

發明專利說明書

(本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫)

※申請案號：94137863

※申請日期：94.10.28

※IPC分類：G06F 17/40 (2006.01)

一、發明名稱：(中文/英文)

機器人資料安全更新之系統及其方法

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

微星科技股份有限公司

MICRO-STAR INT'L CO., LTD.

代表人：(中文/英文)

徐祥

/ HSU, JOSEPH

住居所或營業所地址：(中文/英文)

台北縣中和市立德街六十九號

No. 69, Li-De St., Jung-He City, Taipei, Taiwan, R.O.C.

國籍：(中文/英文)

中華民國 / Taiwan, R.O.C.

三、發明人 (共 2 人)

姓名：(中文/英文)

洪士哲 / HUNG, SHIH CHE

黎永昇 / LI, YUNG SHENG

國籍：(中文/英文)

中華民國 / Taiwan, R.O.C.

中華民國 / Taiwan, R.O.C.

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係為一種機器人資料安全更新之系統及其方法，特別係在控制裝置與機器人間可安全進行操作機器人及更新韌體之系統及其方法。

【先前技術】

工業機器人自從 1970 年代引入市場，目前已是自動化製造不可或缺的生產工具。以往機器人的應用範疇多半侷限於航太、海洋、軍事、醫療或工業上，近年由於微電子與資訊科技的快速進步，機器人也由原本的高科技領域轉向朝擬人化資訊家電發展。

這些能站立、行走並做許多擬人化動作的機器人，雖然依據目前之開發進度所能執行的功能仍然非常有限，但是其內部構造，不論在軟、硬體方面皆需要很精密的計算才能達成，其中在硬體平台上，包括有：電子控制系統、電力控制系統、馬達控制系統、影音處理系統、及網路處理系統…等等；而在要搭配的軟體模組，除了原先用以驅動硬體所需的各種驅動程式外，還包括：影像處理模組、聲音處理模組、運動控制模組、及聯網控制模組…等等功能程式。

由於整個機器人系統在開發時程上往往拉的很長，因此雖然產品只有完成了基本之雛形，但為了在市場上搶得先機，

以及打下市場佔有率，甚至為了提昇產品之知名度，尤其是在機器人這種高單價之產品上更需如此，所以，產品在後續仍然會需要不斷的進行更新，特別是在韌體的更新上。

過去在韌體的更新上，往往需要將機器人送回到原廠或者是經銷商及服務站，由熟悉機器人之工程師進行更新，這對使用者而言極為不便，另一種方式便是將更新檔案透過網路下載，在藉由電腦端上執行更新程式以進行安裝，但是這樣仍然會面臨手邊沒有電腦的情形發生，而無法立即利用遠端維修服務之功能來進行更新動作；再者，由於機器人的單價就目前來說仍是相當昂貴，如何避免機器人因為韌體被惡意破壞造成使用者之損失，以及保障合法使用者能夠獲得最新韌體之更新，更要避免機器人被偷竊及盜取後即完全歸盜取者所用，實為一重要之課題。

【發明內容】

鑒於以上的問題，本發明的主要目的在於提供一種機器人資料安全更新之系統及其方法，藉以於機器人與控制裝置間各加入一認證模組，當兩者間有資料要傳輸時，皆須先比對認證資料無誤後，才可允許兩者互相傳送資料、及命令，增加機器人在使用上之安全性，防止被他人竊取盜用，以及任意修改內部之韌體資料。

因此，為達上述目的，本發明所揭露之一種機器人資料安

全更新之系統，於機器人端至少必須包含：

第一連接模組，用以與控制裝置端建立連線，並用以接收及傳送資料；第一認證模組，對應有一認證資料，用以比對控制裝置之認證資料是否正確；儲存裝置，用以儲存傳入之更新資料；設定模組，用以接收使用者輸入之操作指令，以及依據更新資料進行韌體之安裝；及控制模組，用以根據接收到合法之命令進行控制機器人之動作。

而於控制裝置端至少必須包含：

第二連接模組，用以與機器人端及服務網站伺服器建立連線，並用以接收及傳送資料；第二認證模組，用以儲存認證資料並比對機器人之認證資料是否正確；及輸入模組，用以接收使用者所輸入之任一操作命令。

依據本發明之目的且達到上述之優點，本發明用於控制裝置上下載更新韌體資料之方法，包含下列步驟：

首先，請求與機器人之服務網站伺服器建立連線，然後，提交第二認證模組之資料進行認證；接著，確認認證資料是否合法？當認證通過時，進一步接收可進行安裝更新之韌體資料；最後，當下載完成後，則中斷與服務網站伺服器之連線。

在本發明之另一實施例中，還提供控制裝置安全操控機器人之方法，包含下列步驟：

一開始請求與機器人建立連線，然後，提交第二認證模組

之資料進行認證，再來，確認認證資料是否正確？當認證通過時，即可進行傳送每一使用者輸入之指令。

而在機器人與控制裝置進行資料傳送之方法，包含了以下步驟：

首先，接收控制裝置所傳來之連線要求，然後，比對認證資料是否正確？確認無誤後，即可接收可進行更新之韌體資料；再來，依據所接收之韌體資料安裝設定來進行內部對應功能之資料更新；最後，將更新後之韌體資料儲存。

本發明還揭露一種同步變更機器人與控制裝置兩者之認證資料之方法，包含下列步驟：

建立兩者之間之連線並達成資料之同步；執行變更認證資料之設定；要求再次輸入先前之第一認證資料；確認無誤後，接收新輸入之第二認證資料；及同步更新機器人及控制裝置之認證資料。

有關本發明的特徵與實作，茲配合圖示作最佳實施例詳細說明如下。

【實施方式】

本發明將揭露一種機器人資料安全更新之系統及其方法。在本發明的以下詳細說明中，將描述多種特定的細節以便提供本發明的完整說明。然而，對熟知技藝者來說，並可以不需要使用該等特定細節便可以實施本發明，或者可以藉著利用

替代的元件或方法來實施本發明。在其他的狀況下，並不特別詳細地說明已知的方法、程序、部件、以及電路，以免不必要地混淆本發明的重點。

請參照「第 1 圖」，此為本發明實施方式之示意圖，機器人 10 可以透過纜線 30 與電腦 230 相連接，使用者可於電腦 230 上進行設定機器人之功能函數，也可由電腦 230 透過網際網路 50 連接至機器人 10 之服務網站伺服器 40，下載最新版本之韌體進行更新；此外，也可透過無線網路(如：802.11x、802.16x…等等)或者是以藍芽傳輸方式自具輸入介面之可攜式裝置 220 進行操控，例如：個人數位助理(PDA, Personal Digital Assistant)、筆記型電腦、或是機器人 10 之專屬搖桿…等等，若是使用者在較長距離之遠端，例如人在國外，則可由手持式行動通訊裝置 210，例如各種通訊規格之手機，在當地以整體封包無線電服務(GPRS, General Packet Radio Service)或是 3G(如：WCDMA、CDMA2000)將操作命令傳至機器人 10 端，機器人 10 仍可依據接收到之命令執行對應之動作。

為達到此一目的，本發明所揭露之機器人 10 與控制裝置 20 兩端之內部架構示意圖，如「第 2 圖」所示，包含了：第一連接模組 110，用以接收控制裝置 20 端傳來之要求並建立連線，當連線建立完成後，可接收及傳送資料，為達成此功能本模組可以為有線之連接方式，例如透過專屬之纜線(cable)，

或具備了通用串列匯流排(USB, Universal Serials Bus)、IEEE1394、RS-232 之乙太網路介面，或者是網路線(RJ-232)；也可以是無線傳輸方式，例如：紅外線(IrDA, Infrared Data Association)、藍芽(blue-tooth)、802.11x、802.16x、以及射頻收送裝置。

當連線完成後，為避免未經授權之資料傳入，進而破壞機器人 10 內部之軟體資料，故當有命令或資料欲傳入機器人 10 時，不論是進行儲存或是執行之動作，皆須先經由第一認證模組 100 先行比對認證碼(Access Right)，其中該認證碼可以是一組分別內置於機器人 10 端及控制裝置 20 端之晶片，於服務網站伺服器 40 亦儲存一份相同之認證資料，經由兩晶片之私密金鑰配對，判斷是否符合其內部設定之認證規則，或是亦可為一組可供使用者進行設定及更改之密碼(password)，當輸入之密碼無誤才允許外部對機器人 10 進行操控及資料之寫入。

控制裝置 20 則在第一認證模組 100 比對認證碼通過後，負責執行所接收之命令或是資料，例如：執行機器人 10 之移動，當接收到之資料為更新軟體時，則是將該軟體存放到儲存裝置 140，並由設定模組 120 進行更新及安裝，若使用者輸入之命令為變更機器人 10 之認證密碼時，則由設定模組 120 確認原本之認證資料輸入無誤後，再要求輸入更新認證資料，經由二次確認無誤後，即可將更新後之認證資料，例如可為另一

使用者之指紋、聲音或密碼存入儲存裝置 140 內，並加入第一認證模組 100 之認證設定之中，同時將服務網站伺服器 40 內原先儲存之認證資料同步變更。

因此，同樣的在控制裝置 20 端必須包含一輸入模組 170，用以接收使用者所輸入之命令，例如欲使機器人 10 進行移動，或者是連接至網路上下載更新之韌體，對機器人 10 內部設定參數之修改包括認證資料之修改…等等，其中控制裝置 20 可為第 1 圖中之手持式行動通訊裝置 210、可攜式裝置 220 及電腦 230，而第二連接模組 160 便是用以傳送使用者所輸入之資料及命令到機器人 10 端，或者是接收至網際網路 50 上所接收之更新資料，其可能進行連接之方式與第一連接模組 110 相同，在此便不再贅述。

第二認證模組 150 亦與第一認證模組 100 同樣均包含一認證碼，當第二連接模組 160 與第一連接模組 110 建立連接時，第一認證模組 100 便會要求比對第二認證模組 150 之認證碼是否配對成功，確認認證碼配對無誤後才由第二連接模組 160 進行更新資料，及使用者所輸入命令之傳送，而認證碼之確認也可使用於手持式行動通訊裝置 210、可攜式裝置 220 及電腦 230 三者之間的資料傳輸；當使用者欲更改機器人 10 之第一認證模組 100 內之認證碼時，必須同步變更至少一控制裝置 20 之第二認證模組 150 之認證碼。

請參照「第 3 圖」，此為控制裝置 20 下載更新韌體資料之方法流程圖。當使用者自輸入模組 170 設定連接與機器人 10 之服務網站伺服器 40 時，第二連接模組 160 便請求與機器人 10 之服務網站伺服器 40 建立連線(步驟 310)，偵測是否有更新之韌體資料，當有較新之韌體可供下載時，提交第二認證模組 150 之資料進行認證(步驟 320)；接著，服務網站伺服器 40 便會確認控制裝置 20 所傳認證資料是否合法(步驟 330)？當認證資料可以被服務網站伺服器 40 所接受時，則控制裝置 20 可再由第二連接模組 160 接收可在機器人 10 上進行安裝更新之韌體資料(步驟 340)並儲存。最後，當更新之韌體資料下載完成後，則中斷與服務網站伺服器 40 之連線(步驟 350)。

接著，便可連接機器人 10 請求進行韌體資料之更新，如「第 4 圖」所示，此為控制裝置 20 傳送命令之機器人 10 端之方法流程圖，首先第二連接模組 160 便請求與機器人 10 之第一連接模組 110 建立連線(步驟 410)，當該連線之請求傳至第一認證模組 100 時，第一認證模組 100 便要求檢查認證資料，以確認所欲傳來之資料或命令為合法，而控制裝置 20 便將第二認證模組 150 之認證資料傳至機器人 10 端進行認證(步驟 420)；第一認證模組 100 便可比對控制裝置 20 之認證資料是否正確(步驟 430)？當控制裝置 20 被認證通過後，即可傳送使用者所輸入欲進行韌體資料更新之操作指令(步驟 440)，進行

後續機器人之韌體資料更新。

所以，請參照「第 5 圖」，此為機器人 10 進行韌體資料更新之方法流程圖，同樣的，第一連接模組 110 會接收到第二連接模組 160 所傳來建立連線之請求(步驟 510)；接著，第一認證模組 100 便可比對控制裝置 20 之認證資料是否正確(步驟 520)？當第二認證模組 150 之認證資料經確認無誤後，即可接收用以進行機器人 10 更新之韌體資料(步驟 530)。接收完成後，設定模組 120 便會依據所接收之韌體資料安裝設定，來進行機器人 10 內部對應功能之資料更新(步驟 540)；最後，控制模組 130 便可將更新後之韌體資料儲存到儲存裝置 140 中(步驟 550)。

請參照「第 6 圖」，此為變更機器人 10 與諸多控制裝置 20 間之認證資料之方法流程圖。當使用者選擇變更機器人 10 之認證資料設定時，首先必須建立與控制裝置 20 端兩者之間之連線，並達成資料之同步(步驟 610)，達成兩者在資料變更時可以一致；接著設定模組 120 執行變更認證資料之設定(步驟 620)；先要求使用者再次輸入先前之第一認證資料(步驟 630)，上述之比對認證資料之動作皆為第一認證模組 100 與第二認證模組 150 間自動執行，而使用者只要使用合法之控制裝置 20 皆可控制機器人 10，並不需確認使用者是否真的知道認證碼，但萬一不知道認證碼之非法使用者也可輕易修改認證