

(此處由本局於收
文時黏貼條碼)

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：94125156

※申請日期：94 年 07 月 25 日

※IPC 分類：605B 9/01, 1/01 (2006.01)

一、發明名稱：

(2006.01)

(中) 智慧控制器方法及裝置之安全切換

(英) Failsafe switching of intelligent controller method and device

二、申請人：(共 1 人)

1. 姓 名：(中) MK S 儀器股份有限公司

(英) MKS INSTRUMENTS, INC.

代表人：(中) 1. 羅伯 克林

(英) 1. KLIMM, ROBER

地 址：(中) 美國麻薩諸塞州威明頓工業路九〇號

(英) 90 Industrial Way, Wilmington, MA 01887, U.S.A.

國籍：(中英) 美國 U.S.A.

三、發明人：(共 4 人)

1. 姓 名：(中) 尼道爾 卡利

(英) KHALIL, NIDAL

國 籍：(中) 美國

(英) U.S.A.

2. 姓 名：(中) 剛特 席夫那茲契

(英) SIFNATSCH, GUENTER

國 籍：(中) 德國

(英) GERMANY

3. 姓 名：(中) 伍茲 雷夫 阿密

(英) LEV AMI, UZI

國 籍：(中) 以色列

(英) ISRAEL

4. 姓 名：(中) 榮恩 海達

(英) HADAR, RON

國 籍：(中) 以色列

(英) ISRAEL

四、聲明事項：◎本案申請前已向下列國家（地區）申請專利 ☐ 主張國際優先權：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1. 美國 ; 2004/07/27 ; 60/591,286 ☒ 有主張優先權
2. 美國 ; 2004/09/23 ; 10/948,085 ☒ 有主張優先權

(英) ISRAEL

四、聲明事項：◎本案申請前已向下列國家（地區）申請專利 ☐ 主張國際優先權：

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1. 美國 ; 2004/07/27 ; 60/591,286 ☒ 有主張優先權
2. 美國 ; 2004/09/23 ; 10/948,085 ☒ 有主張優先權

(1)

九、發明說明

【發明所屬之技術領域】

本發明係關於導入於控制器主機（或第一裝置）及工具（或第二裝置）之間之控制器組件的安全操作。尤其，本發明係關於在媒介第一及第二裝置間的資料轉移之控制器的失效之後，建立第一及第二裝置間之直接連接。一個可利用本發明之環境係具有主機及工具/感測器之半導體製造廠，智慧控制器被加入於主機及工具/感測器之間以使用控制器來媒介工具、與工具相關聯的感測器及資料使用者間之通信，諸如主機系統或分佈型處理器。

【先前技術】

摩爾定律（Moore's law）在縮減價格下允許電腦能力的指數成長。處理能力的強力成長可導引一個人想到此半導體裝置製造將是冒險性事業，如同投機的石油業。事實剛好相反。因為製造批量係非常昂貴且製造過程對於甚至小錯誤係敏感，半導體裝置製造係保守的事業。新設備的驗證循環及標準與老設備的改良係漫長且苛求的。甚至小的改變在釋出生產之前要廣泛地檢查。

由半導體製造所使用之主要組件包括工具（例如，沉積室、反應器）、監視此工具之感測器（例如，FTIR 感測器、質譜儀、熱電偶）、及儲存及分析來自感測器有關工具操作的資料之主機或分佈型處理器。

一習知案說明收聽來自感測器的資料以及使用諸如

(2)

TCP/IP 的高速且防誤技術在乙太網路上將此資料提供給主機或分佈型處理器的透通方法。此習知案（案名 "Method and Apparatus for monitoring Host to Tool Communications"，申請案號 U.S. 09/935213）係由發明人 Uzi Lev-Ami 及 Yossf Ilan Reich 在 2001 年八月提出，此案在本文中併入參考。習知案說明一收聽柱（post），其可使用光學隔絕的連接器來竊聽來自工具或感測器之串列通信。使用此竊聽方法，使用者可證明 Fab 側通信及資料收集次結構可在低風險下升級而無需工具或感測器的修改。升級可行性可無需拆除憑依的通信次結構而實施。

Fab 側儀器及支援端分析能力的下一解決方法將包含增加智慧控制器，以媒介控制器的一側上的工具及感測器與另一側之工具主機或分佈的處理器間之連通，無需更換或改變感測器的分析特徵。處理器能力的增大及儲存成本的減少產生先前已不再使用於 Fab 側環境的架構之機會。

發明人 Uzi Lev-Ami，Guenter Sifnatsch 及 Mark Attwood 的第二習知案，案名 "Controller and Method to Mediate Data Collection from Smart Sensors for Fab Applications"，2004 年四月 7 日申請案號 U.S.10/819903，說明具有各種能力之智慧控制器。

現在有機會來補充智慧控制器或任何其它網路附加裝置的分析特性，如果中間裝置失效或停機，此網路附加裝置媒介能夠與直接連結兩其它裝置的安全開關直接連通的兩個其它裝置間之連通。較佳地，中間裝置的更可靠且信

(3)

心激勵安裝可實現。

【發明內容】

本發明係關於與工具相關聯的感測器的控制及來自工具相關聯的感測器之資料收集。尤其，本發明關於使用控制器來媒介工具、與工具相關聯之感測器及資料使用者間之通信，諸如主機系統或分佈型處理器。本發明的特別形態係說明於申請專利範圍、說明書及圖式。

【實施方式】

以下詳細說明係參考圖式而製作。較佳實施例被說明來解說本發明，不是用來限制其範圍，此範圍係由請求項所界定。熟習此項技藝者將認知到各種在以下說明上之等效變化。

引言

當通信及處理器加速時，數年前發展的半導體製造廠及鑄造廠的工具及其它自動化或半自動化設備所使用之 SECS 訊息協定、通信次結構及主機模式係相對地受限。用於製造應用之 SECS 訊息協定係設計來利用低速串列通信。這些訊息協定包括結構性訊息，其甚至可以低速通信快速地傳輸。結構性訊息過去是且現在仍難以翻譯及瞭解。當第一訊息設定回應用之上下文時，此困難加中，且，第二回應訊息不會重複此上下文；亦即，上下文有關回應

(4)

僅在與對應的上下文設定訊息成對時才有意義。通信通常係沿著相似用於終端機及分時電腦的數據機及電話線之專用通路而經由 RS232 或等效串列連通。主機系統運轉在主機架、迷你電腦或工作站。主機系統通常係單片的，其控制且監視製造中之所有或一實質組的工具。主機系統依賴轉接器而與工具及感測器形成介面。主機系統通常接收來自工具及感測器之資料，且發出控制指令給工具。主機系統經常接收且產生顯著容量的串列通信訊息。

用辭"工具主機"係使用於廣意上，其包括工具控制主機及更限制或彈性分佈的處理器兩者。工具主機包括具有綜合性整體工具控制功能的主機及運轉在分佈的處理器上具有更限制的任務特定功能的主機兩者。工具主機包括諸如 Consilium 的 FAB300 (TM) 軟體之產品，此產品被說明為提供由顧客特定商業過程的中央化定義所驅動之單綜合性工廠管理系統。

工具主機的目錄係設計來取代傳統製造執行系統，此系統係設計來控制由不同賣主所提供之工具。在來自傳統製造執行系統之工具主機頻譜的相對端，組件處理可被運轉在分佈的處理器上以處理各種特定功能，而不需請求為綜合性管理系統。沿著此頻譜，諸如 Consilium 的 FAB300 (TM) 軟體之產品可被考量為用於某些目的之工具控制主機及運轉在分佈的處理器上用於其它目的之處理。

於以上所引用的應用中，說明可監視在一或更多工具

(5)

主機及一或更多工具間之有線通信通路之可移除收聽裝置。收聽裝置係被動的。收聽裝置可選擇性地包括標準隔絕裝置，其保護通信通路免受由此收聽裝置所產生之雜訊。此隔絕裝置可包括光學隔絕器、光阻抗放大器、或使有線通信通路與收聽裝置有效隔絕之任何其它組件。有線通信通路可以是 RS232、RS422 或 CAN-順應通路，或如果可以是前述之通信通路的任一者。

控制器及聰明感測器

揭示於另一習知應用使用智慧控制器及聰明上下文認識感測器之處理。智慧控制器認識到工具的狀態及/或工具處理的工作件（例如，晶圓或光罩）。這些類型的控制器與對工具及工作件狀態資訊反應之聰明感測器連通。取代依賴作為工具及工作件狀態改變的重構指令而定，感測器收聽且回應狀態改變。取代需要辨識指令，它們以預編程方式對狀態改變之反應。

新的智慧控制器改變用於工具、感測器、控制器及資料使用者之操作模型。控制器認識到工具及工作件狀態的其中一者。控制器可竊聽或中繼控制工具的指令。替代地，工具可公開其狀態給控制器。或者，控制器可查詢關於工具的狀態，週期性地或回應當需要進一步查詢時之辨識的事件。控制器將狀態資訊給感測器而傳輸。狀態資訊可關於工具及工作件。感測器被預構以回應狀態資訊。為回應此狀態資訊，感測器可採用資料收集計劃，自動效準，

(6)

設定輸出範圍，或關聯具有目前狀態資訊之資料。控制器將收集自感測器的資料而傳輸至資料使用者。資料使用者可以是運轉在主機架上的傳統工具主機，或可以是運轉在分佈的處理器上之更新軟體。資料使用者可以是單片的系統，或者獨立或合作操作的聯合封裝。控制器亦可監視來自感測器的資料，辨識利益的事件，以及，請求已經收集的進一步資料或改變用於感測器的收集計劃以回應所監視的資料。

各種操作環境

圖 1 解說本發明的形態係特別有用之環境。此解說處理室 125、各種對處理室的輸入及自處理室的輸出、正感測器、控制通路及控制器。室 125 可被使用於各種反應，諸如沉積、清洗、蝕刻、植入、灰化等。其它類型工具，未被此圖式解說，亦可收益自本發明的形態。

Fab 網路 111，可能經由網際網路而接達，虛擬專用網路或廣域網路 112 具有經由控制器、防火牆或其它連接器 162 對工具網路路 112 之控制接達。此圖式中的工具網路路係顯示連接撞擊處理室 125 之控制器及感測器成環狀。熟習此項技藝者將瞭解到，此架構僅係解說用；串列通路、以太網路（Ethernet）或分級通路比環狀網路更可能使用於 Fab 網路。

對處理室 125 的氣態輸入包括通過氣體盒壓力轉換器 113 及質量流控制器（MFC）114 之氣體。某些氣體可通

(7)

過臭氧產生器 133。其它氣體及氣體混合物可通過反應氣體產生器 115 及氣體成份監視器 117。反應氣體產生器 115 可在處理室 125 內側或外側產生電漿。氣體成份監視器 117 可與反應氣體產生器串聯或並聯。質量流控制器 114 係與反應氣體產生器 115 及氣體成份監視器 117 而氣體連通，且，最後或直接與處理室 125 氣體連通。氣態輸入裝置 113、114、133、115 及 117 係與一或更多數位控制器 142、室控制器 152 及連接點 162 而連通。此連通通常包括控制及遙測兩者。這些裝置可包括回應給裝置的操作或氣態輸入及/或輸出之控制及感測器兩者。

其它輸入可包括：材料輸送 134、冷卻次系統 145 及各種動力注入器 153、154 及 155。反應室 125 可以是沉積室、蝕刻器、熱處理器或其它類型的反應器。依據反應室的類型而定，材料輸送系統 134 可供應例如用於沉積在工作件 136 上之材料。當大部份化學反應將進行在溫度敏感的速率時，冷卻次系統 145 可幫助調整室 125 內之溫度。供應至此室之動力可包括：微瓦動力 153、使用來產生電漿之 RF 動力 154、及使用來產生電漿及加熱此室或供應至此室之氣體或其它材料之 DC 動力 155。另一輸入，如同氣態輸入，係與一或更多數位控制器 142、室控制器 152 及連接點 162 而連通。此連通類型包括控制及遙測兩者。這些裝置可包括回應控制裝置的操作或感應它們的輸入及/或輸出之控制及感測器兩者。

感測器可回應室狀態或作用在來自此室之排氣上。回

(8)

應室狀態之感測器可包括：晶圓監視器 116，其經由視窗 126 深入室 125 以觀察膜厚度、圖案及其它特性（例如，EPI-Online (TM)）；處理監視器 127，諸如具有干涉濾光片或干涉儀之發光監視器，用於蝕刻處理控制；及壓力轉換器 137。作用在來自此室 125 的排氣上之感測器包括：檢漏器 146、真空計 157 及排氣監視器 158。這些感測器可與壓力控制器 148 及控制閥 147 以及與真空組件及/或次系統 156 而相互作用。它們亦可與泵及/或排氣洗滌器（未顯示）相互作用。這些感測器與一或更多數位控制器 142、室控制器 152 及連接點 162 而連通。此連通通常包括控制及遙測兩者。例如，與感測器 147、148 及 156 連通之裝置可包括控制及感測器兩者。

於圖 1 中未解說，安全開關可應用在每當中間裝置插入於第一裝置或諸如 Fab 側網路之網路與第二裝置或諸如工具網路路之網路之間時，此兩裝置或網路可相互連通而無需中間裝置。收集來自工具或感測器的讀數、儲存這些讀數並使其在要求時之控制器可被取得。補充可自感測器取得的資料之控制器係另一實例。將資料自一格式（例如，SECS）轉換成另一格式（例如，標記 XML 格式）之控制器為另一者。熟習此項技藝者將認識到其它情況，其中中間裝置的故障可藉由第一及第二裝置或網路的安全直接連接而提出。

控制器發展及架構

(9)

圖 2 係與工具、感測器及工具主機連通之控制器的區塊圖。此區塊圖可同樣地僅藉由識別作為第一裝置的主機 211、作為第二裝置之感測器 227 或儀器 237、及作為中間裝置之控制器 200 而普及化。於所述的實施例中，控制器 200 構造包括：兩個 SEC/GEM 介面埠 212、216 及兩個網路介面埠 232、236。控制器包括邏輯及資源以經由包括 SECS MUX215 之 SECS 協定而連通。控制器另包括實施與資料使用者連通的 Fab 側介面 234 及與工具、感測器及儀器連通的工具側介面 235 之邏輯及資源。SECS MUX215 及介面 234、235 係邏輯地連接至資料收集及公開資源 225。在控制器的 Fab 側上，傳統工具主機 211 可經由 SECS 順應通信通路、SECS-I、HSMS 或 SECS 的修改版本或後繼版本而連接 SEC/GEM 介面埠 212。於可應用本發明之非製造環境中，其它協定可被使用來與正被監視的工具而連接，諸如醫學工具或數字控制的機械工具。控制器可經由不同於藉由網路 222 載入至儲存 231 及報告 221 資源的 SECS 之 Fab 側協定而連接。在控制器 200 的工具及感測器側上，對工具或工具群集之 SEC/GEM 介面 217 可被連接 SEC/GEM 介面埠 216。控制器亦可連接網路介面埠 236 至網路 226，網路 226 主持感測器 227、儀器 237 及可能包括工具 217 之其它裝置。雖然此圖解說經由網路而連接至感測器之控制器，控制器可替代地使用 SECS-I 或另一串列基協定而與感測器連接。

圖 3 係使用單型的通信通路而與工具、感測器及工具

(10)

主機連通之控制器的區塊圖。圖 4 解說使用多型的通信通路。於圖 3 中，SECS 支配的情況被解說。控制器 303 使用 SECS 協定 307、309 而與工具 301 及感測器 302 兩者連通。工具 301 及感測器 302 間之連接 308 可包括任一類型的正常感應的能量或力，包括圖 1 的說明中所辨識之感應的任一者。於圖 4 中，SECS 及網路通信的更複雜組合被角說。獨特的 SECS 通信通路 307 於此情況係位於控制器 303 及主機 301 之間。工具側網路 409 使控制器與感測器 302A-B、管理開關 413 及網路附加儲存（NAS）415 而連接。Fab 側網路 419 使控制器 303 與諸如傳統工具主機或分佈的處理器之分析軟體 423、諸如網際網路、VPN 或專用的內部網路之延伸網路 425、及持續或儲存由控制器所公開的資料之資料庫 427。替代地，資料庫 427 可留在控制器 303 上。

安全開關對網路之導入

圖 5 係增加安全開關至圖 3 所述的網路的區塊圖。兩個新組件被介紹，旁通開關 511 及插孔或開關 512。於許多架構中，僅旁通開關 511 將是新的。網路的此配置假設係經由網路協定而與工具連通。如果工具尚未使用網路協定時，此通信協定可由導入協定轉換器在插孔或開關 512 及工具 501 間而配置。替代地，兩個通信通路可由旁通開關 511 而控制，例如，承載 SECS 通信之串列連接及載入其它通信之乙太網路連接，如圖 3 所示，控制器 303 於正

(11)

常操作模式與工具 301 及感測器 302 兩者而連通。感測器係連結至工具以量測或記錄工具狀態或性能的某些形態。來自工具網路或主機 304 之訊息係經由旁通開關 511 而傳送至控制器 303，且，自控制器背部經由旁通開關傳送至插孔或開關 512。插孔或切換係與裝置互連之習知網路組件。控制器 303 包括至少兩個網路介面 521、522。這些介面係經由與工具網路 304 及工具 301 或感測器 302 連通之旁通開關 511 而有效地連結。控制器 303 及旁通開關 511 間之額外連接 523 承載心跳，或其它使保持旁通開關於正常（非安全）模式的信號而保持有電流，如以下所述。於此圖中，兩個操作模式被解說，以實線標示的 controllers 的正常操作，及以虛線標示的旁通操作。雖然通過旁通開關之兩個連接出現於此圖中，這些連接可以是在單線或連接上的操作的邏輯模式，不必要是一對旁通開關 511 及工具網路 304 或插孔或開關 512 間之連接。再者，旁通開關可控制超過一個的連接。

圖 6 係增加安全開關至網路於圖 4 所述之區塊圖。於此圖中，由工具側網路 409 連接至旁通開關 511 之插孔或切換通常係由自旁通開關至工具 301 及感測器 302A-B 的多點網路連接所隱含。旁通開關及控制器間之三個連接出現於此圖中，如前所述。

回到圖 5，解說安全開關的操作的一實施例。於控制器故障的例子中，為方便控制器不再作為無需中間控制器可連通的兩個裝置間之有用角色，連接性直接建立於裝置

(12)

之間，例如主機 304 及工具 301。於一實施例中，具有簡單嵌入的微控制器之切換被使用。Shore Micro 提供至少一作用之開關。此開關當切換時產生可靠的"點選"之繼電器。開關中的微控制器經由諸如串聯、並聯、USB、韌體、Ethernet 或其它之連接 523 而收聽來自控制器之心跳 (heartbeat) 信號。依據設在安全開關之邏輯及資源而定，除了心跳外的其它協定可被使用。例如，安全開關可對控制器作週期性地查詢，且回應誤差狀態指示會回應超時。這些查詢對於高通信量、低通信量及/或利益的其它操作狀態的某些程度可以是規則或適合的。微控制器-控制的切換類似於雙極雙投開關，其將控制器 303 分成具有主機 304 的電路或分出自主機 304。於正常模式中，控制器係物理地連接於電路。於安全模式中，主機及工具/感測器係直接連接的。替代的，電子切換可被利用，其放棄繼電器的可靠點選。

實施心跳及安全連接之軟體可包括設定封裝位址之裝置驅動器、用於捕捉當網路介面運轉於雜亂模式時的封裝之核心鉤、監視預設程式 (watch dog daemon)、及使用者空間程式。以下說明係 Linux 導向 (oriented)。其它操作系統可被使用，諸如 BSD 版本、Unix 版本或 Windows。系統可被寫入以運轉在虛擬器上，諸如即時版本的 Java，以使僅對軟體的小變化，以控制低階層網路化功能，需要將軟體自一操作系統轉移至另一操作系統。

裝置驅動器將掛鉤至 TCP/IP 堆疊且使控制器顯而易

(13)

見，猶如控制器未被連接。藉由改變訊息包中之來源位址及資訊，呈現出猶如它們來自工具或主機，而取代中間控制器。裝置驅動器將來自使用者空間的資料複製至核心空間的 TCP/IP 掛鉤。

控制器可藉由自一網路介面橋接至另一網路介面而操作未提出至 HSMS 埠之選擇的訊息包，無需由控制器處理這些訊息包。例如，脈衝信號（ping）或 ICMP 訊息包可被通過，無需由控制器處理。此選擇性地橋接可被輸入至訊息包類型及/或埠。

核心鉤係數行的碼，其保存至少某些當網路介面運轉於雜亂模式時之訊息包，主要地發覺未預定給網路介面出現的位址之訊息包。儘管是運轉雜亂模式中的介面，未修改的 Linux 核心，例如，4.2.26，未捕捉到未提出給其本身（層 2 或 MAC 層）之訊息包。此 Linux 核心傾印 `ip_rcv` 功能中之內容。核心鉤傳輸某些訊息包給不是將被操作的未修改的核心的部份之功能。

監式程式告訴此開關，傳送出心跳。如果切換聽不到自此程式中的心跳，切換將保障此連接（切換繼電器）。在開關充電之後之隱含連接係安全。心跳程式寫入至系統登錄。

使用者空間程式建立 IP 或其它位址、控制器本身的埠及第一與第二裝置，控制器位在第一與第二裝置之間，例如工具/感測器及主機。

於 Linux 中，使用者編寫架構資訊，且開始固定其它

(14)

組件一起。軟體係與樣本架構檔案綁束。架構檔案包含主機 IP、工具 IP、用於觸發監視預設程式定時器之時間間隔、用於與安全開關連通的監視預設程式之通信埠號碼、及用於將來強化之選擇性模式。當以 Linux 4.2.26 實施時，起動原稿較佳地運轉在系統登錄及網路之後及之前。原稿開始及停止程式操作如典型的起動原稿。其可被命名，例如 `hsmsfsd` 起動。此原稿可簡單地採取些微長於其它原稿，因為其發現工具及主機兩者的 MAC 位址且增加適當路由，若需要的話。為了成功發現到，第一及第二裝置，例如工具及主機，係啟動時而連接至控制器。替代地，預定 IP 位址可被載入及使用而無需任何發現。啟動原稿亦增加路由，以告訴 TCP/IP 堆疊控制器 IP 位址如何關連至網路介面 `eth0` 及 `eth1`。

控制器或其它中間裝置有可能加入其中最簡單架構包括工具及主機。於此簡單例中，工具及主機 IP 位址係已知且係於架構表中。當控制器運轉 `hsmsfsd` 起動原稿時，起動開關監視預設程式。此程式絲毫不知任何關於安全機的剩餘部份，然而，如果藍盒未持續為此傳送心跳或指令而待在線上，簡單使開關（Shore Micro switch）切換至安全切換（物理性地連接至工具的主機）。

只要控制器係正常作用，開關待在線上且經由藍盒而連接工具及主機。起動原稿可使用標準 ARP 協定以建立工具及主機的 MAC 位址並更新局部 ARP 表。關於 ARP 協定之更多細節係藉由以下 RFC、ARP 所說明於一般的

(15)

826、PROXY ARP # 1027、DHCP ARP # 2131 及 UNARP # 1868。如果主機或工具回覆在第二網路介面上，例如，主機路由被加至具有此 IP 位址之第二介面。

於此實施例中，工具及主機係位在相同網路子網路，因為工具及主機係控制器網路介面。控制器發現或架構來知道哪一個介面連接至主機及工具，以使控制器可傳輸訊息。TCP/IP 堆疊的隱含路由將以不會作用的不同方式而被使用，因為包括主機及工具兩者的相同網路子網路的所有訊息將被傳輸至相同網路子網路。模組被載入，然後，具有 IP 位址之應用係獲得自架構檔案，而，用於這些 IP 位址之 MAC 位址係獲得自局部 ARP 表。現在，主機及工具係經由藍盒而連接。藍盒架構在 EMX 設定下係被動，架構將接受來自主機之連接，且主動以工具的 IP 位址而連接至工具。被動及主動 HSMS 設定必須共同地具有相同埠。

由裝置驅動器所保持之表，其附加至核心中的 TCP/IP 堆疊鉤，將具有工具的入口及主機的出口。至於第二裝置，例如，工具/感測器，表的登錄可以是：

入口編號	藉由 app 的順序
協定	0x6 用於 TCP
旗標	1 意指 MAC 位址係合法
目的地 MAC 位址	取自起動原稿
目的地 IP 位址	取自起動原稿
目的地埠	取自架構

(16)

來源 IP 位址	未知
來源埠	未知

至於第一裝置，例如主機，表的登錄可以是：

入口編號	藉由 app 的順序
協定	0x6 用於 TCP
旗標	1 意指 MAC 位址係合法
目的地 MAC 位址	取自起動原稿
目的地 IP 位址	取自起動原稿
目的地埠	未知
來源 IP 位址	取自架構
來源埠	取自架構

至於 TCP/IP，獨特連接通常係由 4 元組所識別，4 元組包含來源 IP、來源埠、目的地 IP、及目的地埠。此將使連接通用於網路中，且，獨特的網路協定支持使用 4 元組之獨特連接。所謂的半結合亦是可取得的，其包括目的地 IP 及埠，其中埠係關於服務，而，IP 係連接被製作至其上之機器。例如，www.mksinst.com 係埠 80，且某 IP 提出區域名稱伺服器（Domain Name Server）將由名稱 www.mksinst.com 決定。至於 ISP 使用者，ISP's 端的伺服器將保持你的 IP 及分配局部埠，其組成獨特 4 元組。每當有人開啓瀏覽器的另一視窗時，另一獨特 4 元組被產生，其具有相同目的地 IP 及埠、相同來源 IP、不同來源埠

(17)

被分配以滿足獨特性要件。

於實際操作中，主機將例如，試圖連接至工具或感測器；控制器以其操作於雜亂模式的網路介面而攔截一或更多來自主機之訊息。附接至輸入鉤之第一濾波器被應用，其決定訊息包是否屬於控制器上之任一網路介面。第一濾波器將屬於一介面之任何訊息包給至此介面且離去。如果訊息包不屬於控制器的網路介面，濾波器查詢以上裝置驅動器中的目的地埠及 IP。如果目的地被發現於裝置驅動器表中，濾波器將訊息包的目的地改變成控制器相關位址，且將其轉給 TCP/IP 堆疊。在訊息包係由 TCP/IP 堆疊所操作之後，附接至輸出鉤之第二濾波器恢復此目的地，以使承認或回應將出現來自原始目的地。此處理有時稱為偽入（masquerading in）。此方法支援同時發生的對話。控制器直接處理訊息包或將訊息包轉達其原始目的地，依據訊息包的種類及對話的歷史而定。

於實際操作中，工具/感測器將可試圖連接至主機。中間裝置，控制器將試著傳送訊息包至主機。IP 傳送的功能查詢目的地訊息包及目的地埠。如果目的地被找到，此功能修改其為控制器 IP 之訊息包來源 IP 為表中之工具 IP，複製目的地埠（其碰巧是控制器的來源埠）至此表。工具將回應訊息包，且，接收功能將收到此回應。此表現在是完成。因此，查詢將接替且重導此訊息包給我們的堆疊。此處理有時稱為偽出（masquerading out）。

當 ARP 輸入年齡時，工具或主機將要求其 MAC 位址

(18)

。工具例如，將要求主機 IP 的 MAC 位址，而工具未連接至主機，其連接至控制器。控制器於其表的入口而查詢主機的 IP 位址，且以適當主機用之 MAC 位址而回應 ARP 請求訊息。此係裝置驅動器中的 ARP 鉤。由控制器提供之 MAC 位址係主機的真正 MAC 位址，或，為回應來自主機之 ARP 請求，是工具的真正 MAC 位址。訊息包行程發生在連接至 TCP/IP 堆疊的模組內（`hsmfs.o` 裝置驅動器）。

如果控制器為了任何理由凍結或遭受系統鎖定，安全功能可被啓動。只要串列開關預設程式正在運轉此系統且系統似乎正常，控制器將保留在線上，且，主機及工具將經由控制器而連接。如果預設程式失效，切換將難以安全化，且，主機及工具將相互直接連接。選擇性地，預設程式可評估使控制器的操作的正常狀況，預測或傳送失效，且適當地回應。於預測失效的例子中，主機可被告知，且，選擇性地，控制器正常的傳送可被修改。當安全開關被拋出時，新直接連接的對話中之參與者重試或重建自主機至工具之連接。當連接被重建時，安全操作被完成。於機械繼電器的一實施例中，對切換之電力損失致使繼電器採取安全設定，且直接連接主機至工具。

當主機失去連接時，主機應企圖再啓動對話。因為 ARP 表係最新的，直接連接可隨時建立。重新啓動對話有時稱為強固傳訊（`robust messaging`）。

安全的實施例具有許多有趣特徵，其中有些由替代實

(19)

施例所共用。軟體無需加至第一或第二裝置（主機或工具）。主機及工作係在相同子網路上，以使它們將能夠連通於安全直接連接的例子中。中間裝置或控制器係在如工具及主機的相同子網路上。如果控制器被啓動於安全模式，工具及主機可"相互看見"。當操作自正常模式切換至安全模式時，主動對話將由工具、主機或兩者而自動地重試。

第二操作實施例

於第二實施例中，選擇性橋接係無需控制器回應給主機及工具間的 ARP 請求訊息而實施的。ARP 訊息及自主機指定至工具的其它選擇的訊息，反之亦然，係自控制器的一側橋接至另一側，自操作於雜亂模式的一網路介面通過至另一網路介面且重新傳送。工具回應自主機發送的 ARP 請求訊息，且反之亦然。控制器選擇性地橋接及發送 ARP 請求訊息及具有辨識來源及目的地之另一訊息例如，基於表查詢。以上為有用表。橋接係選擇性的。具有未辨識的目的地的訊息包未由核心鉤所操作，而允許通過一般 TCP/IP 堆疊處理，其然後可丟下訊息包。過濾出某些訊息減小網路上的循環。例如，如果主機經由五個控制器連接至五個工具，第一控制器可安全地濾出某些或所有導引至第二至第五工具之訊息。工具側網路的通信可被實質地減少。如另一實例，控制器可自主機預期或他請求的選擇權之工具而檢索及儲存資料，而尚未請求。控制器可滿足濾出圍繞控制器用之資料通信，且減少主機側網路的通信。

(20)

一可被應用於選擇性橋接的規則係用來僅發送具有主機及目的地之訊息包，此訊息包係藉由與控制器連通之識別。再者，所選擇類型的廣播訊息可被橋接。上述的核心鉤係適於提供用於通過訊息包於網路介面間及用於橋接訊息包之所需支援。

在操作訊息包時，優先權被指定給 HSMS 架構的埠，以使連接藉由邏輯處理而操作在藍盒上。假設目的地 IP 係於邏輯表中，ICMP、UDP、ARP、TCP（除了 HSMS 外的埠）訊息包被發送在此兩網路介面間。因此性能係相似於橋接，而選擇性地限制在此表中的 IP 位址以避免循環於網路中。ARP 限制係甚至更嚴厲，在被發送之前，來源及目標 IP 兩者必須在此表中，其意指僅工具及主機可相互 ARP 跨過控制器的網路介面。

第三操作實施例

替代地，控制器或中間裝置可採取可直接連通的裝置的 IP 位址，且適當地重新封裝及中繼。此方法非常不同於其它類型的裝置的傳統功能，因為控制器的網路介面具有其本身的硬體層識別碼或 MAC 位址。MAC 位址係一般實施於網路之訊息包定址計劃的部份。至於一般網路介面，網路層（例如，IP）連結至資料連結層（例如，MAC），如第七層 OSI 模型中所指定的。網路協定，例如，ARP，允許網路上的裝置相互關聯 IP 及 MAC 位址。訊息包傳輸的日期多餘特性包括檢查碼，檢查碼係部份地使用來自

(21)

訊息包的資料連結層的資訊而編碼。當兩個例如，連接至分開的網路段之網路介面皆使用相同 IP 位址時，它們仍然具有不同的 MAC 位址。至於將訊息包自主機轉移至工具之控制器，或反之亦然，當控制器借用工具的 IP 位址識別碼時，其必須以校正的檢查碼而重新封裝此訊息包，此檢查碼係使用取代控制器的 MAC 位址之工具的 MAC 位址而編碼。然而，這不是很足夠用於安全的實施。可直接連通之裝置必須更新它們對資料連結層表之網路層，例如，它們的 ARP 表，以在失敗之後校正有效 MAC 位址。當上述的安全開關以安全模式直接連接主及及工具，訊息包將不會自主機直接流入工具，因為主機及工具相互具有的 MAC 位址包括控制器的 MAC 位址。為克服此問題，主機或工具的至少一者必須更新其對資料連結層表的網路層。主機、工具或兩者可適於其表的頻繁更新，或可適合藉由更新它們的表而回應給取消的對話。以更新的表，破損的對話可被重建，或者，開始新的直接對話。

實施例的進一步說明

本發明可被實際作為適於實施此方法之方法或裝置。相同方法可自諸如 SenseLink 之聰明感測器或轉接器的立體圖，或自諸如 Blue Box 之控制器的立體圖來觀察。本發明可以是製造的物件，諸如加有實施電腦輔助感測控制的邏輯之媒體。

第一方法實施例係透通地建立第一及第二裝置間的直

(22)

接連接於中間裝置的失效的例子。此方法包括連接第一及第二裝置至中間裝置的第一及第二網路介面。第一及第二網路介面具有不同於與第一及第二裝置結合的資料連結層識別碼之資料連結層識別碼。於正常操作模式中，方法另包括操作定址於第一及第二裝置間之訊息，同時中間裝置將其持續正常操作而重複送出信號給安全開關。在安全開關，在來自中間裝置的正常操作的重複送出信號的中斷之後，此方法包括以旁通中間裝置的資料連接所直接連接第一及第二裝置而切換至安全模式。資料連接可旁通第一及第二網路介面。正常操作的重複送出信號可以是連續電路或離散週期性信號。

第一實施例的一個形態在於，切換至安全模式可造成可聽信號，諸如中繼點選。依據另一形態，第一及第二網路介面可被適用於將所接收的所有訊息包傳輸至操作定址至第一及第二裝置或中間裝置的訊息包之濾波器。用於至少某些訊息包之訊息包的操作可包括自第一或第二裝置之中繼訊息包至第二資料連結層識別碼，以取代第一或第二網路介面的資料連結層識別碼。

另一形態係重覆通知如何被實施。其可藉由運轉在中間裝置上之預設程式而實施，中間裝置重複傳送訊息至安全開關，或，中間裝置收聽及回應自安全開關所查詢。替代地，預設程式可控制連續電路。

實施例另可包括回應至第一裝置之多個第二裝置，其使用一個物理通信連結或兩個或更多物理通信連結。當兩

(23)

個或更多物理通信連結被使用時，一者可以是乙太網路段而另一可以是串列連接。串列連接可順應於 IEEE 標準，諸如 RS-232 或 RS-422。

在操作時，建立第一及第二裝置間之直接通信對話可不需更新第一或第二裝置中關聯網路位址至資料連結層位址的任何位址。亦即，ARP 表可不需被更新。更新關聯 IP 及 MAC 位址之任何表可能是需要的。第一及第二裝置與中間裝置皆可操作在相同網路子網路內。

另一方法實施例係在連結在主機及工具間之智慧控制器的失效之後建立主機及工具間之通信連結的失效回復方法 (failover)。此方法包括在智慧控制器的第一埠採用由工具以不同方式之第一硬體階層識別碼，及在使用第一硬體階層識別碼定址時而通知將第一埠給主機。此方法另包括採用由主機以不同方式之第二硬體階層識別碼，及在使用第二硬體階層識別碼定址時而通知將第二埠給工具。此方法另包括在智慧控制器而攔截第一及第二硬體階層識別碼的通知，以使主機及工具不是處於直接通知通信。於操作中，智慧控制器重覆通知安全開關之控制器應被依靠。在重複送出信號的失效之後，安全開關適於以旁通智慧控制器的通信連結而直接連接主機及工具。其後，主機及工具係處於直接通知連接，且，第一及第二硬體階層識別碼的通知促成主機及工具間之通信連結的建立。

此另一實施例的數個形態被說明。依據一形態，識別第一埠之第一邏輯位址、工具所使用之第二邏輯位址、識

(24)

別第二埠之第三邏輯位址、及主機所使用之第四邏輯位址皆可以是不同。這些邏輯位址可以是 IP 位址或其它網路層位址。硬體階層識別碼可以是 MAC 位址。硬體階層識別碼的通知可以是標準順應性 ARP 訊息。

另一實施例進一步可被應用至監視工具之感測器，其中智慧控制器係連結在主機及感測器之間。此應用可包括在智慧控制器的第一埠採用使用由感測器以不同方式之第三硬體階層識別碼，及在使用第三硬體階層識別碼定址時而通知將第一埠給主機。其可進一步包括在使用第二硬體階層識別碼位址時將第二埠通知給感測器，及在智慧控制器攔截第三硬體階層識別碼的通知，以使主機及感測器不是處於直接通知通信。依據此應用，安全開關在重複送出信號失效之後建立在主機及感測器間之直接通信連結，直接通信連結旁通智慧控制器。直接連接可旁通第一及第二埠。不同邏輯 IP 位址、不同網路層位址、硬體識別碼及 ARP 標準順應性的形態皆可適用於此應用。

另一方法實施例介紹失效回復保護智慧控制器及切換至主機及至少一工具或感測器間之通信連結。此方法包括連結切換至主機、智慧控制器及工具，其中主機及工具與智慧控制器連通且當切換處於第一狀態時不會相互直接連通；當切換處於第二狀態時，主機及工具相互直接連通。於第一狀態中，智慧控制器攔截主機及工具間之訊息，修改攔截訊息中之至少一硬體階層源識別碼及至少一硬體階層目的地識別碼，修改攔截訊息中之至少一錯誤校正碼以

(25)

符合修改的硬體階層識別碼，以及中繼具有修改的硬體階層識別碼及修改的校正碼之攔截訊息。於第二狀態中，切換旁通智慧控制器，建立主機及工具間之直接通信。

於此另一方法實施例的一形態中，智慧控制器包括至少第一及第二埠，第一埠與主機而連通地連結，而第二埠與工具而連通地連結。於此形態，第一邏輯位址識別第一埠，第二邏輯位址係由工具所使用，第三邏輯位址識別第二埠，且，第四邏輯位址係由主機所使用。它們的邏輯位址皆是不同。它們可以是 IP 位址或其它網路層位址。此另一方法實施例的硬體階層識別器可以是 MAC 位址。

此另一方法實施例亦可被應用至監視工具之感測器。此另一應用包括連結安全開關至感測器，其中主機及感測器與智慧控制器連通且當安全開關處於第一狀態時不會相互直接連通；當安全開關處於第二狀態時，主機及感測器相互直接連通。於第一狀態中，智慧控制器操作在如上述之主機及感測器間之訊息上用於主機及工具。第二狀態中，安全開關旁通智慧控制器，且，主機與感測器直接連通。此另一實施例的其它形態可被應用至主機、工具及感測器通信。

智慧控制器可包括：多個附接至工具及感測器之埠，其中埠、主機、工具及感測器的邏輯位址皆是不同。如上述，這些邏輯位址可以是 IP 位址或網路階層識別碼。

所有上述的方法可被實際作為具有適於第一及第二裝置間之直接連接的安全開關之中間裝置於中間裝置的失效

(26)

的例子中。一個實施例包括具有第一及第二網路介面的中間裝置，第一及第二網路介面可分別地與第一及第二裝置而通信地連結，第一及第二網路介面具有不同於與第一或第二裝置關聯的任何資料連結層識別碼之資料連結層識別碼。其另包括與中間裝置連通且臨時與第一及第二裝置通信地連結。安全開關具有至少兩種模式，正常及安全操作模式。於正常操作模式，安全開關連接第一及第二裝置與第一及第二網路介面。於安全模式中，此切換直接連接第一及第二裝置，而旁通中間裝置。此連接可以是電連接，或經由隔絕器。中間裝置另包括適於重複通信正常操作信號至安全開關之邏輯及資源。安全開關另包括適於藉由切換至安全模式而回應正常操作的重複信號的中斷之邏輯及資源。

裝置的一個形態，切換至安全模式包括製作聽不見的信號，諸如中繼的點選。中間裝置可另包括濾波器於邏輯及資源中，濾波器保留用於操作定址於第一及第二裝置或中間裝置之訊息包，此濾波器係連結至第一及第二網路介面。此濾波器允許網路介面操作在雜亂模式上。實施此濾波器之邏輯及資源可駐存在中間裝置中或接近或位在中間裝置的網路介面上之處理器。另一形態係為，中間裝置的邏輯及資源另包括送出信號給安全開關之預設程式。此預設程式可作用於以上方法中所述之任一模式。

雖然本發明係參考以上詳述的較佳實施例及實例而揭示，應瞭解到，這些實例的目的係解說而不是限制之用。

(27)

電腦輔助處理被隱含上述實施例。因此，本發明可被具體實施於用於電腦輔助感應之方法、包括實施感測器控制的邏輯之系統、利用電腦輔助感測器控制之系統、加有實施電腦輔助感測器控制的邏輯之媒體、加有實施電腦輔助感測器控制的邏輯之資料流、或實施電腦輔助感測器控制之電腦接受服務。可預期到，修改及結合將隨時發生在熟習此項技藝者上，這些修改及結合將屬於本發明的精神及以下申請專利的範圍內。

【圖式簡單說明】

圖 1 解說本發明的形態之環境係特別有用的。

圖 2 係與工具、感測器、及工具主機連通之控制器的區塊示意圖。

圖 3 係使用單型的與工具、感測器、及工具主機連通之通信通路之控制器的區塊示意圖。

圖 4 解說使用多型的通信通路。

圖 5 係增加安全開關至網路的區塊圖。

圖 6 係增加安全開關至其它網路的區塊圖。

【主要元件之符號說明】

111：Fab 網路

112：廣域網路

113：氣體盒壓力轉換器

114：質量流控制器（MFC）

(28)

- 115：反應氣體產生器
- 116：晶圓監視器
- 117：氣體成份監視器
- 125：處理室
- 126：視窗
- 127：處理監視器
- 133：臭氧產生器
- 134：材料輸送
- 136：工作件
- 137：壓力轉換器
- 142：數位控制器
- 145：冷卻次系統
- 146：檢漏器
- 147：控制閥
- 148：壓力控制器
- 152：室控制器
- 153、154、155：動力注入器
- 156：次系統
- 157：真空計
- 158：排氣監視器
- 162：連接器
- 200：控制器
- 211：主機
- 212、216：SEC/GEM 介面埠

(29)

215 : SECS MUX

217 : SEC/GEM 工具介面

221 : 報告

222 : 網路

225 : 公開資源

226 : 網路

227 : 感測器

231 : 儲存

232、236 : 網路介面埠

234 : Fab 側介面

235 : 工具側介面

237 : 儀器

301 : 工具

302 : 感測器

302A-B : 感測器

303 : 控制器

304 : 工具網路或主機

307、309 : SECS 協定

308 : 連接

409 : 工具側網路

413 : 管理開關

415 : 網路附加儲存 (NAS)

419 : Fab 側網路

423 : 分析軟體

(30)

425：延伸網路

427：資料庫

501：工具

511：旁通開關

512：插孔或開關

521、522：網路介面

523：額外連接

五、中文發明摘要

發明之名稱：智慧控制器方法及裝置之安全切換

本發明係關於與工具相關聯的感測器的控制及來自工具相關聯的感測器之資料收集。尤其，本發明關於使用控制器來媒介工具、與工具相關聯之感測器及資料使用者間之通信，諸如主機系統或分佈型處理器。本發明的特別形態係說明於申請專利範圍、說明書及圖式。

六、英文發明摘要

發明之名稱：

FAILSAFE SWITCHING OF INTELLIGENT CONTROLLER METHOD AND DEVICE

The present invention relates to control of and data collection from sensors associated with tools. In particular, it relates to using a controller to mediate communications among a tool, sensors associated with the tool and data users, such as a host system or distributed processors. Particular aspects of the present invention are described in the claims, specification and drawings.



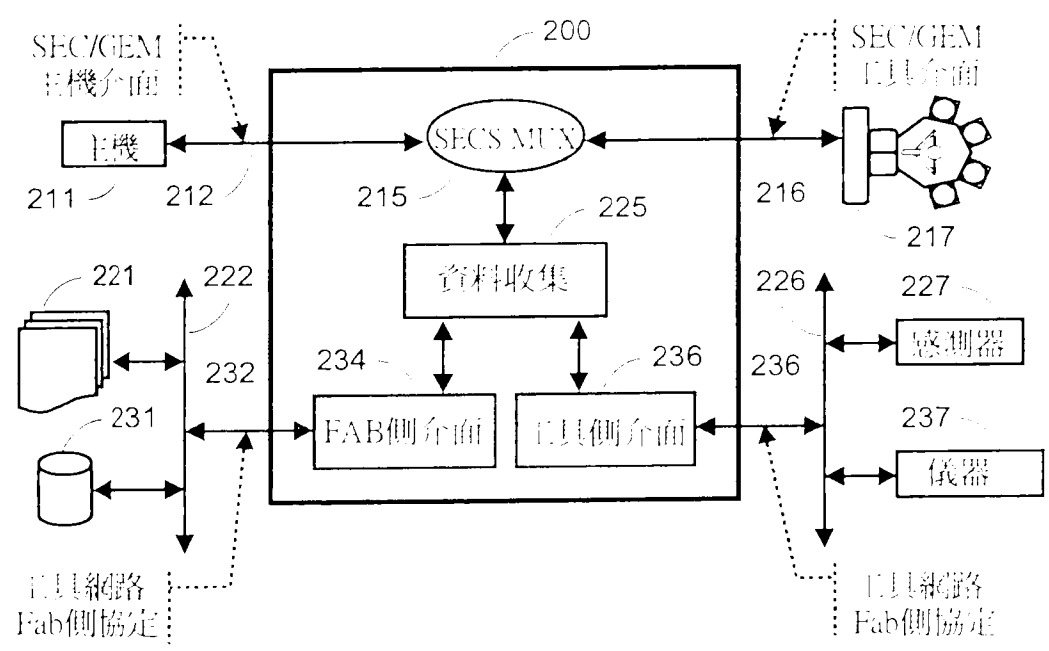


圖 2

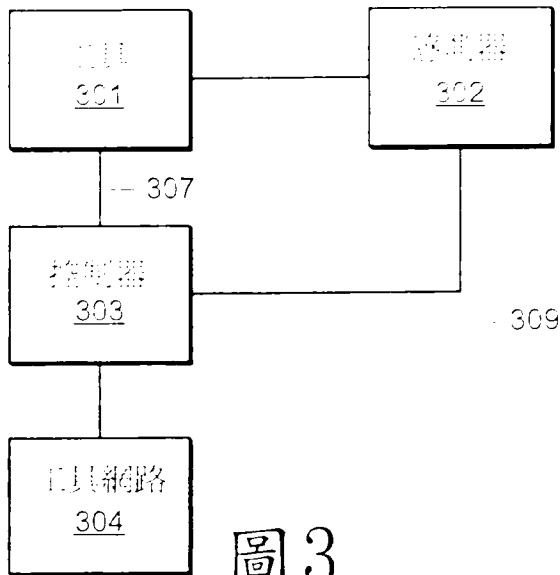


圖 3

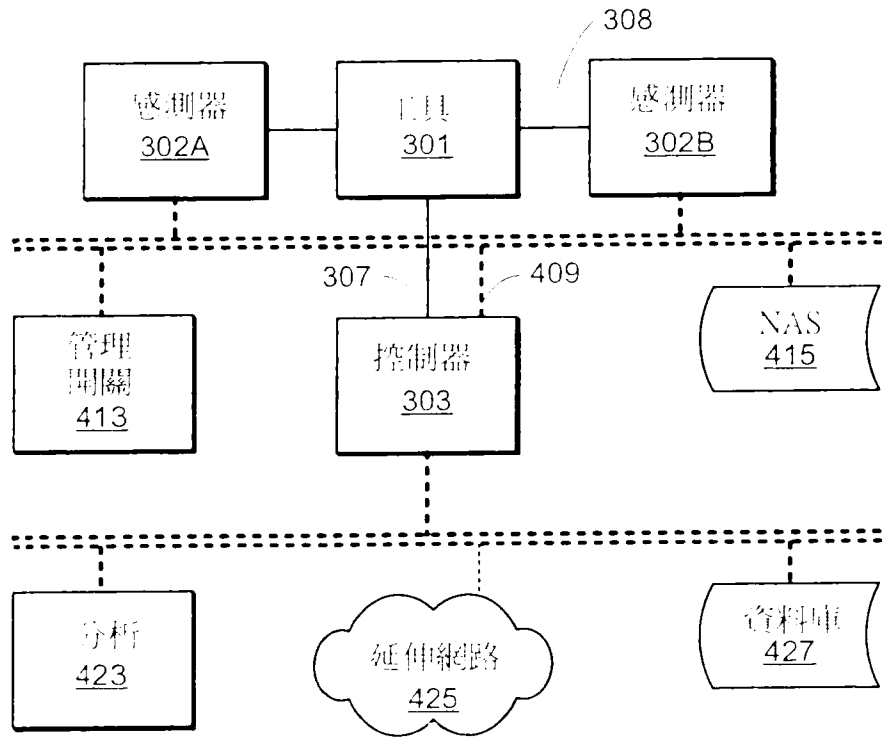


圖 4

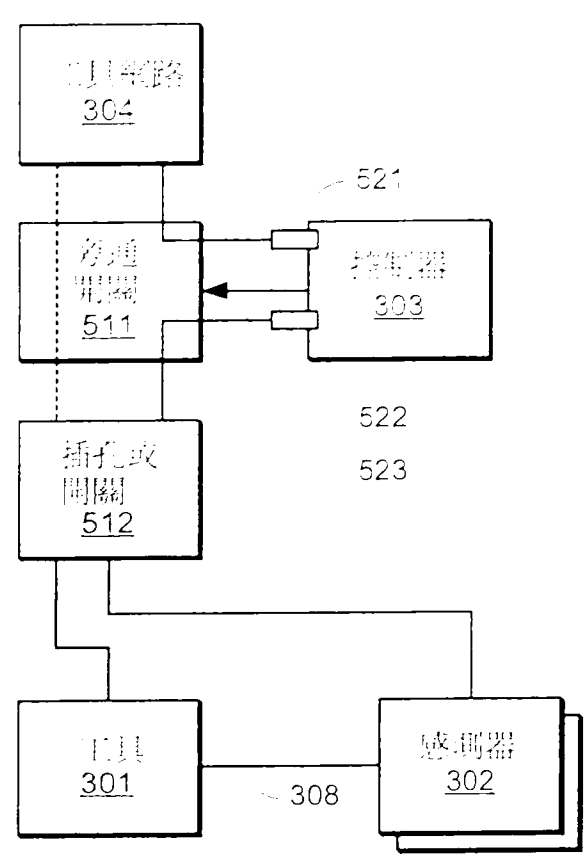


圖 5

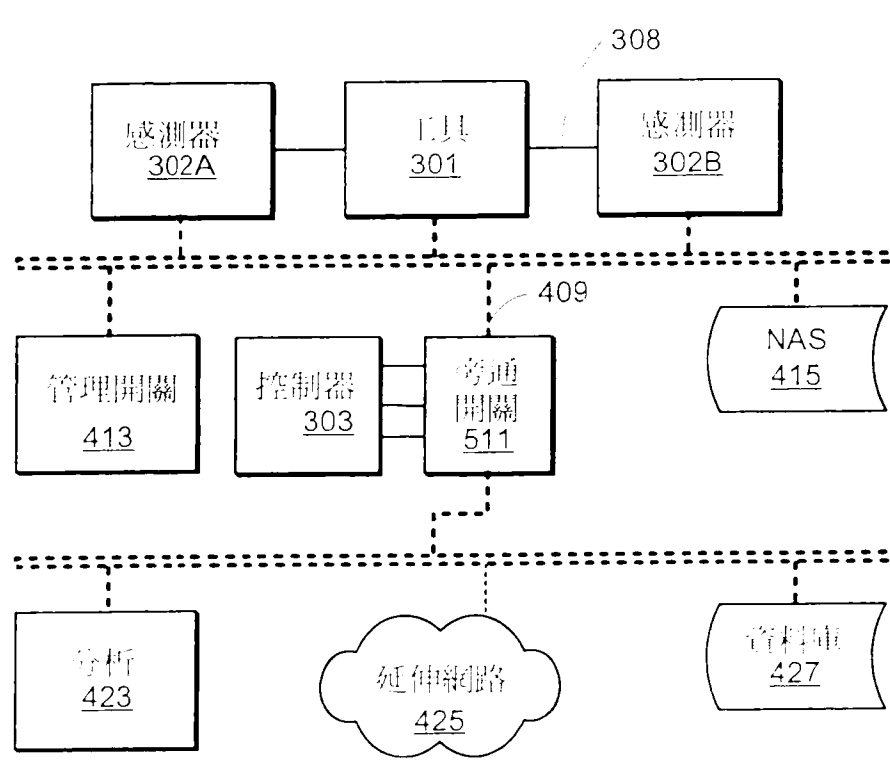


圖 6

七、指定代表圖：

(一)、本案指定代表圖為：第 (5) 圖

(二)、本代表圖之元件代表符號簡單說明：

301：工具

302：感測器

303：控制器

304：工具網路或主機

308：連接

511：旁通開關

512：插孔或開關

521、522：網路介面

523：額外連接

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：無

附件 3 ：第094125156號申請專利範圍修正本

民國 101 年 7 月 16 日修正

十、申請專利範圍

1. 一種在發生中間裝置的失效時透過地 (transparently) 建立第一及第二裝置間的連接之方法，該方法包括：

連接第一及第二裝置至中間裝置的第一及第二網路介面，第一及第二網路介面之資料連結層識別碼係不同於與第一及第二裝置關聯之資料連結層識別碼；

於正常操作模式中，當中間裝置將其連續的正常操作之信號重複地傳送至安全開關時，操作定址在第一及第二裝置間之中間裝置訊息，其中所操作之訊息呈現為已來自該等裝置的其中之一裝置而至該等裝置中之另一裝置，以致其切換至安全模式能容許該其中之一裝置與該另一裝置之間的網路對話繼續而無須重新啟動；及

在安全開關，在來自中間裝置之正常操作的重複信號中斷之後，藉著以旁通中間裝置之資料連接，直接地連接第一及第二裝置而切換至安全模式。

2. 如申請專利範圍第 1 項之方法，其中將安全開關切換至安全模式包括製作可收聽信號。

3. 如申請專利範圍第 2 項之方法，其中可收聽信號係中繼點選 (relay click)。

4. 如申請專利範圍第 1 項之方法，其中第一及第二網路介面係適於將所接收的所有訊息包傳送至保留用於定

址至中間裝置的訊息包之濾波器。

5. 如申請專利範圍第 1 項之方法，其中訊息包的操作包括，用於至少某些訊息包，將來自第一或第二裝置之訊息包中繼至第二或第一裝置，及，於中繼訊息包的來源識別域中，指定實際來源的資料連結層識別碼，以取代第一或第二網路介面的資料連結識別碼。

6. 如申請專利範圍第 1 項之方法，其中重複地傳送連續正常信號係藉由運轉在傳送訊息至安全開關的中間裝置上之預設程式(daemon)而實施。

7. 如申請專利範圍第 1 項之方法，其中重複地傳送連續正常信號係藉由運轉在收聽且回應來自安全開關的查詢的中間裝置上之預設程式而實施。

8. 如申請專利範圍第 1 項之方法，另包括數個使用單一物理通信連結而連接至第一裝置之第二裝置。

9. 如申請專利範圍第 8 項之方法，其中單一物理通信連結係乙太網路段(Ethernet segment)。

10. 如申請專利範圍第 1 項之方法，另包括數個使用兩個或更多物理通信連結而連接至第一裝置之第二裝置。

11. 如申請專利範圍第 10 項之方法，其中物理通信連結的一者係乙太網路段，而，另一者係串列連接。

12. 如申請專利範圍第 11 項之方法，其中串列連接遵守 RS-232 或 RS-422 標準。

13. 如申請專利範圍第 1 項之方法，其中建立第一及第二裝置間的直接通信對話不需於第一或第二裝置中更新

與網路位址及資料連結層位址相關聯之任何表。

14. 如申請專利範圍第 1 項之方法，其中第一及第二裝置與中間裝置的網路位址都是在相同網路子網路內。

15. 如申請專利範圍第 1 項之方法，其中建立第一及第二裝置間的直接通信對話不需於第一或第二裝置中更新與 IP 及 MAC 位址相關聯之任何表。

16. 一種在連結於主機及工具之間的智慧控制器失效之後建立主機及工具之間的通信連結之失效回復 (fail-over) 方法，該方法包括：

在智慧控制器的第一埠採用由工具以不同方式使用之第一硬體階層識別碼，及，在使用第一硬體階層識別碼定址時將第一埠通知給主機；

在智慧控制器的第二埠採用由主機以不同方式使用之第二硬體階層識別碼，及，在使用第二硬體階層識別碼定址時將第二埠通知給工具；

在智慧控制器攔截第一及第二硬體階層識別碼的通知，以使主機及工具不是處於直接通知通信中；將應依賴智慧控制器之信號重覆地通知安全開關，其中安全開關係適於在重覆通知的失效之後，以旁通智慧控制器的通信連結而直接連接主機及工具，藉此，主機及工具係處於直接通知通信中，且，第一及第二硬體階層識別碼的通知促成主機及工具之間的通信連結之建立。

17. 如申請專利範圍第 16 項之方法，其中識別第一埠之第一邏輯 IP 位址、工具所使用之第二邏輯 IP 位址、

識別第二埠之第三邏輯 IP 位址、及主機所使用之第四邏輯 IP 位址皆是不同。

18. 如申請專利範圍第 16 項之方法，其中識別第一埠之第一邏輯網路層位址、工具所使用之第二邏輯網路層位址、識別第二埠之第三邏輯網路層位址、及主機所使用之第四邏輯網路層位址皆是不同。

19. 如申請專利範圍第 16 項之方法，其中硬體階層識別碼係 MAC 位址。

20. 如申請專利範圍第 16 項之方法，其中硬體階層識別碼的通知(advertisements)係藉由標準順應性 ARP 訊息。

21. 如申請專利範圍第 16 項之方法，進一步應用至監視工具之感測器，其中智慧控制器係連結在主機及感測器之間，該方法另包括：

在智慧控制器的第一埠採用由感測器以不同方式使用之第三硬體階層識別碼，及，在使用第三硬體階層識別碼定址時將第一埠通知給主機；

在使用第二硬體階層識別碼定址時將第二埠通知給感測器；及

在智慧控制器攔截第三硬體階層識別碼的通知，以使主機及感測器不是處於直接通知通信中；

其中，安全開關在重覆通知的失效之後，建立主機及感測器之間的直接通信連結，該感測器旁通智慧控制器。

22. 如申請專利範圍第 21 項之方法，其中識別第一

埠之第一邏輯 IP 位址、工具所使用之第二邏輯 IP 位址、識別第二埠之第三邏輯 IP 位址、主機所使用之第四邏輯 IP 位址、及感測器所使用之第五邏輯 IP 位址皆是不同。

23. 如申請專利範圍第 21 項之方法，其中識別第一埠之第一邏輯網路層位址、工具所使用之第二邏輯網路層位址、識別第二埠之第三邏輯網路層位址、主機所使用之第四邏輯網路層位址、及感測器所使用之第五邏輯網路層位址皆是不同。

24. 如申請專利範圍第 21 項之方法，其中硬體階層識別碼係 MAC 位址。

25. 如申請專利範圍第 21 項之方法，其中硬體階層識別碼的通知係藉由標準順應性 ARP 訊息。

26. 一種將失效回復 (fail-over) 保護智慧控制器及安全開關導入於主機連接到至少一工具之間的通信連結之方法，該方法包括：

連結該安全開關至主機、智慧控制器及工具，其中主機及工具與智慧控制器連通，且，當該安全開關處於第一狀態時不會相互直接連通，而，當該安全開關處於第二狀態時主機及工具相互直接連通；

於第一狀態中，該智慧控制器

攔截主機及工具之間之訊息，

修改攔截的訊息中的至少一硬體階層源識別碼及至少一硬體階層目的地識別碼，

修改攔截的訊息中的至少一錯誤校正碼，以符合修改

的硬體階層識別碼，及

以修改的硬體階層識別碼及修改的校正碼，中繼攔截的訊息；及

於第二狀態中，該安全開關旁通智慧控制器，藉此，主機與工具直接連通。

27. 如申請專利範圍第 26 項之方法，其中

智慧控制器包括至少第一埠及第二埠，第一埠與主機連通地連結，而，第二埠與工具連通地連結；及

識別第一埠之第一邏輯 IP 位址、由工具所使用之第二邏輯 IP 位址、識別第二埠之第三邏輯 IP 位址、及由主機所使用之第四邏輯 IP 位址皆是不同。

28. 如申請專利範圍第 26 項之方法，其中

智慧控制器包括至少第一埠及第二埠，第一埠經由安全開關而與主機連通地連結，而，第二埠經由安全開關而與工具連通地連結；及

識別第一埠之第一邏輯網路層位址、由工具所使用之第二邏輯網路層位址、識別第二埠之第三邏輯網路層位址、及由主機所使用之第四邏輯網路層位址皆是不同。

29. 如申請專利範圍第 26 項之方法，其中硬體階層識別碼係 MAC 位址。

30. 如申請專利範圍第 26 項之方法，進一步應用至監視該工具之感測器，該方法另包括：

連結該安全開關至感測器，其中主機及感測器與智慧控制器連通，當安全開關處於第一狀態時不會相互直接連

通，且，當安全開關處於第二狀態時主機及感測器相互直接連通；

於第一狀態中，智慧控制器

攔截主機及感測器間之訊息，

修改攔截的訊息中的至少一硬體階層源識別碼及至少一硬體階層目的地識別碼，

修改攔截的訊息中的至少一錯誤校正碼以符合修改的硬體階層識別碼，及

以修改的硬體階層識別碼及修改的校正碼而中繼攔截的訊息；及

於第二狀態中，安全開關旁通智慧控制器，藉此，主機與感測器直接連通。

31. 如申請專利範圍第30項之方法，其中

智慧控制器包括至少第一埠及第二埠，第一埠經由安全開關與主機連通地連結，而，第二埠經由安全開關與工具及感測器連通地連結；及

識別第一埠之第一邏輯 IP 位址、由工具所使用之第二邏輯 IP 位址、識別第二埠之第三邏輯 IP 位址、由主機所使用之第四邏輯 IP 位址、及由感測器所使用之第五邏輯 IP 位址皆是不同。

32. 如申請專利範圍第30項之方法，其中

智慧控制器包括至少第一埠及第二埠，第一埠經由安全開關而與主機連通地連結，而，第二埠經由安全開關與工具連通地連結；及

識別第一埠之第一邏輯網路層位址、由工具所使用之第二邏輯網路層位址、識別第二埠之第三邏輯網路層位址、由主機所使用之第四邏輯網路層位址、及由感測器所使用之第五邏輯網路層位址皆是不同。

33. 如申請專利範圍第 30 項之方法，其中

智慧控制器包括至少第一埠、第二埠及第三埠，第一埠經由安全開關與主機連通地連結，第二埠經由安全開關與工具連通地連結及第三埠經由安全開關與感測器連通地連結；及

識別第一埠之第一邏輯 IP 位址、由工具所使用之第二邏輯 IP 位址、識別第二埠之第三邏輯 IP 位址、由主機所使用之第四邏輯 IP 位址、及由感測器所使用之第五邏輯 IP 位址皆是不同。

34. 如申請專利範圍第 30 項之方法，其中

智慧控制器包括至少第一埠、第二埠及第三埠，第一埠經由安全開關與主機連通地連結，第二埠經由安全開關與工具連通地連結及第三埠經由安全開關與感測器連通地連結；及

識別第一埠之第一邏輯網路層位址、由工具所使用之第二邏輯網路層位址、識別第二埠之第三邏輯網路層位址、由主機所使用之第四邏輯網路層位址、及由感測器所使用之第五邏輯網路層位址皆是不同。

35. 一種具有安全開關之中間裝置，該安全開關適於在發生中間裝置的失效時確認第一及第二裝置間之直接連

接，該方法包括：

中間裝置具有分別地與第一及第二裝置連通地連結之第一及第二網路介面，第一及第二網路介面的資料連結層識別碼係不同於與第一及第二裝置關聯的任何資料連結層識別碼；

安全開關與中間裝置連通且與第一及第二裝置臨時連通地連結，其中安全開關係適於第一及第二裝置與第一及第二網路介面連通之正常操作模式，及第一及第二裝置直接連通而旁通中間裝置之安全操作模式；

中間裝置上的邏輯及資源適於：

接收其來自該等裝置的其中之一裝置的該等網路介面之一上的訊息包，

將該等網路介面之另一上的訊息包中繼至該等裝置中之另一裝置，及

重複地傳送中間裝置的正常操作至安全開關；

安全開關上的邏輯及資源適於藉由切換至安全模式以回應來自中間裝置之正常操作的重複通知的中斷；

其中所中繼之訊息包呈現為已來自該其中之一裝置而至該另一裝置，以致其切換至安全模式能容許該其中之一裝置與該另一裝置之間的網路對話繼續而無須重新啟動。

36. 如申請專利範圍第 35 項之中間裝置，其中切換安全開關至安全模式另包括製作可收聽信號。

37. 如申請專利範圍第 36 項之中間裝置，其中可收聽信號係中繼點選。

38. 如申請專利範圍第 35 項之中間裝置，其中中間裝置的邏輯及資源另包括保持用於處理定址至中間裝置的訊息包之濾波器，該濾波器係連結至第一及第二網路介面。

39. 如申請專利範圍第 35 項之中間裝置，其中中間裝置的邏輯及資源另包括運轉在中間裝置上之預設程式，該中間裝置傳送訊息至安全開關。

40. 如申請專利範圍第 35 項之中間裝置，其中中間裝置的邏輯及資源另包括運轉在中間裝置上之預設程式，該中間裝置收聽及回應來自安全開關之查詢。