Unwiderrufbarkeit zu sichern. Somit können die darin enthaltenen Informationen und/oder Befehle als sicher und authentisch betrachtet werden. Sie könnten also zum Beispiel als Beweise im Falle einer Klage benutzt werden. Die Verschlüsselung der Meldungen sichert ausserdem, dass unbefugte Empfänger der Meldungen diese nicht lesen können, damit zum Beispiel Gegner des Benutzers der Waffe 1, die Informationen über die abgefeuerten Schüsse nicht wissen können. Die Übermittlung der Meldungen ist vorzugsweise End-zu-End gesichert, indem die Verschlüsselung mit einem Schlüssel durchgeführt wird, welcher nur dem Sender und Empfänger bekannt sind. Dass heisst, dass nur der Sender, zum Beispiel die Kontrollvorrichtung 2 der Waffe 1, und nur der Empfänger, zum Beispiel die Zentrale 8, die darin enthaltenen Informationen lesen können. Die Datenmeldungen sind somit auch gegenüber dem Betreiber des Netzwerks 7 vertraulich.

[0052] Die Kontrollvorrichtung 2 der Erfindung ist zur

Überwachung von verschiedenen Ereignissen einsetzbar. Es können zum Beispiel Signale der Kontrollvorrichtung 2 geschickt werden, wenn die Waffe 1 ein- oder ausgeschaltet wird, wenn neue Munition geladen wird, wenn das Identifizierungsmodul 6 gewechselt wird, wenn die Waffe bewegt wird, usw. Diese Ereignisse werden vorzugsweise als Datenmeldungen mit einem Zeitstempel entweder der Zentrale 8 gesendet oder in die Kontrollvorrichtung 2 zum Beispiel in einem Logfile gespeichert, welches zum Beispiel der Zentrale 8 zu einem bestimmten späteren Zeitpunkte gesendet wird.

[0053] In einer Variante der Erfindung wird jedes Projektil der Waffe 1 mit einem Identifizierungselement vorgesehen, welches mit der Kontrollvorrichtung 2 der Erfindung kommunizieren kann. Solche Identifizierungselemente sind zum Beispiel RFID-Elemente mit einer eindeutigen Identifizierungsnummer. Vorzugsweise umfassen dann die gesendeten Datenmeldungen über die gefeuerten Schüsse auch die Identifizierungsnummer des gefeuerten Projektils.

[0054] In einer Variante der Erfindung wird eine Kommunikation auf einem Nutzkanal im Netzwerk 7 zwischen der Kontrollvorrichtung 2 und der Zentrale 8 zum Beispiel während einem ganzen Einsatz geöffnet, um Daten auf dem Kanal kontinuierlich senden zu können. Informationen über die abgefeuerten Schüsse können somit durch die Kontrollvorrichtung 2 in Echtzeit der Zentrale 8 geschickt werden. Auf dem Nutzkanal kann auch Ton zwischen der Waffe 1 und der Zentrale 8 ausgetauscht werden. Die Kontrollvorrichtung 2 wird also vorzugsweise mit einem nicht dargestellten Lautsprecher und/oder mit einem nicht dargestellten Mikrophon vorgesehen. Es werden zum Beispiel auf dem Nutzkanal das Knallen der Feuerschüsse, die Geräusche des Ladens der Munition in der Waffe 1, usw., der Zentrale 8 in Echtzeit übermittelt. Vorzugsweise kann auch ein Gespräch zwischen dem Benutzer der Waffe 1 und der Zentrale über die Kontrollvorrichtung 2 aufgestellt werden. Somit können zum Beispiel vokale Befehle und/oder Informationen zwischen dem Benutzer und der Zentrale 8 ausgetauscht werden. Der Benutzer bittet zum Beispiel durch den Nutzkanal die Zentrale 8 um die Erlaubnis zu schiessen, die Zentrale 8 antwortet dann über den Nutzkanal, dass der Benutzer die Erlaubnis hat und sendet gleichzeitig eine Datenmeldung, um die Waffe 1 auszulösen.

[0055] In der obigen Beschreibung wurden Datenmeldungen und/oder Ton zwischen der Waffe 1 und einer entfernten Zentrale 8 ausgetauscht. Der Fachmann wird aber leicht einsehen, dass dieser Austausch auch zwischen zwei Waffen 1 stattfinden kann. Es können zum Beispiel Gruppen von Waffen gebildet werden, welche miteinander Daten und/oder Ton über das Netzwerk 7 oder über ein lokales Netz austauschen können. Der Benutzer einer bestimmten Waffe ist zum Beispiel der Gruppenführer, welcher während einem Einsatz zum Beispiel für die Auslösung und/oder Sperrung der Waffen seiner Gruppe zuständig ist. Er kann also die entsprechenden Datenmeldungen der anderen Waffen seiner Gruppe zum Beispiel mit Hilfe von der Kontrollvorrichtung seiner Waffe entweder direkt oder über eine Zentrale 8 senden. Er kann auch vorzugsweise Daten und oder vokale Befehle den Teilnehmern seiner Gruppe über das Netzwerk 7 durch den Nutzkanal erteilen, usw.

[0056] In der obigen Beschreibung ist die Kontrollvorrichtung 2 mit ihrer drahtlosen Schnittstelle 3 zur Kommunikation im Mobilfunktelekommunikationsnetzwerk 7 in einer persönlichen Waffe 1 integriert. In einer Variante der Erfindung ist aber die Kontrollvorrichtung in einem Mobilfunktelekommunikationsendgerät integriert, welches zum Auswerfen von Projektilen ausgerüstet ist. Die Kontrollvorrichtung der Erfindung benutzt dann vorzugsweise zur Kommunikation im Mobilfunktelekommunikationsnetzwerk 7 die drahtlose Schnittstelle des mobilen Endgeräts, welche zum Beispiel auch für die mit dem Endgerät aufgebauten Telefonverbindungen benutzt wird. Gemäss dieser Variante ist also im Mobilfunkendgerät eine Waffe integriert, die erfindungsgemäss mittels der Kontrollvorrichtung im Endgerät fernkontrolliert werden kann.

Patentansprüche

1. Kontrollvorrichtung (2) zum Fernkontrollieren der Benutzung einer persönlichen Waffe (1), mit:

   einer drahtlosen Schnittstelle (3) zur Kommunikation in einem Mobilfunktelekommunikationsnetzwerk (7),
   einem Detektor (4) zur Ermittlung von einem Ereignis aus der besagten persönlichen Waffe (1),

   Datenverarbeitungsmitteln (5) zur Bearbeitung eines Signals aus dem besagten Detektor (4), zur Vorbereitung einer Datenmeldung mit im besagten Signal enthaltenen Informationen und zum Senden der besagten Meldung über die besagte drahtlose Schnittstelle (3).

2. Kontrollvorrichtung (2) gemäss dem vorherigen Anspruch, die ein Identifizierungsmodul (6) zur Identifizierung der besagten Waffe (1) im besagten Telekommunikationsnetzwerk (7) umfasst.

3. Kontrollvorrichtung (2) gemäss dem vorherigen Anspruch, wobei das besagte Identifizierungsmodul (6) eine Chip-Karte ist.

4. Kontrollvorrichtung (2) gemäss einem der vorherigen Ansprüche, die einen Speicherbereich zur Speicherung der besagten Datenmeldung vor dem besagten Senden umfasst.

5. Kontrollvorrichtung (2) gemäss einem der vorherigen Ansprüche, welche zur Integration in der besagten persönlichen Waffe (1) angepasst ist.

6. Kontrollvorrichtung (2) gemäss einem der vorherigen Ansprüche, wobei die besagte Datenmeldung dem besagten Mobilfunktelekommunikationsnetzwerk (7) angepasst ist.

7. Kontrollvorrichtung (2) gemäss einem der vorherigen Ansprüche, wobei das besagte Signal Informationen über mindestens einen durch die persönliche Waffe (1) gefeuerten Schuss enthält.

8. Kontrollvorrichtung (2) gemäss dem vorherigen Anspruch, wobei der besagte Detektor (4) einen Sensor zur Detektion der durch die besagte persönliche Waffe (1) gefeuerten Schüsse umfasst.

9. Kontrollvorrichtung (2) gemäss einem der Ansprüche 7 oder 8, wobei die besagte Datenmeldung die Uhrzeit und das Datum des besagten mindestens eines Schusses enthält.

10. Kontrollvorrichtung (2) gemäss dem vorherigen Anspruch, wobei die besagte Datenmeldung mit einem Zeitstempel markiert ist.

11. Kontrollvorrichtung (2) gemäss einem der Ansprüche 9 oder 10, wobei die besagte Uhrzeit und das besagte Datum aus dem besagten Telekommunikationsnetzwerk (7) entnommen werden.

12. Kontrollvorrichtung (2) gemäss einem der Ansprüche 9 oder 10, wobei die besagte Uhrzeit und das besagte Datum aus einem sattelitären Standortbestimmungssignal entnommen werden.

13. Kontrollvorrichtung (2) gemäss einem der Ansprüche 7 bis 12, wobei die besagte Datenmeldung die Identität des Benutzers der besagten persönlichen Waffe (1) als der besagte mindestens ein Schuss gefeuert wurde enthält.

14. Kontrollvorrichtung (2) gemäss dem vorherigen Anspruch, wobei die besagte Identität durch ein Identifizierungsmodul (6) in der besagten Kontrollvorrichtung ermittelt wird.

15. Kontrollvorrichtung (2) gemäss einem der Ansprüche 7 bis 14, wobei die besagte Identität mit biometrischen Parametern des besagten Benutzers ermittelt und/oder geprüft wird.

16. Kontrollvorrichtung (2) gemäss einem der Ansprüche 7 bis 15, wobei die besagte Datenmeldung den Standort der besagten persönlichen Waffe (1) als der besagte mindestens ein Schuss gefeuert wurde enthält.

17. Kontrollvorrichtung (2) gemäss einem der Ansprüche 7 bis 16, wobei die besagte Datenmeldung eine Identifizierung des Projektils enthält, welches während dem besagten mindestens einen Schuss abgefeuert wurde.

18. Kontrollvorrichtung (2) gemäss einem der vorherigen Ansprüche, die zum Empfangen von Meldungen über die besagte drahtlose Schnittstelle (3) angepasst ist.

19. Kontrollvorrichtung (2) gemäss dem vorherigen Anspruch, wobei die besagten Meldungen Befehle zur temporären und/oder endgültigen Sperre der besagten persönlichen Waffe (1) enthalten können, wobei die besagte Kontrollvorrichtung (2) zur Interpretierung der besagten Befehle und/oder ihre Weiterleitung an die Waffe (1) dient.

20. Kontrollvorrichtung (2) gemäss einem der vorherigen Ansprüche, wobei das besagte Mobilfunktelekommunikationsnetzwerk (7) ein zellulares Mobiltelefonnetzwerk ist.

21. Persönliche Waffe (1), die eine Kontrollvorrichtung (2) gemäss einem der vorherigen Ansprüche zu ihrem Fernkontrollieren umfasst.

22. Zentrale Datenbank zur Speicherung von Informationen, welche durch mindestens eine Kontrollvorrichtung (2) gemäss einem der Ansprüche 1 bis 20 in Datenmeldungen über das besagte Telekommunikationsnetzwerk (7) gesendet wurden.

23. Verfahren zum Fernkontrollieren der Benutzung einer persönlichen Waffe (1), mit folgenden Schritten:

    Ermittlung von einem Ereignis aus einer persönlichen Waffe (1) durch einen Detektor (4) in einer Kontrollvorrichtung (2) gemäss einem der Ansprüche 1 bis 20,
    Bearbeitung eines Signals aus dem besagten Detektor (4) durch Datenverarbeitungsmittel (5) in der besagten Kontrollvorrichtung (2),
    Vorbereitung einer Datenmeldung mit im besagten Signal enthaltenen Informationen,
    Senden der besagten Meldung über ein Telekommunikationsnetzwerk (7).

24. Verfahren gemäss dem vorherigen Anspruch, wobei die besagte Datenmeldung in der besagten Kontrollvorrichtung (2) vor dem besagten Senden gespeichert wird.

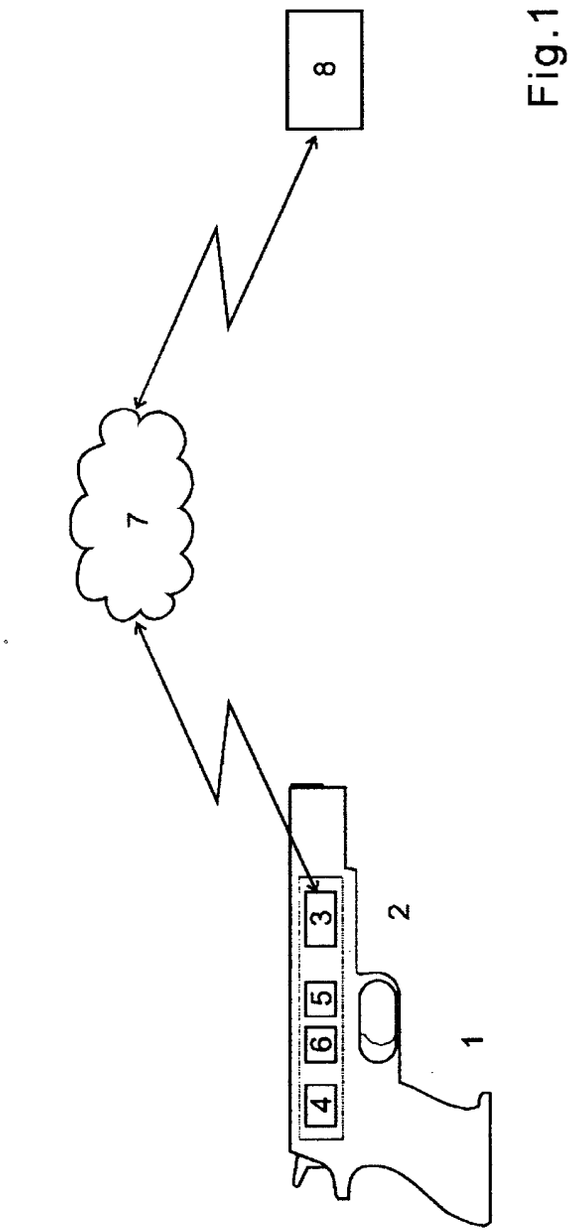

Fig.1

Europäisches Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung
EP 04 10 2570

EINSCHLÄGIGE DOKUMENTE

Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
X	WO 01/84069 A (DELSY ELECTRONIC COMPONENTS AG ; POEHS HANS JUERGEN (DE)) 8. November 2001 (2001-11-08) * Seite 10, Absatz 4 - Seite 12, Absatz 3 * * Seite 13, Absatz 5 - Seite 14, Absatz 1 * * Seite 43, Absatz 3 * * Seite 77, Absatz 4 - Seite 78, Absatz 4 * * Seite 91, Absatz 3 - Seite 92, Absatz 1 * * Anspruch 11; Abbildungen 1A,2A,3A,4A,5A,6A,7A *	1-16,18, 20-24	F41A17/06
Y	& DE 200 13 901 U (DELSY ELECTRONIC COMPONENTS AG) 7. Juni 2001 (2001-06-07)	17,19	

X	US 2004/099134 A1 (GOTFRIED BRADLEY L) 27. Mai 2004 (2004-05-27) * Absätze [0014] - [0017], [0019], [0025], [0027], [0032], [0035], [0044] * * Abbildungen *	1,2	RECHERCHIERTE SACHGEBIETE (Int.Cl.7) F41A F41C
Y		19	
A		3-18, 20-24	

Y	WO 01/79777 A (BROSOW JOERGEN ; INFINEON TECHNOLOGIES AG (DE)) 25. Oktober 2001 (2001-10-25) * Absätze [0016] - [0018], [0035], [0036] *	17	

Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt

Recherchenort	Abschlußdatum der Recherche	Prüfer
Den Haag	12. Oktober 2004	Gex-Collet, A-L

KATEGORIE DER GENANNTEN DOKUMENTE

X : von besonderer Bedeutung allein betrachtet
Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie
A : technologischer Hintergrund
O : nichtschriftliche Offenbarung
P : Zwischenliteratur

T : der Erfindung zugrunde liegende Theorien oder Grundsätze
E : älteres Patentdokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht worden ist
D : in der Anmeldung angeführtes Dokument
L : aus anderen Gründen angeführtes Dokument

& : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument

EPO FORM 1503 03.82 (P04C03)

ANHANG ZUM EUROPÄISCHEN RECHERCHENBERICHT ÜBER DIE EUROPÄISCHE PATENTANMELDUNG NR. EP 04 10 2570

In diesem Anhang sind die Mitglieder der Patentfamilien der im obengenannten europäischen Recherchenbericht angeführten Patentdokumente angegeben.
Die Angaben über die Familienmitglieder entsprechen dem Stand der Datei des Europäischen Patentamts am
Diese Angaben dienen nur zur Unterrichtung und erfolgen ohne Gewähr.

12-10-2004

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 0184069 A	08-11-2001	DE 20013901 U1	07-06-2001
		AU 6387701 A	12-11-2001
		WO 0184069 A1	08-11-2001
DE 20013901 U	07-06-2001	DE 10002767 A1	26-07-2001
		DE 20013901 U1	07-06-2001
		AU 6387701 A	12-11-2001
		WO 0184069 A1	08-11-2001
		AU 2680601 A	31-07-2001
		DE 10190171 D2	30-04-2003
		WO 0154051 A2	26-07-2001
US 2004099134 A1	27-05-2004	KEINE	
WO 0179777 A	25-10-2001	DE 10018369 A1	25-10-2001
		AU 6385401 A	30-10-2001
		BR 0110076 A	31-12-2002
		CN 1436294 T	13-08-2003
		WO 0179777 A1	25-10-2001
		EP 1274965 A1	15-01-2003
		JP 2003535297 T	25-11-2003
		US 2003097776 A1	29-05-2003

EPO FORM P0461

Für nähere Einzelheiten zu diesem Anhang : siehe Amtsblatt des Europäischen Patentamts, Nr.12/82