I772976

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I772976 B**

(45)公告日： 中華民國 111 (2022) 年 08 月 01 日

(21)申請案號：109140890 (22)申請日： 中華民國 109 (2020) 年 11 月 20 日

(51)Int. Cl.： *G06F11/00 (2006.01)* *H04L12/22 (2006.01)*
G06F21/70 (2013.01) *G06F21/56 (2013.01)*

(30)優先權：2019/11/20 美國 62/938,158

(71)申請人：美商奈米創尼克影像公司 (美國) NANOTRONICS IMAGING, INC. (US)
美國

(72)發明人：樸特曼 馬修 C PUTMAN, MATTHEW C. (US)；皮斯基 巴迪姆 PINSKIY, VADIM (US)；黎莫葛 達瑪斯 LIMOGE, DAMAS (US)；桑斯壯 安德魯 SUNDSTROM, ANDREW (US)

(74)代理人：陳長文

(56)參考文獻：

TW	I409658	CN	105960777A
CN	106687981A	CN	107835982A
CN	107851047A	CN	107976969A
JP	4621773B2	US	2010/0131202A1
US	2018/0321667A1		

審查人員：廖天佑

申請專利範圍項數：20 項 圖式數：6 共 36 頁

(54)名稱

用於判定網路攻擊及產生警告之製造系統及電腦實施方法

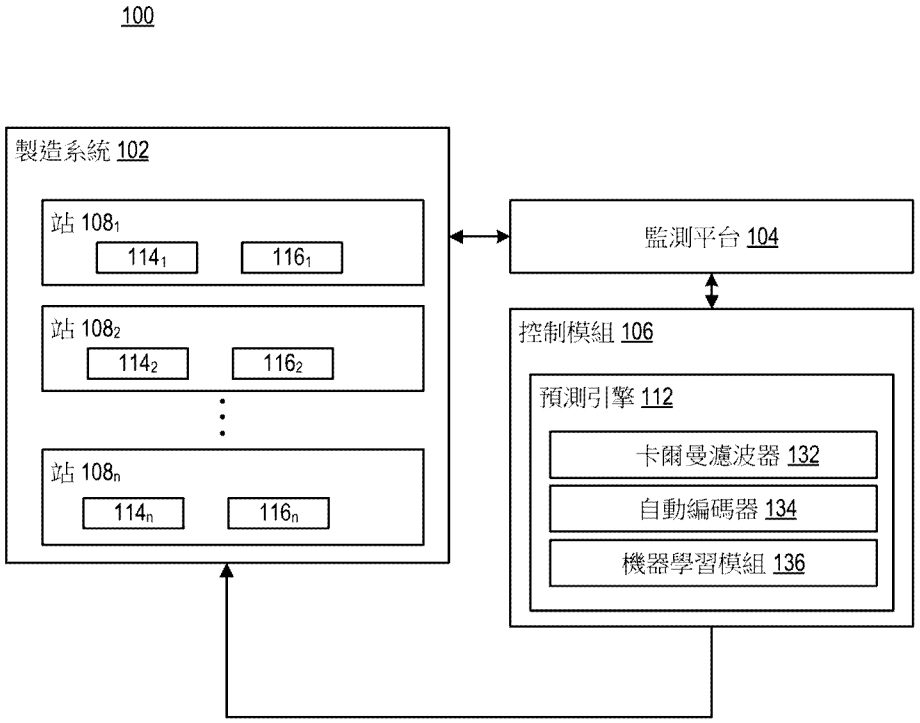
(57)摘要

本文中揭示一種製造系統。該製造系統包含一或多個站、一監測平台，及一控制模組。該一或多個站之各站經組態以針對一組件執行一多步驟製造程序中之至少一個步驟。該監測平台經組態以監測該組件在整個該多步驟製造程序的進展。該控制模組經組態以偵測對該製造系統之一網路攻擊。該控制模組經組態以執行操作。該等操作包含接收該一或多個站之一第一站之控制值。該等操作進一步包含使用一或多個機器學習演算法而基於該第一站之該等控制值來判定存在一網路攻擊。該等操作進一步包含產生一警告以終止該組件之處理。在一些實施例中，該等操作進一步包含校正由該網路攻擊引起之錯誤。

A manufacturing system is disclosed herein. The manufacturing system includes one or more stations, a monitoring platform, and a control module. Each station of the one or more stations is configured to perform at least one step in a multi-step manufacturing process for a component. The monitoring platform is configured to monitor progression of the component throughout the multi-step manufacturing process. The control module is configured to detect a cyberattack to the manufacturing system. The control module is configured to perform operations. The operations include receiving control values for a first station of the one or more stations. The operations further include determining that there is a cyberattack based on the control values for the first station using one or more machine learning algorithms. The operations further

include generating an alert to cease processing of the component. In some embodiments, the operations further include correcting errors caused by the cyberattack.

指定代表圖：



【圖1】

符號簡單說明：

100:製造環境

102:製造系統

104:監測平台

106:控制模組

108_1 至 108_n:站

114_1 至 114_n:程序控制器

116_1 至 116_n:控制邏輯

132:卡爾曼濾波器

134:自動編碼器

136:機器學習模組

111年01月07日 所提修正

公告本

I772976

【發明摘要】

【中文發明名稱】

用於判定網路攻擊及產生警告之製造系統及電腦實施方法

【英文發明名稱】

MANUFACTURING SYSTEM AND COMPUTER-IMPLEMENTED METHOD FOR DETERMINING CYBERATTACK AND GENERATING ALERT

【中文】

本文中揭示一種製造系統。該製造系統包含一或多個站、一監測平台，及一控制模組。該一或多個站之各站經組態以針對一組件執行一多步驟製造程序中之至少一個步驟。該監測平台經組態以監測該組件在整個該多步驟製造程序的進展。該控制模組經組態以偵測對該製造系統之一網路攻擊。該控制模組經組態以執行操作。該等操作包含接收該一或多個站之一第一站之控制值。該等操作進一步包含使用一或多個機器學習演算法而基於該第一站之該等控制值來判定存在一網路攻擊。該等操作進一步包含產生一警告以終止該組件之處理。在一些實施例中，該等操作進一步包含校正由該網路攻擊引起之錯誤。

【英文】

A manufacturing system is disclosed herein. The manufacturing system includes one or more stations, a monitoring platform, and a control module. Each station of the one or more stations is configured to perform at least one step in a multi-step manufacturing process for a component. The monitoring platform is configured to monitor progression of the component throughout the multi-step manufacturing process. The control

module is configured to detect a cyberattack to the manufacturing system. The control module is configured to perform operations. The operations include receiving control values for a first station of the one or more stations. The operations further include determining that there is a cyberattack based on the control values for the first station using one or more machine learning algorithms. The operations further include generating an alert to cease processing of the component. In some embodiments, the operations further include correcting errors caused by the cyberattack.

【指定代表圖】

圖1

【代表圖之符號簡單說明】

100: 製造環境

102: 製造系統

104: 監測平台

106: 控制模組

108_1至108_n: 站

114_1至114_n: 程序控制器

116_1至116_n: 控制邏輯

132: 卡爾曼濾波器

134: 自動編碼器

136: 機器學習模組

【發明說明書】

【中文發明名稱】

用於判定網路攻擊及產生警告之製造系統及電腦實施方法

【英文發明名稱】

MANUFACTURING SYSTEM AND COMPUTER-IMPLEMENTED METHOD FOR DETERMINING CYBERATTACK AND GENERATING ALERT

【技術領域】

【0001】 本發明大體上係關於一種用於製造程序之系統、方法及媒體。

【先前技術】

【0002】 過去數十年之網路攻擊(cyberattack)已見證一驚人程度之擴散、適應、特異性及複雜性。工業及軍事安全性係限制資訊之惡意插入或移除之實體及數位壁之研究。針對高安全性工廠及軍事裝置，此意謂產生自全域電腦網絡移除且通常自內部網路移除之系統。

【發明內容】

【0003】 在一些實施例中，本文中揭示一種製造系統。該製造系統包含一或多個站、一監測平台及一控制模組。該一或多個站之各站經組態以針對一組件執行一多步驟製造程序中之至少一個步驟。該監測平台經組態以監測該組件在整個該多步驟製造程序之進展。該控制模組經組態以偵測對該製造系統之一網路攻擊，該控制模組經組態以執行操作。該等操作包含接收該一或多個站之一第一站之控制值。該等控制值包含該第一處理站之屬性。該等操作進一步包含使用一或多個機器學習演算法基於該第一站之該等控制值判定存在一網路攻擊。該等操作進一步包含基於該判定，

產生一警告以終止該組件之處理。

【0004】 在一些實施例中，本文中揭示一種電腦實施方法。一運算系統接收經組態以處理一組件之一製造系統的一或多個站之一第一站之控制值。該等控制值包含該第一站之屬性。該運算系統使用一或多個機器學習演算法基於該第一站之該等控制值判定存在一網路攻擊。該運算系統基於該判定產生一警告以終止該組件之處理。該運算系統產生用以校正由該網路攻擊引起之錯誤之一組動作。該組動作與該製造系統之下游站相關聯。

【0005】 在一些實施例中，本文中揭示一種製造系統。該製造系統包含一或多個站、一監測平台及一控制模組。該一或多個站之各站經組態以針對一組件執行一多步驟製造程序中之至少一個步驟。該監測平台經組態以監測該組件在整個該多步驟製造程序之進展。該控制模組經組態以偵測對該製造系統之一網路攻擊，該控制模組經組態以執行操作。該等操作包含接收該一或多個站之一第一站之控制值。該等控制值包含該第一站之屬性。該等操作進一步包含使用一或多個機器學習演算法基於該第一站之該等控制值判定存在一網路攻擊。該等操作進一步包含基於該判定產生一警告以終止該組件之處理。該等操作進一步包含使用一或多個第二機器學習演算法產生用以校正由該網路攻擊引起之錯誤之一組動作。該組動作與該製造系統之下游站相關聯。

【圖式簡單說明】

【0006】 可藉由參考實施例(其等之一些在隨附圖式中繪示)進行上文簡要概述之本發明之一更具體描述，使得可詳細理解本發明之上述特徵之方式。然而，應注意，隨附圖式僅繪示本發明之典型實施例且因此不應

視為限制其範疇，此係因為本發明可允許其他相等有效實施例。

【0007】 圖1係繪示根據例示性實施例之一製造環境的一方塊圖。

【0008】 圖2係繪示根據例示性實施例之實施卡爾曼(Kalman)濾波器之一單輸入單輸出系統之架構的一方塊圖。

【0009】 圖3係繪示根據例示性實施例之實施自動編碼器之一系統之架構的一方塊圖。

【0010】 圖4係繪示根據例示性實施例之使用機器學習模組實施一強化學習方法之一系統之架構的一方塊圖。

【0011】 圖5係繪示根據例示性實施例之管理對一製造程序之一網路攻擊之一方法之一流程圖。

【0012】 圖6A繪示根據例示性實施例之一系統匯流排運算系統架構。

【0013】 圖6B繪示根據例示性實施例之具有一晶片組架構之一電腦系統。

【0014】 為了促進理解，已在可能之處使用相同元件符號以指定圖共有之相同元件。經審慎考慮，一項實施例中揭示之元件可在無具體敘述之情況下有利地用於其他實施例。

【實施方式】

相關申請案之交叉參考

【0015】 本申請案主張2019年11月20日申請之美國臨時申請案第62/938,158號的優先權，該案之全文藉此係以引用的方式併入本文中。

【0016】 製造程序可係複雜的且包含藉由不同處理站(或「站」)處理直至產生一最終產品之原始材料。在一些實施例中，各處理站接收用於

處理之一輸入且可輸出一中間輸出，該中間輸出可被傳遞至一後續(下游)處理站以進行額外處理。在一些實施例中，一最終處理站可接收用於處理之一輸入且可輸出最終產品或更一般言之，最終輸出。

【0017】 在一些實施例中，各站可包含可執行一組程序步驟之一或多個工具/設備。例示性處理站可包含(但不限於)運送帶、射出模製機、切割機、模壓機、擠壓機、電腦數控(CNC)磨機、研磨機、組裝站、三維印表機、品質控制站、驗證站及類似者。

【0018】 在一些實施例中，各處理站之操作可由一或多個程序控制器控管。在一些實施例中，各處理站可包含可經程式化以控制處理站之操作之一或多個程序控制器。在一些實施例中，一操作者或控制演算法可為站控制器提供可表示各控制值之所要值或值範圍之站控制器設定點。在一些實施例中，在一製造程序中用於回饋或前饋之值可稱為控制值。例示性控制值可包含(但不限於)：速度、溫度、壓力、真空、旋轉、電流、電壓、功率、黏度、在站處使用之材料/資源、通量率、中斷時間、有毒煙霧、pH、光吸收、顆粒密度及幾何構形及類似者。

【0019】 統計程序控制(SPC)係採用統計方法以監測且控制一程序之一品質控制方法。一般言之，SPC需要針對一製造程序中之各步驟建立且貫穿生產生命週期監測之程序標準。SPC之目標係在整個生命週期持續改良程序。

【0020】 為了SPC之目的，假定只要各節點在規範內操作，最終產品亦將在規範內。可基於標的物專業知識及歷史效能設定規範。在SPC中未直接調整一個節點對下一或後續節點之相依性及影響；而是，可將各子程序檢查為一獨立實體。此方法導致各節點之操作條件之更廣裕度，從而

防止系統甚至在絕對最高效率或穩定性中操作。自一安全性觀點，此裕度可被複雜程序網路攻擊鎖定目標。如果一系統中之一單一節點或若干節點開始在其等規範之上界(或下界)處操作，則將不觸發個別警報，但整體程序品質將受影響。此尤其適用於中間人網路攻擊，其中經報告感測器信號(例如)由惡意程式碼偽造。節點之生命週期亦將受影響，因此需要增加停機時間以進行修理。下游節點之若干層亦將受影響且隨著時間，系統之持續漂移將趨向於不合規。至該點，復原系統所需之校正將係大量且成本過高。

【0021】 本文中提供之一或多種技術係關於用於藉由將可疑惡意活動視為一程序變動且憑藉主動地調諧系統之操作參數來校正其而實現工業安全性之一新穎方法。隨著對工業系統之威脅在數目及複雜性上增加，習知安全性方法需要與程序控制中之進步齊頭並進以整體強化系統。

【0022】 圖1係繪示根據例示性實施例之一製造環境100的一方塊圖。製造環境100可包含一製造系統102、一監測平台104及一控制模組106。製造系統102可廣泛地代表一多步驟製造系統。在一些實施例中，製造系統102可代表一組裝線系統，其中各處理站可代表一人類工人。在一些實施例中，製造系統102可代表用於積層製造之一製造系統(例如，3D列印系統)。在一些實施例中，製造系統102可代表用於減材製造(例如，CNC機械加工)之一製造系統。在一些實施例中，製造系統102可代表用於積層製造及減法製造之一組合之一製造系統。更一般言之，在一些實施例中，製造系統102可代表用於一一般製造程序中之一製造系統。

【0023】 製造系統102可包含一或多個站108_1至108_n (一般言之，「站108」)。各站108可代表一多步驟製造程序中之一步驟及/或站。例

如，各站108可代表一3D列印程序中之一層沈積操作(例如，站108_1可對應於層1，站108_2可對應於層2等)。在另一實例中，各站108可對應於一特定處理站。在另一實例中，各站108可對應於執行一組裝線製造程序中之一特定任務之一特定人類操作者。

【0024】 各站108可包含一程序控制器114及控制邏輯116。各程序控制器114_1至114_n可經程式化以控制各各自站108之操作。在一些實施例中，控制模組106可為各程序控制器114提供可表示各控制值之所要值或值範圍之站控制器設定點。控制邏輯116可係指與一站108之程序步驟相關聯之屬性/參數。在操作中，取決於一最終品質度量之一當前軌道，可在整個製造程序藉由控制模組106動態地更新各站108之控制邏輯116。

【0025】 監測平台104可經組態以監測製造系統102之各站108。在一些實施例中，監測平台104可係製造系統102之一組件。例如，監測平台104可係一3D列印系統之一組件。在一些實施例中，監測平台104可獨立於製造系統102。例如，監測平台104可改裝至一現有製造系統102上。在一些實施例中，監測平台104可代表經組態以在一多步驟程序之各步驟處擷取一產品或工具(例如，一工人或一程序工具)之一影像之一成像裝置。例如，監測平台104可經組態以擷取在各站108處之組件之一影像及/或在各站108處開發產品之一組件(例如，工具、人類等)之一影像。一般言之，監測平台104可經組態以擷取與一產品之產生(例如，一影像、一電壓讀取、一速度讀取等)及/或工具(例如，手位置、工具位置等)相關聯之資訊，且將該資訊作為輸入提供至控制模組106以供評估。

【0026】 控制模組106可經由一或多個通信頻道與製造系統102及監測平台104通信。在一些實施例中，一或多個通信頻道可代表經由網際網

路(諸如蜂巢式或Wi-Fi網路)之個別連線。在一些實施例中，一或多個通信頻道可使用直接連線(諸如射頻識別(RFID)、近場通信(NFC)、Bluetooth™、低能量Bluetooth™ (BLE)、Wi-Fi™、ZigBee™、環境反向散射通信(ABC)協定、USB、WAN或LAN)連接終端機、服務及行動裝置。

【0027】 控制模組106可經組態以控制製造系統102之各程序控制器。例如，基於由監測平台104擷取之資訊，控制模組106可經組態以調整與一特定站108相關聯之程序控制。在一些實施例中，控制模組106可經組態以基於一經投射最終品質度量而調整一特定站108之程序控制。

【0028】 如上文論述，用於偵測程序攻擊之習知方法係各種SPC技術。SPC係用於程序控制之一靜態非干預性方法，其中被動地觀察經良好定義統計性質以在各節點處通過或失敗。僅在最後節點之處理之後，此等習知系統作出關於是否係保持或摒棄經製造產品之一決策。

【0029】 為了改良習知程序，控制模組106包含錯誤偵測模組130。錯誤偵測模組130可經組態以偵測一給定站108或製造系統102之節點處之一錯誤。例如，錯誤偵測模組130用作用於程序控制之一動態干預性方法之部分，其中接在引起經偵測損害之節點之後的各節點被編織成一最佳化問題(例如，一損害恢復問題)且經主動地控制以具現化該最佳化問題之一解決方案。在一些實施例中，此程序可即時或接近即時完成且係在各週期在進行中時而非在一給定週期之結束。

【0030】 為了理解由錯誤偵測模組130實施之一或多種技術，重要的係理解控制模組106如何定義一製造系統(例如，製造系統102)。可使用廣泛多種拓樸方案(包含回饋及前饋組織)定義一製造系統。在一些實施例

中，一製造系統F可定義為在一經前饋連結鏈中連接之標記為$1,\ldots,N$之一線性序列之n個處理節點(或站108)。例如：

$$F: \rightarrow 1 \rightarrow 2 \rightarrow \cdots \rightarrow i \rightarrow \cdots \rightarrow n$$

【0031】 類似地，在一些實施例中，一製造系統F可定義為標記為$1,\ldots,N$之一非線性序列之n個處理節點(或站108)。在一些實施例中，由各節點i完成之處理可具有兩個屬性分佈：一預期分佈Q_i；及一經觀察分佈P_i。Q_i可藉由μ_{Q_i}及σ_{Q_i}表徵。如果$Q_i = N(\mu_{Q_i}, \sigma_{q_i}^2)$，則$Q_i$可經完全表徵。$P_i$可藉由$\mu_{P_i}$及$\sigma_{P_i}$表徵。如果$P_i = N(\mu_{P_i}, \sigma_{P_i}^2)$，則$P_i$可經完全表徵。

【0032】 在一些實施例中，由節點i引起之損害可定義為P_i相對於Q_i之庫貝克-李柏(Kullback-Leibler)發散：

$$d_i = D_{KL}(P_i||Q_i) = \sum_{x \in X} P_i(x) \log\left(\frac{P_{i(x)}}{Q_i(x)}\right)$$

【0033】 在一些實施例中，損害可係累積的或跨F相加。例如：

$$d_f = \sum_{i=1}^{n} d_i$$

【0034】 返回參考錯誤偵測模組130，錯誤偵測模組130可經組態以偵測在製造系統102之一給定節點k處之損害或一錯誤。例如，如果錯誤偵測模組130偵測節點k已引起損害(即，已產生一經損害或經失真分佈)，則錯誤偵測模組130可採用自P_k取樣且產生自其流動之全部後續所得分佈$P_{k+1},\ldots,P_n$，使得剩餘累積損害$d_{k+1},\ldots,d_k$可減少或最小化之一控制策略。因此，可將錯誤偵測模組130之損害恢復問題公式化為：

$$\underset{\{P_{k+1},\ldots,P_n\}}{\operatorname{argmin}} \left\{ \sum_{i=k+1}^{n} D_{KL}(P_i||Q_i) \right\}$$

【0035】 在一些實施例中，錯誤偵測模組130可實施用以識別或校

正在一給定節點處偵測到之損害的一或多種技術。在一些實施例中，錯誤偵測模組130可使用一卡爾曼濾波器132以偵測一給定處理節點處之損害或錯誤。在一些實施例中，錯誤偵測模組130可包含用以偵測一給定處理節點處之損害或錯誤之一自動編碼器134。在一些實施例中，錯誤偵測模組130可使用機器學習模組136深度強化學習技術以偵測一給定處理節點處之損害或錯誤，且校正由下游節點或站108處之損害或錯誤引起之經偵測變動。在一些實施例中，錯誤偵測模組130可使用卡爾曼濾波器132、一自動編碼器134或機器學習模組136之一或多者以偵測一給定處理節點處之損害或錯誤，及/或校正由下游節點或站108處之損害或錯誤引起之經偵測變動。

【0036】 在一些實施例中，錯誤偵測模組130可實施卡爾曼濾波器132以偵測一處理節點處之錯誤。為了一般化上文之分佈描述，即，d_i，可將一單輸入單輸出系統以一狀態空間形式建立為：

$$\dot{\vec{x}}_i = A_i\vec{x}_i + B_i u_{\varepsilon,i}(t)$$

$$y_i(t) = C_i^T\vec{x}_i$$

針對經定義為系統之任意狀態之 $\vec{x}_i$，經定義為系統之輸出之y，且A, B, C可係定義基礎動力學之常微分方程式的系統矩陣。此系統之輸入u_ε可係藉由以下項定義之一有雜訊輸入信號：

$$u_{\varepsilon,i} = u_i(t) + \varepsilon_t$$

其中ϵ_t可係由$\varepsilon_t \sim \mathcal{N}(\mu_{\varepsilon,i}, R_i)$貢獻之相加雜訊。在一些實施例中，經觀察輸出$y_V$可係系統輸出之一函數，如：

$$y_{V,i} = y_i(t) + \mathcal{V}_t$$

針對一類似地有雜訊的信號量測，其中 $\mathcal{V}_t \sim \mathcal{N}(\mu_{V,i}, \sigma_{V,i}^2)$。在一些實施例

中，此標記可係藉由針對一程序之一給定節點i建立$y_{v,i}\sim Q_i$來協調。在一不受影響系統中，雜訊貢獻之均值可係零，使得$\mu_{\varepsilon,i}=\mu_{v,i}=0$。然而，在一惡意網路攻擊中，偏差可顯現為一非零均值輸入雜訊。

【0037】 一般言之，一卡爾曼濾波器132可依賴於零均值雜訊；然而，在一惡意網路攻擊之情況中，一輸入指令之一偏移可顯現為一非零均值相加雜訊。因而，可針對以下項之經假定非時變系統來解釋一卡爾曼濾波器132：

$$\dot{\vec{x}}_i = A_i\vec{x}_i + B_i u_{\varepsilon,i}(t)$$

$$y_i(t) = C_i^T\vec{x}_i$$

【0038】 在一些實施例中，卡爾曼濾波器132可使用一節點或一程序之輸出$y_{v,i}(t)$之量測及正準未觸碰輸入指令$u_i(t)$建構。如果正確地校準程序，則一站108或節點之輸入/輸出感測器量測應具有零均值雜訊。然而，在一惡意網路攻擊之情況中，將存在一非零偏差。

【0039】 在一些實施例中，卡爾曼濾波器132可理解為：

$$\bar{\vec{x}}_{i,k} = A_i\hat{\vec{x}}_{i,k-1} + B_i u_{i,k}$$

$$\bar{\Sigma}_{i,k} = A_i\Sigma_{i,k-1}A_i^T + R_i$$

$$K_{i,k} = \bar{\Sigma}_{i,k}C_i\left(C_i^T\bar{\Sigma}_{i,k}C_i + \sigma_{v,i}^2\right)^{-1}$$

$$\hat{\vec{x}}_{i,k} = \bar{\vec{x}}_{i,k} + K_{i,k}\left(y_{v,i,k} - C_i^T\bar{\vec{x}}_{i,k}\right)$$

$$\Sigma_{i,k} = \left(I - K_{i,k}C_i^T\right)\bar{\Sigma}_{i,k}$$

針對一處理節點i之第k樣本，其中$\bar{}$可係量測更新標記，$\Sigma_{i,k}$可係狀態預測之協方差，R_i可係輸入雜訊之協方差，ε_t及$K_{i,k}$可係卡爾曼增益。使用一足夠大樣本，創新分佈$\tilde{y}_{i,k} = y_{v,i,k} - C_i^T\bar{\vec{x}}_{i,k}$應係$\tilde{y}_{i,k}\sim\mathcal{N}\left(\mu_{\tilde{y},i,k}=0, C_i^T\Sigma_{i,k|k-1}C_i\right)$。然而，使用一惡意網路攻擊$\mu_{\tilde{y},i,k}\neq 0$，但此可在最小樣本內自然地發生。一旦可滿足一樣本臨限值$k > k_{min}$，便可

針對$\tilde{y}_{i,k} > \gamma_i$建立一警報，其中$\gamma_i$可針對一處理節點經調諧。如果創新錯誤非零且高於臨限值γ_i，則錯誤偵測模組130可判定一惡意網路攻擊可能正在發生。

【0040】 圖2係繪示根據例示性實施例之實施卡爾曼濾波器132之一單輸入單輸出系統(下文為「系統200」)之架構的一方塊圖。

【0041】 如展示，系統200可包含一控制器202 (例如，$C(s)$)、一設備204 (例如，$G(s)$)、一量測206 (例如，$H(s)$)、一攻擊208 (例如，$A(s)$)及卡爾曼濾波器132 (例如，KF)。在一些實施例中，系統200可包含一第二控制器202。在一些實施例中，控制器202、設備204及量測206可表示節點控制之基本組成部分，而卡爾曼濾波器132產生一創新錯誤。

【0042】 在一些實施例(諸如圖2中展示之實施例)中，一雙控制器可用作卡爾曼濾波器132之一無偏差參考。

【0043】 返回參考圖1，在一些實施例中，錯誤偵測模組130可使用一自動編碼器134以偵測對應於一網路攻擊之異常。針對一序列經量測輸出$\vec{y}_{v,i}$，可具現化一非監督式自動編碼器訓練以將輸出觀察之一熵映射至一參數集θ_{AE}上，使得

$$\hat{\vec{y}}_{v,i} = f(\vec{y}_{v,i}, \theta_{AE})$$

【0044】 在一些實施例中，自動編碼器134之錯誤可定義為：

$$\tilde{\vec{y}}_{v,i} = \vec{y}_{v,i} - \hat{\vec{y}}_{v,i}$$

且針對$\tilde{\vec{y}}_{v,i} \sim \mathcal{N}(\mu_{\tilde{y},i}, \Sigma_{\tilde{y},i})$之一正常操作，其中$\mu_{\tilde{y}}$及$\Sigma_{\tilde{y},i}$可以最大可能性擬合至分佈。隨後，針對一序列之一異常分數a_i可定義為：

$$a_i = \mathcal{A}\left(\tilde{\vec{y}}_{v,i,\mu_{\tilde{y},i}}, \Sigma_{\tilde{y},i}\right)$$

$$= \left(\tilde{\vec{y}}_{v,i} - \mu_{\tilde{y},i}\right)^T \Sigma_{\tilde{y},i}^{-1} \left(\tilde{\vec{y}}_{v,i} - \mu_{\tilde{y},i}\right)$$

【0045】 類似於卡爾曼濾波器132，當異常分數$a_i > \gamma_i$時，錯誤偵測模組130可使用自動編碼器134偵測一異常。

【0046】 圖3係繪示根據一些實施例之實施自動編碼器134之一系統300之架構的一方塊圖。如展示，系統300可包含一控制器302 (例如，$C(s)$)、一設備304 (例如，$G(s)$)、一量測306 (例如，$H(s)$)、一攻擊308 (例如，$A(s)$)、自動編碼器134 (例如，AE)及一警報312 (例如，$\mathcal{A}$)。控制器302、設備304及量測306可表示節點控制之基本組成部分，而自動編碼器134可偵測錯誤。在一些實施例中，錯誤偵測模組130可基於一足夠異常分數觸發一警報312。

【0047】 返回參考圖1，在一些實施例中，錯誤偵測模組130可使用一或多個深度強化學習技術以識別對應於一網路攻擊之處理中之一錯誤或異常。如上文提及，給定損害之定義d_i，可針對設法建構一組分佈$P_{k+1},\ldots,P_n$之一強化學習代理器公式化一經延遲獎勵函數以求解以下損害恢復問題

$$\underset{\{P_{k+1},\ldots,P_n\}}{\operatorname{argmin}}\left\{\sum_{i=k+1}^{n} D_{KL}(P_i||Q_i)\right\}$$

針對

$$r_i(\vec{\alpha}_i^j) = P_i(\vec{\alpha}_i^j)\log\frac{P_i(\vec{\alpha}_i^j)}{Q_i(\vec{\alpha}_i^j)}$$

此係透過其動作$\vec{\alpha}_i^j$，針對$i = k+1,\ldots,n$，完成某一組迭代$j = 1,\ldots,m$：

$$R(\vec{\alpha}^j) = \sum_{i=k+1}^{n} r_i(\vec{\alpha}_i^j)$$

【0048】 在一些實施例中，錯誤偵測模組130可在一行動者關鍵模

態中訓練一代理器，使得給定一程序之第i節點之第k樣本之一狀態$\vec{x}_{i,k}$，一個網路可產生一動作$\alpha_{i,k}$，且另一網路可產生經由參數$\theta_{Q,i}$學習之Q值$Q_{i,k}^{\pi}(\vec{x}_{i,k},\alpha_{i,k}|\theta_{Q,i})$之一預測，其中$\pi_i(\vec{x}_{i,k},\theta_{\pi,i})$可係經由參數$\theta_{\pi,i}$學習之一原則。在一些實施例中，可使用一貝爾曼(Bellman)公式計算獎勵使得：

$$Q_i(\vec{x}_{i,k},\alpha_{i,k}) = r_{i,k} + \gamma_i Q_i(\vec{x}_{i,k+1},\pi_i(\vec{x}_{i,k+1})|\theta_{\pi,i})$$

【0049】在一些實施例中，與強化學習技術相關聯之更新定律可係：

$$-\nabla_{\theta_{\pi j}} J = \mathbb{E}_{\alpha_{i,k}\sim p}[\nabla_{\alpha_i} Q_i(\vec{x}_{i,k},\alpha_{i,k}|\theta_{\pi,i})]$$

【0050】在一些實施例中，更新定律可減小或最小化Q值，藉此最小化損害，且可顯現於目標為將分佈返回至其正準形狀之動作中。在一些實施例中，一動作之一個公式可係：

【0051】在一些實施例中，一動作之一公式可係：

$$u_{i,k} = \alpha_{i,k} u_{i,k}^{*},$$

其中$u_{i,k}$可係$\dot{\vec{x}}_i = A_i\vec{x}_i + B_i u_{\varepsilon,i}(t)$及$y_i(t) = C_i^T\vec{x}_i$之輸入，$\alpha_{i,k}$可係一指令修改器，且$u_{i,k}^{*}$可係針對節點$i$之一特定樣本$k$讀取之指令。如果此指令被損壞，且該損壞以各種狀態顯現，則原則$\pi_{i,k}$可行動以校正其。

【0052】藉由利用一強化學習方法，錯誤偵測模組130可藉由將基於程序之惡意網路攻擊統整成標稱程序變動而解決系統安全性之一新方式且提供該等變動之直接控制及校正。方法不僅僅係偵測或被動防止之一方法；實情係，可假定一網路攻擊顯現為一常規(例如，可能)系統變動，諸如機器超出規範或原始材料存料超出嚴格規範。

【0053】圖4係繪示根據一些實施例之使用機器學習模組136實施一強化學習方法之一系統400之架構的一方塊圖。如展示，系統400可代表

一多節點系統$i = 0, \ldots, N$。針對各節點i，可存在一控制器402_0、402_1及402_N（例如，$C_0(s), C_i(s), \ldots C_N(s)$）、一設備$404_0$、$404_i$及$404_N$（例如，$G_0(s), G_i(s), G_N(s)$）及一量測$406_0$、$406_i$及$406_N$（例如，$H_0(s), H_i(s), H_N(s)$）。節點可一起嵌入由系統400在自資料儲存器408（例如，γ）取樣之時間k, S_k之狀態管控之一原則學習回饋迴路中，且原則獲取當前狀態410作為輸入$\pi(S_k)$。可針對一單一節點i藉由區塊$A(s)$表示一攻擊412。

【0054】 在一些實施例中，為了識別所採取之用以校正由一網路攻擊引起之錯誤之一組動作，可將針對時間樣本k之狀態S_k輸入至一非線性濾波器，可選取該非線性濾波器之權重以在給定一經觀察假影或分量之情況下最小化一時間樣本$k + n$之後續損害。在一些實施例中，濾波器之輸出可係修改指定程序設定點或控制值之一純量或向量。自狀態至動作之變換可稱為原則。

【0055】 圖5係繪示根據例示性實施例之管理對一製造程序之一網路攻擊之一方法500之一流程圖。方法500可作為步驟502開始。

【0056】 在步驟502，控制模組106可自製造系統102之一站108接收控制值。在一些實施例中，控制模組106可自與一給定站108相關聯之一程序控制器接收控制值。程序控制器可通常經程式化以控制站108之操作。例示性控制值可包含(但不限於)：速度、溫度、壓力、真空、旋轉、電流、電壓、功率、黏度、在站處使用之材料/資源、通量率、中斷時間、有毒煙霧及類似者。更一般言之，一控制值可係指站108之一屬性，而非由站108處理之一組件之一屬性。

【0057】 在步驟504，控制模組106可基於自站108接收之控制值判定一網路攻擊存在。例如，在一些實施例中，錯誤偵測模組130可使用卡

爾曼濾波器132以在給定控制值之情況下產生站108之一異常分數。例如，如果異常分數大於一預定義臨限值，則控制模組106可判定一網路攻擊當前在進行中。在另一實例中，錯誤偵測模組130可使用自動編碼器134以在給定控制值之情況下產生站108之一異常分數。例如，如果異常分數大於一預定義臨限值，則控制模組106可判定一網路攻擊當前在進行中。在另一實例中，錯誤偵測模組130可使用機器學習模組136以預測對應於站108之一Q值。例如，如果Q值在可接受值之一範圍之外，則控制模組106可判定一網路攻擊當前在進行中。

【0058】 在一些實施例中，方法500可包含步驟506。在步驟506，回應於判定一網路攻擊正在發生，控制模組106可觸發一警告或警報。在一些實施例中，警告或警報可係對監督製造系統102之一使用者之一通知。在一些實施例中，警告或警報可係停止或終止製造系統102之各站108_1至108_n之處理之一信號。

【0059】 在一些實施例中，方法500可包含步驟508至510。在步驟508，回應於判定一網路攻擊正在發生，控制模組106可產生用以校正由網路攻擊引起之損害之一或多個動作。例如，錯誤偵測模組130可在一行動者關鍵模態中訓練一代理器，使得給定一程序之第i節點之第k樣本之一狀態$\vec{x}_{i,k}$，一個網路可產生一動作$\alpha_{i,k}$，且另一網路可產生透過參數$\theta_{Q,i}$學習之Q值$Q_{i,k}^{\pi}(\vec{x}_{i,k},\alpha_{i,k}|\theta_{Q,i})$之一預測，其中$\pi_i(\vec{x}_{i,k},\theta_{\pi,i})$可係透過參數$\theta_{\pi,i}$學習之一原則。在一些實施例中，可使用一貝爾曼公式計算獎勵使得：

$$Q_i(\vec{x}_{i,k},\alpha_{i,k}) = r_{i,k} + \gamma_i Q_i(\vec{x}_{i,k+1},\pi_i(\vec{x}_{i,k+1})|\theta_{\pi,i})$$

【0060】 在一些實施例中，與強化學習技術相關聯之更新定律可係：

$$-\nabla_{\theta_{\pi,i}} J = \mathbb{E}_{\alpha_{i,k}\sim p}\left[\nabla_{\alpha_i} Q_i\left(\vec{x}_{i,k}, \alpha_{i,k} \middle| \theta_{\pi,i}\right)\right]$$

【0061】 在一些實施例中，更新定律可減小或最小化Q值，藉此最小化損害，且可顯現於目標為將分佈返回至其正準形狀之動作中。

【0062】 在一些實施例中，一動作之一公式可係：

$$u_{i,k} = \alpha_{i,k} u^*_{i,k'}$$

其中 $u_{i,k}$ 可係 $\dot{\vec{x}}_i = A_i\vec{x}_i + B_i u_{\varepsilon,i}(t)$ 及 $y_i(t) = C_i^T\vec{x}_i$ 之輸入，$\alpha_{i,k}$ 可係一指令修改器，且 $u^*_{i,k}$ 可係針對節點 i 之一特定樣本 k 讀取之指令。如果此指令被損壞，且該損壞以各種狀態顯現，則原則 $\pi_{i,k}$ 可行動以校正其。

【0063】 在步驟510，控制模組106可為下游站108提供由機器學習模組136產生之經更新動作。在一些實施例中，控制模組106可將經更新指令傳輸至各下游站108之程序控制器。

【0064】 圖6A繪示根據例示性實施例之一系統匯流排運算系統架構600。系統600之一或多個組件可使用一匯流排605彼此電通信。系統600可包含一處理器(例如，一或多個CPU、GPU或其他類型之處理器) 610及將各種系統組件(包含系統記憶體615，諸如唯讀記憶體(ROM) 620及隨機存取記憶體(RAM) 625)耦合至處理器610之一系統匯流排605。系統600可包含與處理器610直接連接、緊密接近處理器610或作為處理器610之部分整合之高速記憶體之一快取區。系統600可自記憶體615及/或儲存裝置630複製資料至快取區612用於藉由處理器610進行快速存取。以此方式，快取區612可提供避免處理器610在等待資料時延遲之一效能增強。此等及其他模組可控制或經組態以控制處理器610以執行各種動作。亦可用其他系統記憶體615以供使用。記憶體615可包含具有不同效能特性之多個不同類型之記憶體。處理器610可代表一單一處理器或多個處理器。處理器

610可包含一通用處理器或一硬體模組或軟體模組(諸如儲存於記憶體裝置630中之經組態以控制處理器610之服務1 632、服務2 634及服務3 636)以及其中軟體指令併入實際處理器設計中之一專用處理器之一或多者。處理器610可基本上係含有多個核心或處理器、一匯流排、記憶體控制器、快取區等之一完全自含型運算系統。一多核心處理器可係對稱或不對稱的。

【0065】 為實現與運算裝置600之使用者互動，一輸入裝置645可係任何數目個輸入機構，諸如用於語音之一麥克風、用於手勢或圖形輸入之一觸敏螢幕、鍵盤、滑鼠、運動輸入、話音等。一輸出裝置635亦可為熟習此項技術者已知之數個輸出機構中之一或多者。在一些例項中，多模式系統可使一使用者能夠提供多個類型之輸入以與運算裝置600通信。通信介面640一般可控管及管理使用者輸入及系統輸出。在任何特定硬體配置上操作係沒有限制的，且因此，此處之基本特徵在其等被開發時可容易由經改良硬體或韌體配置取代。

【0066】 儲存裝置630可係一非揮發性記憶體，且可為一硬碟或可儲存可藉由一電腦存取之資料之其他類型的電腦可讀媒體，諸如盒式磁帶、快閃記憶卡、固態記憶體裝置、數位多功能光碟、匣、隨機存取記憶體(RAM) 625、唯讀記憶體(ROM) 620，及其等之混合。

【0067】 儲存裝置630可包含用於控制處理器610之服務632、634及636。審慎考慮其他硬體或軟體模組。儲存裝置630可經連接至系統匯流排605。在一個態樣中，執行一特定功能之一硬體模組可包含經儲存於與必要硬體組件(諸如處理器610、匯流排605、顯示器635等)連接之一電腦可讀媒體中以實行功能的軟體組件。

【0068】 圖6B繪示根據例示性實施例之具有一晶片組架構之一電腦

系統650。電腦系統650可係可用於實施所揭示技術之電腦硬體、軟體及韌體之一實例。系統650可包含代表能夠執行經組態以執行經識別運算之軟體、韌體及硬體之任何數目個實體及/或邏輯相異資源的一或多個處理器655。一或多個處理器655可與一晶片組660通信，該晶片組660可控制至一或多個處理器655之輸入及來自一或多個處理器655之輸出。在此實例中，晶片組660將資訊輸出至輸出665 (諸如一顯示器)，且可讀取資訊且將資訊寫入至儲存裝置670，該儲存裝置670可包含(例如)磁性媒體及固態媒體。晶片組660亦可自RAM 675讀取資料，且將資料寫入至RAM 675。可提供用於與各種使用者介面組件685介接之一橋680，用於與晶片組660介接。此等使用者介面組件685可包含一鍵盤、一麥克風、觸控偵測及處理電路、一指標裝置(諸如一滑鼠)等。一般言之，至系統650之輸入可來自各種源(機器產生及/或人為產生)之任何者。

【0069】 晶片組660亦可與可具有不同實體介面之一或多個通信介面690介接。此等通信介面可包含用於有線及無線區域網路、用於寬頻無線網路以及個人區域網路之介面。用於產生、顯示且使用本文中揭示之GUI之方法的一些應用可包含經由實體介面接收有序資料集或藉由機器自身憑藉分析經儲存於儲存器670或675中之資料的一或多個處理器655來產生。此外，機器可自一使用者透過使用者介面組件685接收輸入，且藉由使用一或多個處理器655解譯此等輸入來執行適當功能(諸如瀏覽功能)。

【0070】 可瞭解，例示性系統600及650可具有一個以上處理器610或係經網路連結在一起以提供更大處理能力之運算裝置之一群組或叢集之部分。

【0071】 雖然上文係關於本文中描述之實施例，但可設想其他及進

一步實施例而不脫離其基本範疇。例如，本發明之態樣可實施於硬體或軟體或硬體及軟體之一組合中。本文中描述之一項實施例可實施為用於與一電腦系統一起使用之一程式產品。程式產品之(若干)程式定義實施例(包含本文中描述之方法)之功能且可含有在各種電腦可讀儲存媒體上。闡釋性電腦可讀儲存媒體包含(但不限於)：(i)資訊永久地儲存於其上之不可寫入儲存媒體(例如，一電腦內之唯讀記憶體(ROM)裝置，諸如可由一CD-ROM光碟機讀取之CD-ROM光碟，快閃記憶體、ROM晶片，或任何類型之固態非揮發性記憶體)；及(ii)其上儲存可更改資訊之可寫入儲存媒體(例如，一軟式磁碟機內之軟碟或硬碟機或任何類型之固態隨機存取記憶體)。此等電腦可讀儲存媒體在攜載引導所揭示實施例之功能之電腦可讀指令時係本發明之實施例。

【0072】 熟習此項技術者將瞭解，前述實例係例示性且非限制性的。旨在其全部排列、增強、等效物及改良在熟習此項技術者在閱讀說明書且研究圖式之後顯而易見且包含於本發明之真實精神及範疇內。因此，旨在以下隨附發明申請專利範圍包含如落在其他教示之真實精神及範疇內之全部此等修改、排列及等效物。

【符號說明】

【0073】

100: 製造環境

102: 製造系統

104: 監測平台

106: 控制模組

108_1至108_n: 站

114_1至114_n: 程序控制器

116_1至116_n: 控制邏輯

132: 卡爾曼濾波器

134: 自動編碼器

136: 機器學習模組

200: 系統

202: 控制器/第二控制器

204: 設備

206: 量測

208: 攻擊

300: 系統

302: 控制器

304: 設備

306: 量測

308: 攻擊

312: 警報

402_0: 控制器

402_i: 控制器

402_N: 控制器

404_0: 設備

404_i: 設備

404_N: 設備

406_0: 量測

406_i: 量測

406_N: 量測

408: 資料儲存器

410: 當前狀態

412: 攻擊

500: 方法

502: 步驟

504: 步驟

506: 步驟

508: 步驟

510: 步驟

600: 系統匯流排運算系統架構

605: 匯流排

610: 處理器

612: 快取區

615: 系統記憶體

620: 唯讀記憶體(ROM)

625: 隨機存取記憶體(RAM)

630: 儲存裝置

632: 服務1

634: 服務2

635: 輸出裝置

636: 服務3

640: 通信介面

645: 輸入裝置

650: 電腦系統

655: 處理器

660: 晶片組

665: 輸出

670: 儲存裝置

675: 隨機存取記憶體(RAM)

680: 橋

685: 使用者介面組件

690: 通信介面

【發明申請專利範圍】

【請求項1】

一種用於判定網路攻擊及產生警告之製造系統，其包括：

一或多個站，各站經組態以針對一組件執行一多步驟製造程序中之至少一個步驟；

一監測平台，其經組態以監測該組件在整個該多步驟製造程序之進展；及

一控制模組，其經組態以偵測對該製造系統之一網路攻擊，該控制模組經組態以執行操作，該等操作包括：

接收該一或多個站之一第一站之控制值，該等控制值包括該第一處理站之屬性；

藉由以下動作，使用一或多個機器學習演算法，基於該第一站之該等控制值來判定存在一網路攻擊：

基於該等控制值來產生該第一站之一異常分數，及判定該異常分數超過指示一網路攻擊之一臨限值；及

基於該判定，產生一警告以終止該組件之處理；

藉由判定一組經修改控制值，產生用以校正由該網路攻擊引起之錯誤之一組動作以最小化該網路攻擊造成之損害；及

提供該組動作至與該製造系統之至少一下游站相關聯之至少一程序控制器。

【請求項2】

如請求項1之製造系統，其中該一或多個機器學習演算法包括一卡爾曼濾波器。

【請求項3】

如請求項2之製造系統，其中基於該等控制值來產生該第一站之該異常分數，包括：

使用該卡爾曼濾波器，基於該等控制值來產生該第一站之該異常分數。

【請求項4】

如請求項1之製造系統，其中該一或多個機器學習演算法包括一自動編碼器。

【請求項5】

如請求項4之製造系統，其中基於該等控制值來產生該第一站之該異常分數包括：

使用該自動編碼器，基於該等控制值來產生該第一站之該異常分數。

【請求項6】

如請求項1之製造系統，其中該一或多個機器學習演算法包括一深度學習演算法。

【請求項7】

如請求項6之製造系統，其中使用該一或多個機器學習演算法基於該第一站之該等控制值來判定存在一網路攻擊進一步包括：

基於該一或多個控制值來產生該組件之一經預測品質度量；及

判定該經預測品質度量落在可接受值之一範圍之外。

【請求項8】

一種用於判定網路攻擊及產生警告之電腦實施方法，其包括：

藉由一運算系統接收經組態以處理一組件之一製造系統的一或多個站之一第一站的控制值，該等控制值包括該第一站的屬性；

藉由以下動作，藉由該運算系統，使用一或多個機器學習演算法，基於該第一站之該等控制值來判定存在一網路攻擊：

基於該等控制值來產生該第一站之一異常分數，及判定該異常分數超過指示該網路攻擊之一臨限值；及

藉由該運算系統，基於該判定來產生一警告以終止該組件之處理；

藉由該運算系統，藉由判定一組經修改控制值來產生用以校正由該網路攻擊引起之錯誤之一組動作以最小化該網路攻擊造成之損害；及

藉由該運算系統，使該製造系統之至少一下游站，藉由使與該至少一下游站相關聯之至少一程序控制器基於該組經修改控制值調整該至少一下游站之一組屬性，執行該組動作。

【請求項9】

如請求項8之電腦實施方法，其中該一或多個機器學習演算法包括一卡爾曼濾波器。

【請求項10】

如請求項9之電腦實施方法，其中基於該等控制值來產生該第一站之該異常分數，包括：

使用該卡爾曼濾波器，基於該等控制值來產生該第一站之該異常分數。

【請求項11】

如請求項8之電腦實施方法，其中該一或多個機器學習演算法包括一自動編碼器。

【請求項12】

如請求項11之電腦實施方法，其中基於該等控制值來產生該第一站之該異常分數，包括：

使用該自動編碼器，基於該等控制值來產生該第一站之該異常分數。

【請求項13】

如請求項8之電腦實施方法，其中該一或多個機器學習演算法包括一深度學習演算法。

【請求項14】

如請求項13之電腦實施方法，其中使用該一或多個機器學習演算法基於該第一站之該等控制值來判定存在一網路攻擊進一步包括：

基於該一或多個控制值來產生該組件之一經預測品質度量；及

判定該經預測品質度量落在可接受值之一範圍之外。

【請求項15】

一種用於判定網路攻擊及產生警告之製造系統，其包括：

一或多個站，各站經組態以針對一組件執行一多步驟製造程序中之至少一個步驟；

一控制模組，其經組態以偵測對該製造系統之一網路攻擊，該控制模組經組態以執行操作，該等操作包括：

接收該一或多個站之一第一站之控制值，該等控制值包括該第一站之屬性；

使用一或多個機器學習演算法，基於該第一站之該等控制值來判定存在一網路攻擊；

基於該判定，產生一警告以終止該組件之處理；

使用一或多個第二機器學習演算法，藉由判定一組經修改控制值來產生用以校正由該網路攻擊引起之錯誤之一組動作以最小化該網路攻擊造成之損害；及

藉由使與至少一下游站相關聯之至少一程序控制器基於該組經修改控制值調整該至少一下游站之一組屬性，使該製造系統之該至少一下游站執行該組動作。

【請求項16】

如請求項15之製造系統，其中該一或多個機器學習演算法包括一卡爾曼濾波器，且該一或多個第二機器學習演算法包括一深度學習演算法。

【請求項17】

如請求項16之製造系統，其中使用該一或多個機器學習演算法基於該第一站之該等控制值來判定存在一網路攻擊包括：

使用該卡爾曼濾波器，基於該等控制值來產生該第一站之一異常分數；及

判定該異常分數超過指示一網路攻擊之一臨限值。

【請求項18】

如請求項15之製造系統，其中該一或多個機器學習演算法包括一自動編碼器。

【請求項19】

如請求項18之製造系統，其中使用該一或多個機器學習演算法基於該第一站之該等控制值來判定存在一網路攻擊包括：

使用該自動編碼器，基於該等控制值來產生該第一站之一異常分

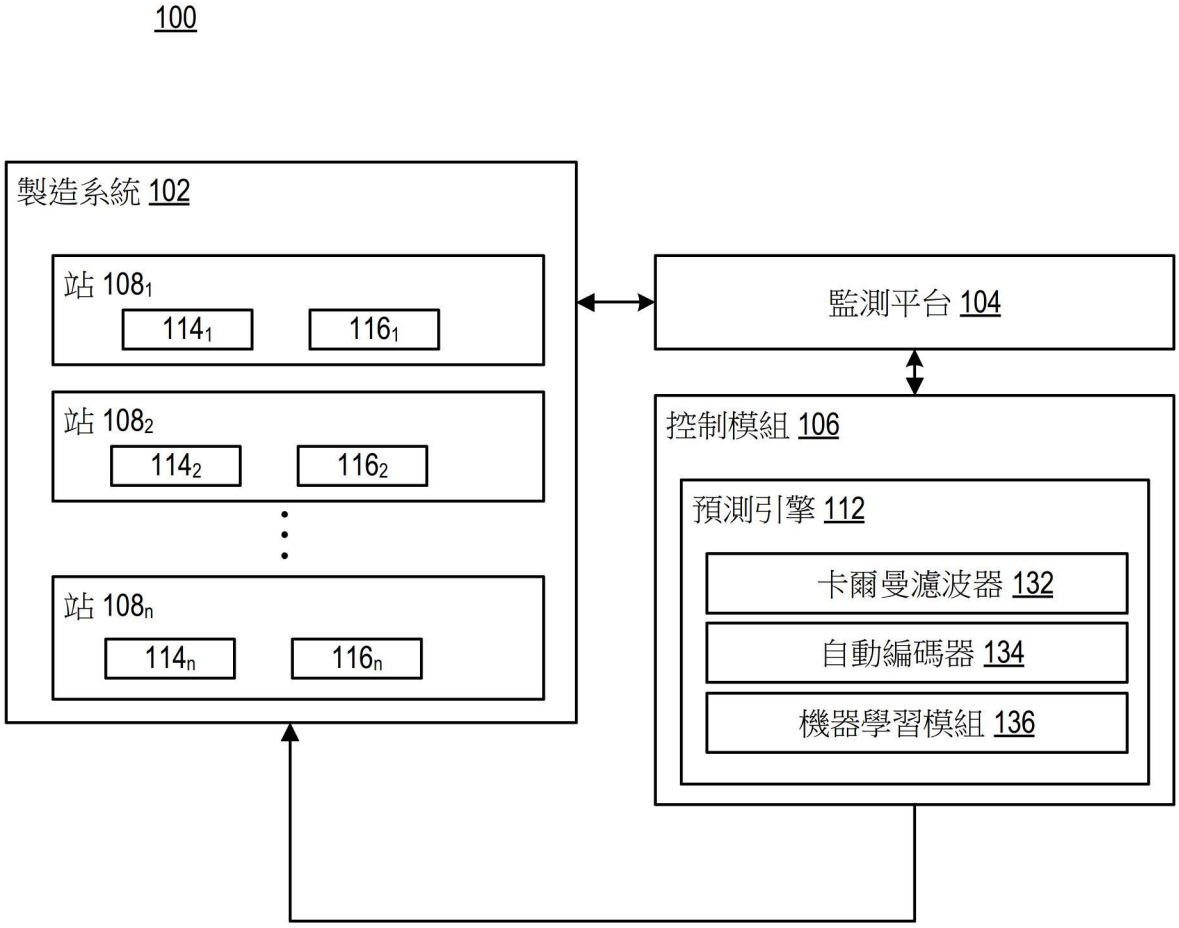
數；及

判定該異常分數超過指示一網路攻擊之一臨限值。

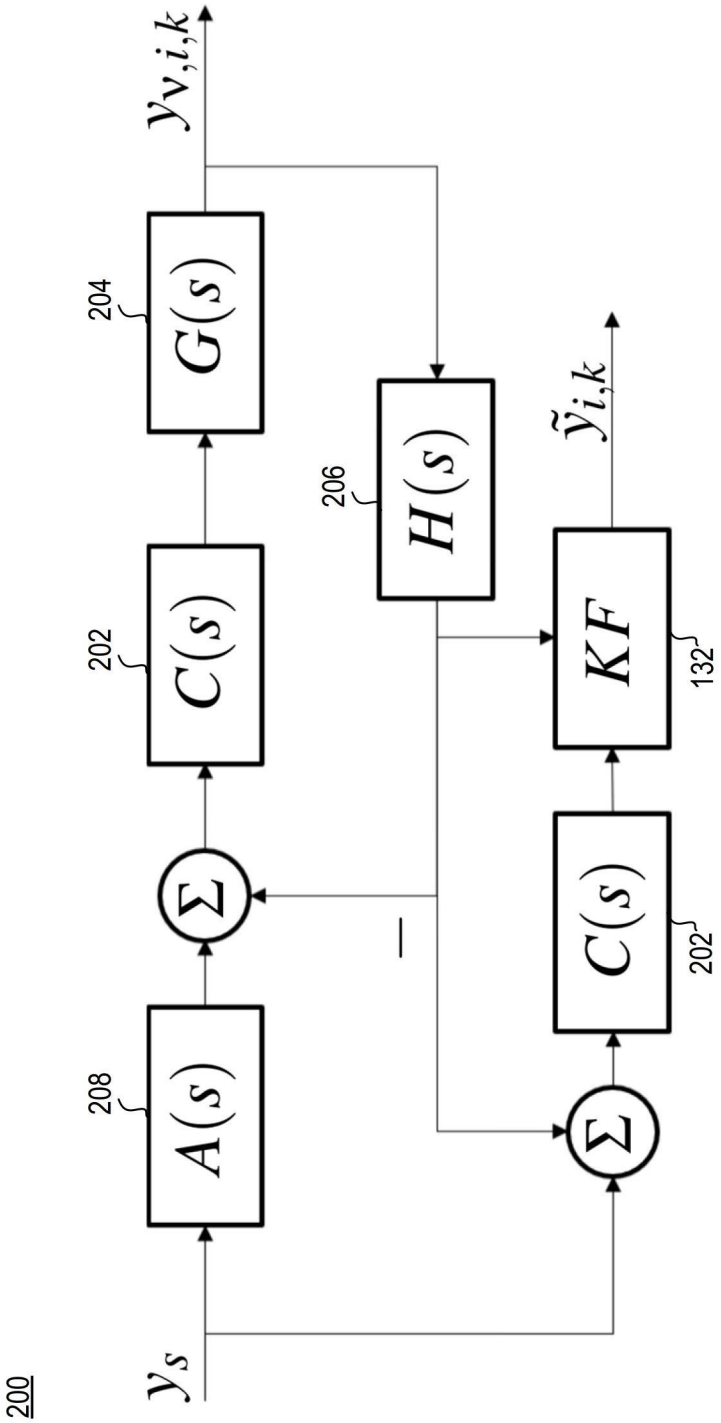
【請求項20】

如請求項15之製造系統，其中該一或多個機器學習演算法包括一深度學習演算法。

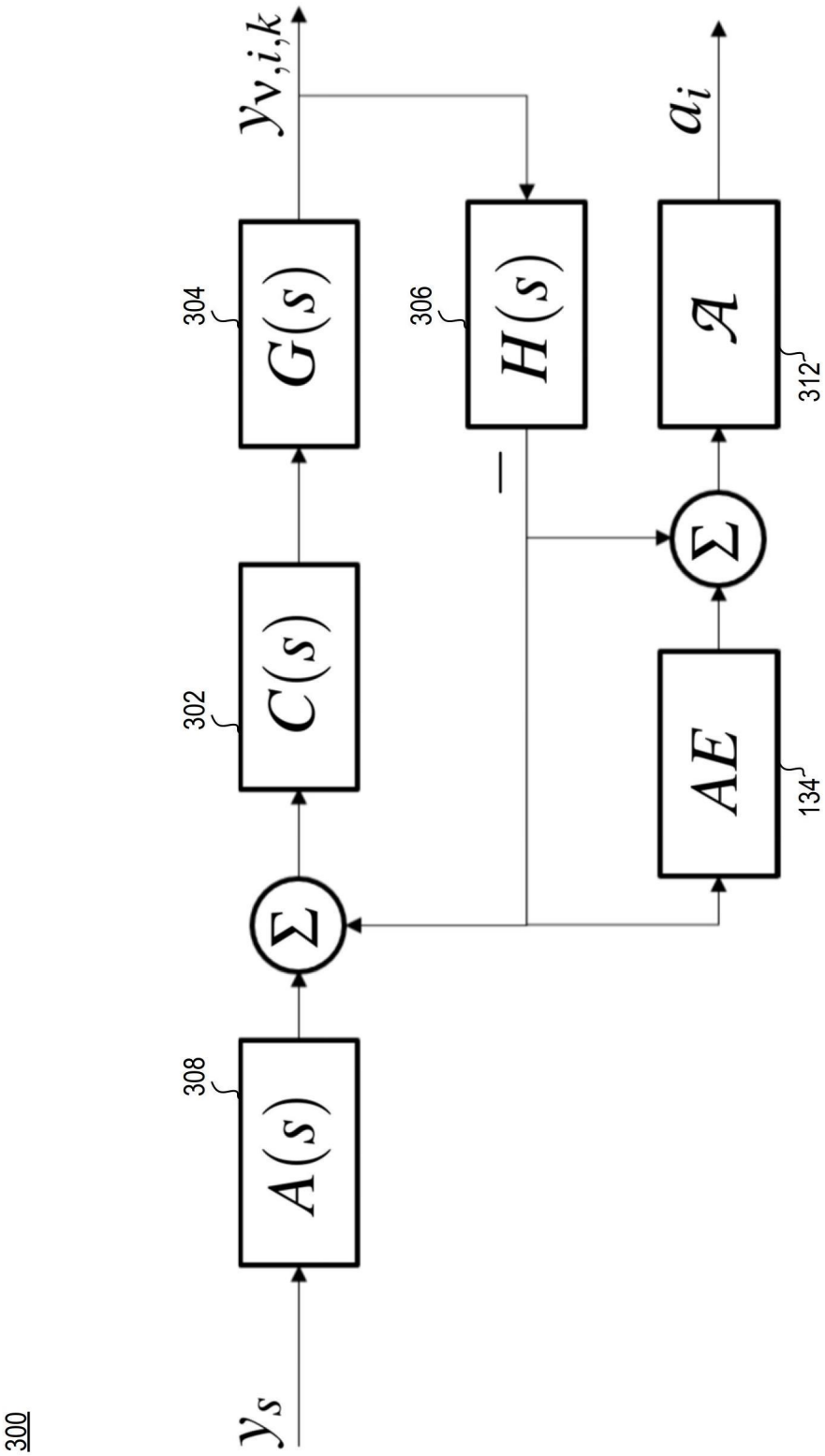
【發明圖式】


100
製造系統 102
站 108_1
114_1
116_1
站 108_2
114_2
116_2
站 108_n
114_n
116_n
監測平台 104
控制模組 106
預測引擎 112
卡爾曼濾波器 132
自動編碼器 134
機器學習模組 136

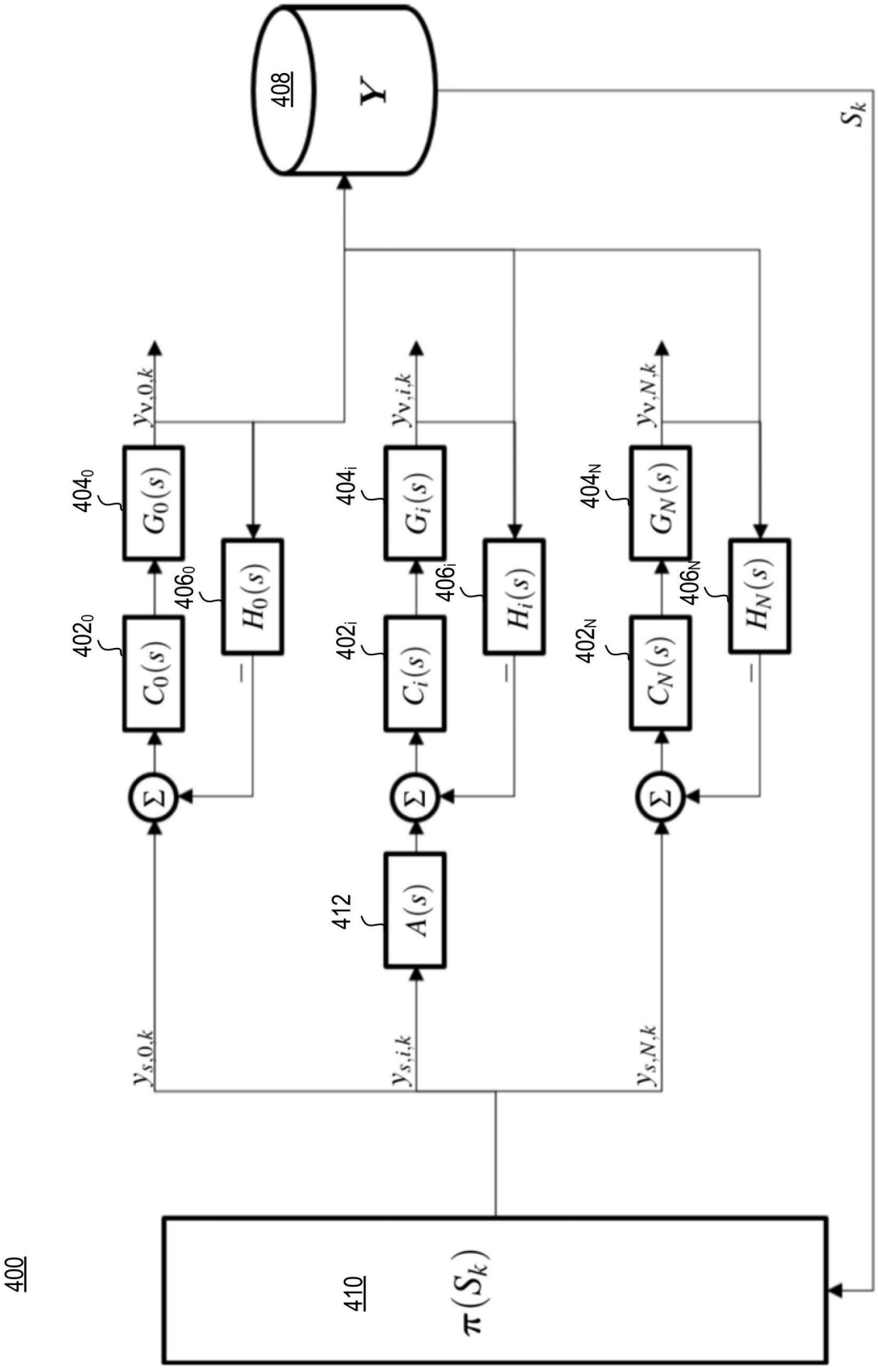
【圖1】


200
y_s
208
$A(s)$
202
$C(s)$
Σ
$-$
202
$C(s)$
204
$G(s)$
206
$H(s)$
Σ
KF
132
$\tilde{y}_{i,k}$
$y_{v,i,k}$

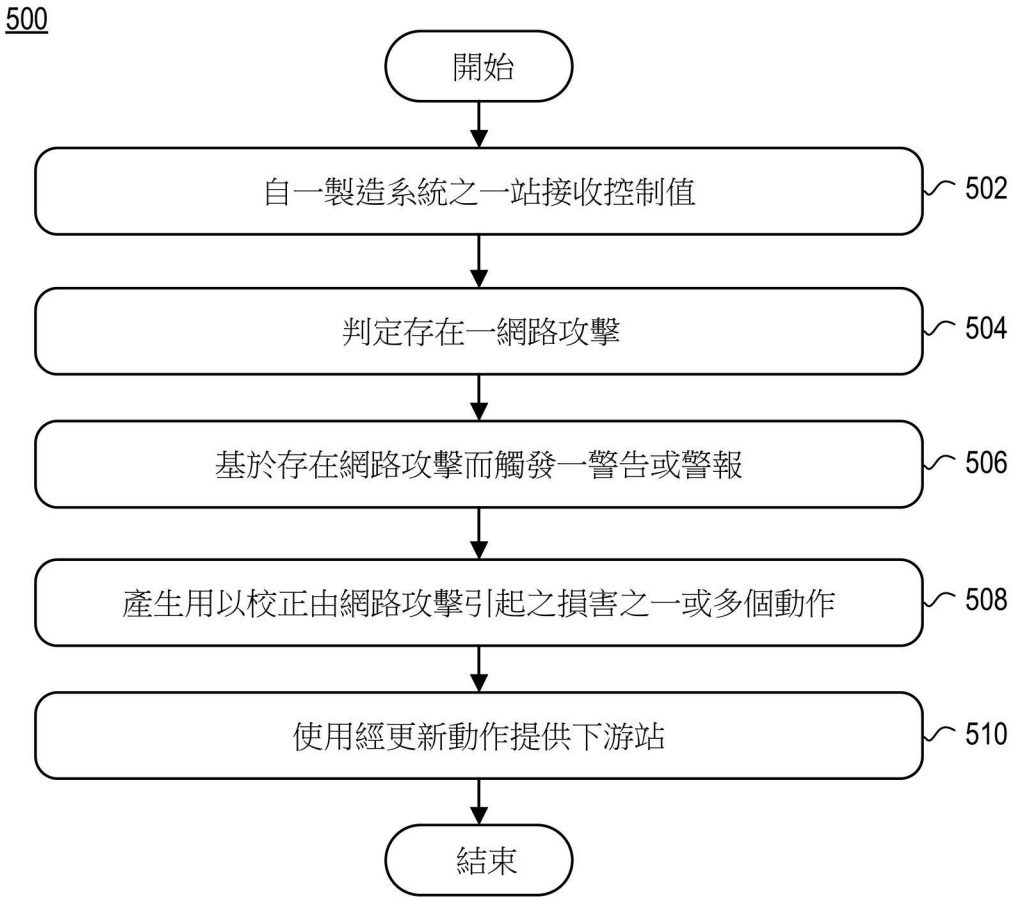
【圖2】



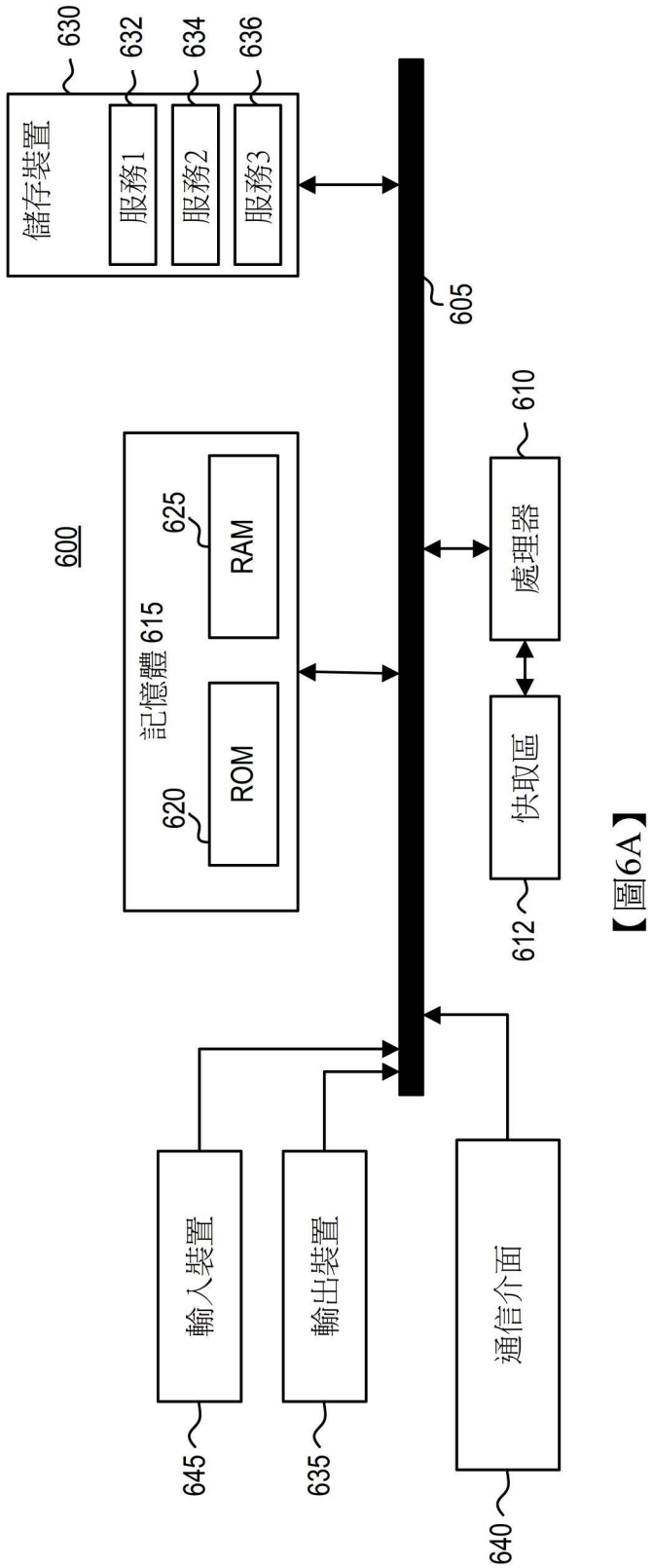
【圖3】


400
410
$\pi(S_k)$
412
$A(s)$
408
Y
S_k
$y_{s,0,k}$
$y_{s,i,k}$
$y_{s,N,k}$
$y_{v,0,k}$
$y_{v,i,k}$
$y_{v,N,k}$
402_0
$C_0(s)$
404_0
$G_0(s)$
406_0
$H_0(s)$
402_i
$C_i(s)$
404_i
$G_i(s)$
406_i
$H_i(s)$
402_N
$C_N(s)$
404_N
$G_N(s)$
406_N
$H_N(s)$
Σ

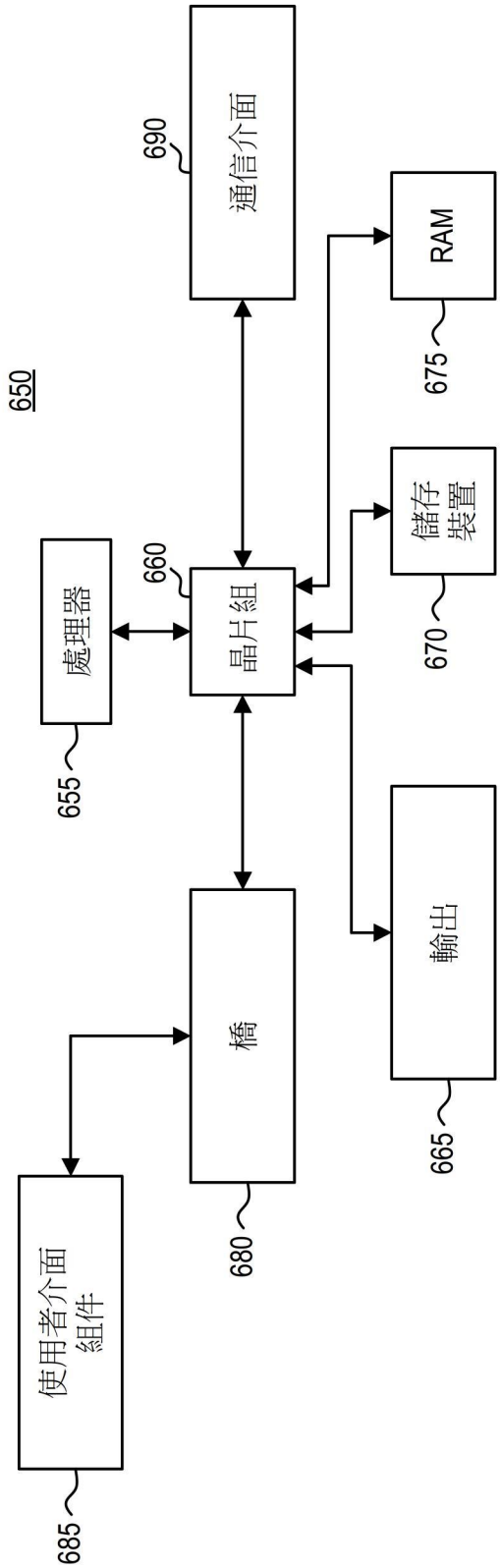
【圖4】


500
開始
自一製造系統之一站接收控制值
502
判定存在一網路攻擊
504
基於存在網路攻擊而觸發一警告或警報
506
產生用以校正由網路攻擊引起之損害之一或多個動作
508
使用經更新動作提供下游站
510
結束

【圖5】


600
630
儲存裝置
632
服務1
634
服務2
636
服務3
605
610
處理器
625
RAM
記憶體 615
620
ROM
快取區
612
輸入裝置
645
輸出裝置
635
通信介面
640

【圖6A】


650
690
通信介面
675
RAM
處理器
660
晶片組
670
儲存裝置
655
665
輸出
橋
680
使用者介面
組件
685

【圖6B】