司騰達股份有限公司
BHP Industry Solution

司騰達股份有限公司

HMS 台灣總代理 – Remote Access 跨國遠端連綫與自動化工業的最佳選擇

司騰達公司致力於推廣數位化工廠和 IIoT 工業物聯網的解決方案，並與歐洲最先進的公司 – HMS 集團合作，同時透過引進更多歐美的技術能量，提供客戶關於工業 4.0 的顧問諮詢服務，並將教育與產業連結，協助台灣產業逐步完成從現場設備、生產資訊、通訊 IoT 的垂直整合，並整合 M2M 工業總線與軟體開發，從而實現數位化工廠與自動化機械領域的創新。

LINE

官網

司騰達聯絡訊息
臺北客服專線：(02)-2242-1625
台中客服專線：(04)-2451-0611
客服信箱：sales@bhp.com.tw
Line ID：@bhp.tw
www.bhp.com.tw

Ewon® BY HMS NETWORKS

白皮書：
工業遠端存取入門

輕鬆安全地遠端存取您的機器

瞭解您想知道的遠端存取的所有資訊

HMS

目錄

簡介

現如今在工業領域，售後工程師和技術人員必須定期前往工廠檢修機器和各種設備。如果一種方案可以實現無論身在何處，都能夠遠端執行一些簡單操作並安全地解決大多數問題，這對機器製造商和工業公司而言不是很棒嗎？

假設

假設您在製造業或自動化領域工作，雖然您可能非常熟悉行銷、製造、維護或使用的機器及其PLC等，但您可能不太熟悉遠端存取、網際網路、安全性、雲端計算以及使用機器提供的資料等技術。

本白皮書中使用的圖示

在本白皮書中，我們使用特殊圖示來強調重要資訊。所述特殊圖示如下：

此圖示表示要記住的重要資訊。

此圖示表示技術內容。

此符號表示有用資訊。

注意此建議，可避免帶來巨大損失的過失。

白皮書未盡事宜

為方便起見，我們在此僅介紹工業遠端存取。
如果您想更詳細地瞭解該主題，請訪問：
https://www.hms-networks.com/ewon

BHP Industry Solution

工業遠端存取的定義及其優勢

在本章中，我們將提出以下問題：

- 為什麼現在比以往任何時候都更加有必要進行遠端存取？
- 可以採用哪些方式來實現遠端存取？
- 遠端存取有哪些優勢？

遠端存取需求的定義

工業機器製造商一直夢想能夠遠端連接到他們的機器。事實上，對於在許多遠端客戶網站安裝機組的原始設備製造商(OEM)以及在多個網站進行製造的公司而言，能夠遠端查看設備的功能體現了絕佳的競爭優勢。

遠端存取工業機械設備的常見用例包括：

- PLC的故障排除和遠端程式設計
- 從您的人機介面(HMI)進行遠端查看和控制
- 連接到網路攝像頭獲取說明
- 協助現場技術人員進行調試

遠端存取的優勢

遠端存取機器控制系統有助於排除故障並解決遇到的大多數問題，避免技術人員或工程師親自前往現場。這些問題通常不是靠修理機器來解決的，而是需要調整其程式設計或設置。例如，它們通常是由於原材料變更、機器磨損或其他可能隨時間發生變化的生產參數造成的。遠端存取是實現資料數位化和利用的第一步。

BHP Industry Solution

要點

遠端存取使您能夠從被動支援模式轉變為主動支援模式，從而說明您保持競爭力。事實上，一旦您遠端連接到您的機器（或機組），除了對它們進行故障排除和快速干預之外，您還可以出於其他目的進行資料分析。例如：

- 提高反應能力
- 減少緊急情況造成的影響
- 優化工程師的工作量
- 最大限度地提高機器可用性和生產效率
- 降低差旅費用
- 最大限度地減少對環境的影響
- 提高可持續性
- 最大限度地減少機器停機時間
- 最大限度地提高整體設備效率(OEE)
- 最大限度地提高安全性

快速解決問題意味著減少停機時間並讓終端客戶更快地恢復生產。在現場仍然需要人工物理幹預的情況下，遠端存取有助於確保前往現場的人員擁有適當的技能、機器零件和工具，從而提高一次性糾正問題的可能性。所有這些都有助於改善客戶體驗並最大限度地減少機器停機時間。

近年來，工業公司採用遠端存取策略的壓力越來越大。例如，全球興起的遠端辦公就促成了這一點。新冠肺炎疫情的爆發成為最終的催化劑，工業公司擔心外人參觀其設施會給員工帶來感染風險。

毋庸置疑，生態、經濟和社會因素也發揮著重要作用。可持續性和環境影響對我們的生活方式日益重要。在這方面，很明顯工業遠端存取是實現這一目標且最大限度地降低成本並提高整體設備效率(OEE)的安全有效方式。

機器製造商同時認識到，遠端存取提供的機會，可以為其客戶提供新的收入生成、積極主動和預防性服務。這裡指的是利用資料來促進預測性維護。

最基本地，遠端存取可以提高每個人的效率。機器製造商可以獲得競爭優勢（如圖1-1所示），從而服務更多客戶並開拓新市場；而機器使用者將提高其整體設備效率。

- 減少現場到訪的高昂成本
- 為您的客戶提供即時線上說明

- 定期接觸您的設備
- 減少對環境的影響
- 減少機器停機時間
- 最大限度地提高OEE
- 提高安全性
- 提高生產效率

圖 1-1：通過遠端存取提高效率並獲得競爭優勢

遠端存取的發展歷史

在早期，遠端存取機器包括使用通過類比固定電話和數據機連接的終端控制台進行“點對點”管理。這些系統速度慢，不易安裝，而且運營和維護費用昂貴。

然而，由於高速行動網路網路的可用性，通過路由器連接進行遠端存取至今一直廣為流行。這種遠端存取方式的主要亮點在於能夠訪問機器控制器(PLC)的資料，同時避免使用客戶的電腦網路。許多PLC供應商都提供通過行動電話供應商的資料網路進行通信的無線路由器。

儘管有時無法保證生產區域中無線信號的可用性，但這種方法無需使用有線電話線或接入公司電腦網路。

這意味著持續的網路訪問和使用者費用可快速累積。

利用網際網路

遠端存取機器另一種較好的方式是利用網際網路技術和雲端計算。主要的挑戰是如何安全地管理機器與終端使用者公司網路的連接，進而實現機器與網際網路的連接。出於顯而易見的安全原因，大多數公司的IT部門都不願意向非員工授予訪問公司網路的許可權。

依需遠端存取

機器製造商並不特別需要持續的網路連接。事實上，可以通過按需連接實現對機器進行故障排除、維護或檢修的遠端存取，從而最大限度地降低成本並提高安全性。
按需訪問有哪些優勢？首先，終端使用者可能希望阻止對機器的持續遠端存取。將機器與區域網路(LAN)斷開連接並非保證安全性的必然之舉，但能使終端使用者以物理方式控制訪問機器時間及時長。在這種情況下，通常會將機器與區域網路斷開連接。僅在必要時或只有機器製造商要求下才連接機器。
此外，如果依據批量定價方案（例如，行動網路技術）進行遠端連接，則可能需要建立連接並僅在必要時付費。

對外連接

從技術角度而言，虛擬私人網路絡(VPN)是一種極好的解決方案。但是，在確保安全性的同時啟用適當的對內網路訪問可能是一項複雜的任務。每個PLC製造商通常使用一組不同的網路埠，並且需要仔細配置通過客戶防火牆的清晰路徑。此外，IT部門通常不這麼做，因為他們不願意創建安全性漏洞。

有了工廠區域網路(LAN)建立的對外連接，可以從一開始就解決許多防火牆問題。這是因為如果沒有建立對內連接，對內連接便不需要在公司的防火牆中啟動埠，也不需要變更IT來建立通信；這是完全安全的。此配置下，工程師只可訪問被授權機器，而不能訪問工廠區域網路(LAN)。

基於軟體的解決方案

通過網際網路，可以使用虛擬網路計算(VNC)技術或PC上的其他遠端存取軟體遠端存取和控制本地監管PC。在這種情況下，軟體會回復可遠端存取的操作員介面電腦並放棄對它的控制。雖然這種解決方案對於遠端連接到PC而言可能是可以接受的，但它通常為使用者提供了對整個網路的存取權限，從安全角度而言這是不可接受的。

這種方法假設有一台能夠在遠端機器上運行應用程式的工業PC。這種硬體和軟體會產生額外的費用，使其總成本高於專用解決方案的成本。

基於安全工業路由器的VPN解決方案

最好的解決方案是借助工業路由器和安全的雲端架構來使用按需VPN連接。SSL(安全通訊端層)VPN連接通常不會給客戶的IT部門帶來什麼麻煩。

從安全角度而言，這種方法更值得一提，因為它會自動在機器和工廠區域網路之間添加邏輯網路隔離。機器製造商可以通過一個簡單且安全的介面管理機組。終端使用者可以使用該平臺來管理遠端存取許可權。

由於這是最好的解決方案，我們將在後面的章節中詳細介紹。

瞭解及使用Ewon遠端存取解決方案

您將在本章瞭解如下內容：

- Ewon Cosy和Talk2M工業雲端伺服器簡介和功能
- 如何連接到Talk2M工業雲端伺服器
- 如何使用eCatcher通過Talk2M連接到您的機器
- 如何通過VPN連接進行通信
- Ewon的其他解決方案

Ewon Cosy工業路由器簡介

Ewon Cosy是一款安全的工業路由器，用於實現與機器或設備的安全遠端連接。借助Ewon Cosy，機器製造商和工業公司可以排除機器故障、糾正PLC錯誤並遠端使用人機介面(HMI)或操作IP攝像機，而無需前往現場。Ewon Cosy既與絕大多數PLC相容，也與舊款機器（“傳統/棕色現場設備”）相容。

這種方法有助於您：

- 顯著降低成本
- 提高機器效率
- 最大限度地減少碳排放
- 輕鬆升級舊款設備

Ewon Cosy的工作原理

Ewon Cosy可隨時隨地在您和您的機器之間建立安全的VPN連接。該連接是通過Talk2M這種高度安全的工業雲建立的。Ewon Cosy可通過乙太網路或無線方式（4G或Wi-Fi）建立連接，以便在任何情況下輕鬆進行遠端存取。

將Ewon Cosy與Talk2M結合使用，用戶可以輕鬆地通過網際網路連接到他們的機器，如圖4-1所示。該解決方案非常易於使用，不需要任何IT專業知識。

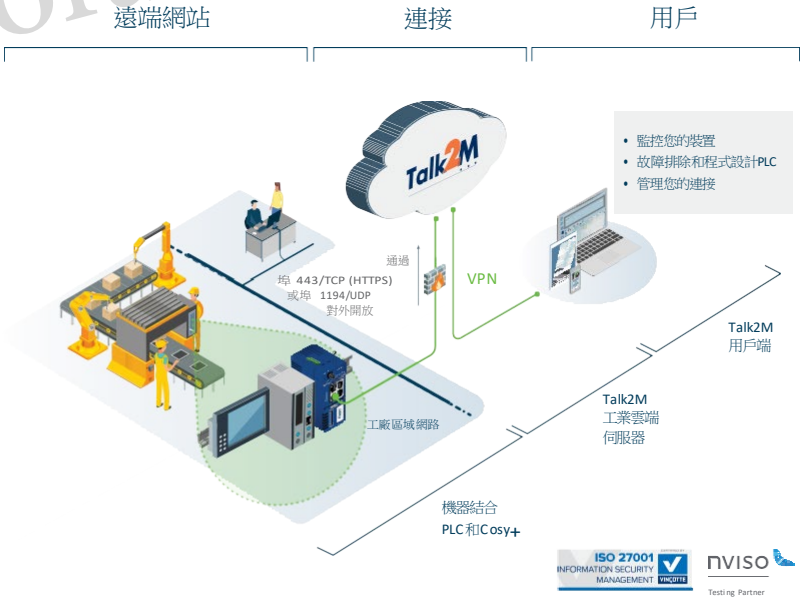


圖 4-1：Talk2M是一種工業雲端伺服器，用戶可以通過網際網路連接到其機器。

Ewon為用戶提供了三種通過Talk2M連接機器的解決方案：

- eCatcher：一款Talk2M用戶端軟體
- eCatcher Mobile：一款智慧手機應用
- M2Web：一個專用網際網路門戶

要點

您還可以在不安裝eCatcher應用程式的情況下使用Web瀏覽器（例如，Google Chrome、Microsoft Internet Explorer/Edge或Mozilla Firefox）連接到您的機器（稱為M2Web）。

使用Ewon Cosy將您的機器連接到網際網路

可通過以下幾種方法將您的機器連接到網際網路：

- 有線網路**(乙太網路)**：大多數工業網站都配備了連接到網際網路的有線網路。這種方法通常是首選方法。乙太網路區域網路連接通常是免費的，並可提供可靠的高速訪問。在某些情況下，區域網路受到複雜安全性原則約束，可能會對您的機器連接進行限制。在這些情況下，無線連接可以是一種替代方法。

- 無線網路**(Wi-Fi)**：Wi-Fi網路在工廠中日益普及。與區域網路連接一樣，Wi-Fi訪問通常是免費的，可提供高速連接。許多工廠提供獨立於公司區域網路的“訪客”Wi-Fi網路。該解決方案允許機器製造商和用戶訪問網際網路而無需更改防火牆配置。

- 行動網路網路**(4G)**：無法使用區域網路或Wi-Fi連接時，行動網路技術便是一個很好的選擇。行動網路服務在世界範圍內通常以不同的速度提供，但某些地區的信號覆蓋可能有限或不可靠。此外，在行動網路網路上使用資料的成本可能很高，而且各地的行動網路技術也不盡相同，因此可能需要在機器的路由器中安裝不同的SIM模組。這就是通常首選區域網路或Wi-Fi連接（如果可用）的原因。

將機器連接到Talk2M

連接到網際網路後，Ewon會分三個階段嘗試連接到Talk2M：

1. Ewon連接到中央訪問伺服器(AS)並通過超文字傳輸協定安全(HTTPS)會話進行身份驗證。
2. Ewon通過HTTPS連接請求要使用的VPN伺服器的IP位址(VPN伺服器位址因連接而異)。
3. Ewon與VPN伺服器建立VPN隧道。

這些階段如圖 4-2 所示。

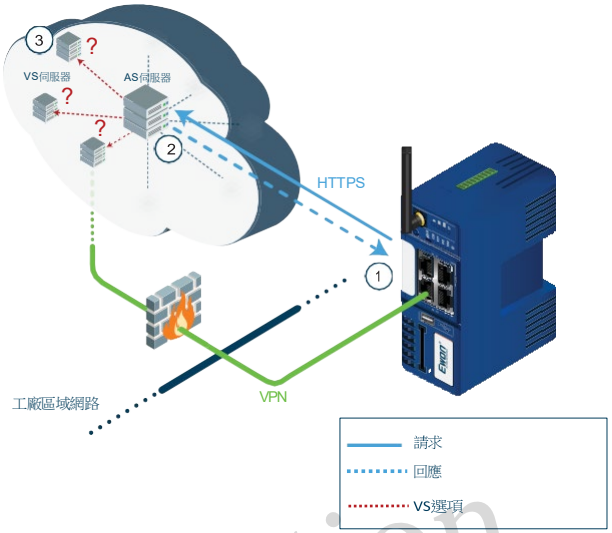


圖 4-2：分三個階段將Ewon連接到Talk2M。

將用戶連接到Talk2M

當使用者啟動eCatcher軟體時，第一步是使用以下資訊驗證身份：

- 帳戶名稱：可以使用eCatcher創建Talk2M帳戶。可以創建無限個帳戶。每個帳戶都包含可連接到該帳戶中註冊的Ewon設備的所有使用者。
- 用戶名：一個帳戶可以註冊無限個用戶。帳戶的用戶名必須是唯一的。
- 密碼：每個使用者都有自己的密碼。

注意

進行身份驗證後，您可以訪問在Talk2M帳戶中註冊且您具有存取權限的Ewon列表。該列表提供以下項目：

- 每個Ewon的名稱和狀態
- Ewon及所連接機器的簡要說明
- 當前連接到Ewon的所有用戶
- 所連接的所有部分(Ewon組)
- 控制器類型(PLC)
- 遠端連接類型(例如區域網路或行動網路)
- Ewon網路上聲明的其他設備的IP位址

當您點擊列出的Ewon時，如果其連接狀態指示為“線上”（這意味著正在執行VPN連接），eCatcher將創建一個連接到指定Ewon的VPN隧道。

您還可以在eCatcher中執行其他幾項操作，例如：

- 在當前帳戶中註冊一個新的Ewon
- 編輯和刪除有關Ewon的資訊
- 添加、更改或刪除當前帳戶中的使用者或群組資訊(一個群組即為一組用戶)
- 在當前帳戶中添加、更改或刪除部件(一個部件即為一組Ewon)
- 編輯帳號資訊

使用VPN連接

建立VPN連接時會創建兩個“隧道”：一個在Ewon和VPN伺服器之間，另一個在eCatcher和VPN伺服器之間。如圖4-3所示。每個隧道都會自動獲得一個唯一的VPN IP位址。雖然可以在Ewon端和eCatcher端訪問VPN位址，但無法在VPN伺服器端進行訪問。

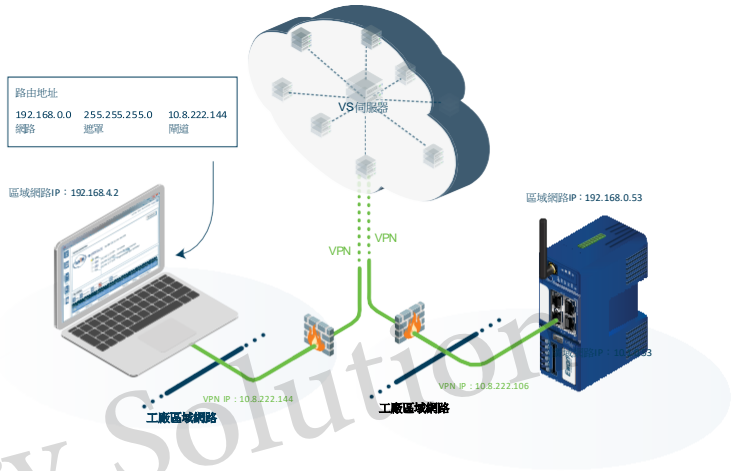


圖 4-3：eCatcher軟體自動將路由添加到目標Ewon的區域網路IP位址。

技術內容

要連接Ewon的機器端，您的電腦/平板電腦/智慧手機需要知道，在Ewon區域網路的IP位址範圍內包含目標IP位址的所有流量。為此，eCatcher在VPN連接打開時自動添加路由，在VPN連接關閉時自動刪除路由，如圖 4-3 所示。eCatcher軟體知道Ewon的區域網路 IP位址，因為在每個Ewon在Talk2M帳戶註冊時都要提供IP地址。如果您想連接到另一個 Ewon，eCatcher會自動刪除之前的路由並添加具有適當目標位址範圍的新路由。

在機器端，通過VPN隧道的流量會自動傳輸到Ewon的區域網路（機器）端。要讓區域網路端的機器與使用者進行通信，您有以下兩種選擇：

- 網路位址轉譯(NAT)功能（也稱為“隨插即用路由”）可以將Ewon區域網路IP位址替換為使用者的IP地址（這是Ewon中的默認設置）。
- Ewon區域網路端的單台機器可以手動配置為使用Ewon的區域網路IP位址作為預設閘道器。

瞭解其他Ewon解決方案

通過Ewon Cosy和Talk2M進行遠端存取是實現數位化的第一步。為了更進一步，Ewon通過Ewon Flexy和Talk2M提供監控和資料獲取解決方案。

Ewon Flexy是一款真正多功能的IIoT閘道，同時也是一款先進的工業路由器。除了進行遠端存取之外，您還能監控和收整體設備效率(OEE)至關重要的關鍵績效指標(KPI)。您還能將這些資料從機器回饋到雲端，並對其進行分析進而組織預測性維護。

Ewon Flexy的功能包括：

- 安全的**VPN**遠端存取：Ewon Flexy也包括與Talk2M相容的VPN，可實現高度安全的遠端存取以進行維護、監控和資料獲取。它可以遠端連接到PLC、IP攝像機、HMI等。
- 擴展卡：除了基本功能外，Ewon Flexy還可以通過添加擴展卡（乙太網路、Wi-Fi、4G、USB、串列等）來適應您的特定連接需求。
- 資料獲取：Ewon Flexy使用串列或乙太網路埠執行本地資料獲取。採集過程圍繞帶標記的資料庫構建，其中每個標記都與輸入/輸出 (I/O) 伺服器相關聯。
- 警報和通知管理：Ewon Flexy允許觸發並跟蹤警報和通知。可以對每個變數設置警報閾值和參數。可跟蹤、監控和分析完整的警報週期。警報通知可以通過電子郵件、SMS或SNMP（簡單網路管理協定）和/或FTP（檔案傳輸通訊協定）Trap（邊界陷阱）指令來完成。
- 資料記錄和檢索：可以對每個變數執行連續資料記錄和緩衝。可以以固定的時間間隔記錄每個變數，也可以更改觸發器。Ewon將資料值和時間戳記存儲在其內部資料庫中（最多一百萬個時間戳記點），用於統計分析和後續審查（歷史記錄）或分析最近的趨勢（即時記錄）。
- **HMI**（人機介面）網路服務器：Ewon Flexy具有用於配置和資料視覺化的集成式Web伺服器，可以在任何標準Web瀏覽器中流覽。
- **Talk2MAPI**：使用API對協力廠商軟體和雲解決方案進行企業級集成（例如，Ewon IIoT合作夥伴：AmazonWeb Services、Microsoft Azure、Siemens MindSphere、IBMBluemix等）。

Ewon Flexy尤其適用於再生能源、太陽能發電、建築管理、智慧計量、用水和廢水管理、能源監控、灌溉系統等領域的連接。

圖 4-4 列示了這些應用領域。

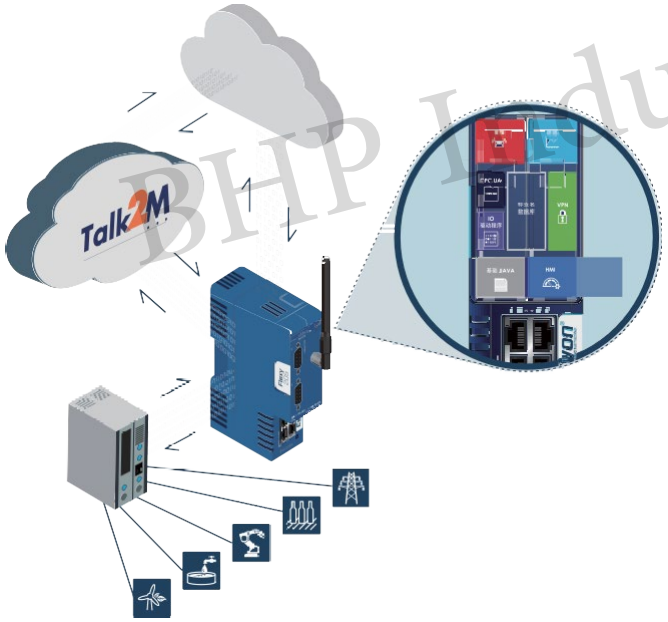


圖 4-4：Ewon Flexy使用不同的通信協定連接遠端設備。

要點 有關Ewon Flexy的更多資訊，請訪問www.ewon.biz/flexy

確保安全可靠的遠端存取

在本章中，您將能夠：

- 瞭解提高安全性的技巧
- 瞭解有關網路安全威脅的更多資訊
- 瞭解有關防火牆和VPN的更多資訊
- 選擇網路託管架構
- 採用“多層”安全方法
- 瞭解Ewon Cosy及其功能

提高安全性的技巧

安全性就像一根鏈條，隨時都會因為其中最薄弱的一環而斷裂。因此，必須在安全性和易用性之間找到最佳平衡。為此，我們提供了以下幾項可以在實施工業遠端存取解決方案之前輕鬆驗證的技巧：

1. 不要修改工廠的防火牆，以便保持其完好無損。使用對外連接可以最大限度地降低開放網路許可權的風險。此外，借助鑰匙開關或HMI按鈕，終端使用者可以保持對遠端存取的物理控制。“您所要做的就是轉動鑰匙。”
2. 能夠審核您的連接！管理員必須能夠確定誰能訪問、何時訪問以及訪問什麼。
3. 多因素身份驗證：除了傳統的識別字（用戶名/密碼）之外，建議借助多因素身份驗證增加第二次安全認證。例如，通過SMS發送每個連接的唯一識別金鑰。
4. 認證：您使用的解決方案必須經過專業審核和認證，這一點很重要。ISO27001標準是這方面的參考。但是，確定此認證的背景以及它所認證的確切內容同樣很重要。例如，認證可以僅限於編寫使用說明，但這幫助不大。我們建議您確保雲、連接和工業路由器都符合相關標準。

5. 審核和滲透測試：確保您的供應商由一家聲譽良好的外部公司進行適當的審計，該公司經常更新其測試。當然，我們的目標是與事件保持同步，避免每年重複相同的測試或相同的過程，或審核過於局限的部分。

6. 最後，讓我們不要太天真：“All that glitters is not gold”(諺語:不是所有閃閃發亮的東西都是金子)一所以選一個認真、成熟且專業的合作夥伴。

網路安全威脅

媒體經常報導涉及洩露數百萬個識別字的大型安全性漏洞。然而，還有一個更大且可能更具破壞性的威脅：對關鍵基礎設施和大型機器的網路攻擊。尤其包括公用事業、應急系統、建築物和工業設備的環境控制措施。

例如：2021年5月，為美國東海岸提供45%燃料供應的Colonial Pipeline成為網路攻擊的目標。勒索軟體攻擊迫使該公司關閉其8,000公里長的管道長達數天。

通常出於經濟利益或者出於政治或社會原因，駭客團體可能會試圖獲得贖金或損壞連接到網際網路的工業機械設備。有些國家還通過參與網路攻擊來實現各種戰略目標。

例如，據稱2010年的震網病毒是由一個或多個針對伊朗核計畫的國家開發的。該病毒感染了伊朗納坦茲核設施易受攻擊的PLC和西門子Step7軟體，導致離心機變速旋轉，繼而引起過度振動，最終自我摧毀。

最近，據稱Solarwinds公司的安全軟體中引入的惡意程式碼已經感染了 18,000 多名客戶並造成了資料洩露。其首席執行官Mandia先生表示，這次攻擊只可能由“具有一流進攻能力的國家”實施的。*因此，確保安全性必須成為所有希望遠端連接到其客戶的機器的機器製造商、原始設備製造商(OEM)和系統集成商的首要任務。*

根據Palo Alto Networks最近的一份報告，98%的物聯網流量未經加密，近60%的設備容易受到（中度到重度）網路攻擊。由於惡意攻擊日益複雜，因此保護工廠免受惡意攻擊比以往任何時候都更加重要。

瞭解防火牆和虛擬私人網路絡(VPN)

防火牆控制區域網路(LAN)和網際網路等網路之間的通訊流量。防火牆通常安裝在它所保護的網路邊緣，可能由硬體設備、軟體或硬體和軟體組合組成。

您可以將路由器視為中世紀城堡的入口，將防火牆視為入口處對城堡的訪問進行控制的吊橋。

儘管存在許多先進的設計和技術，但防火牆的基本功能是根據一組預先配置的規則，過濾來自未經批准的網路（例如，網際網路）的所有流量。*預設情況下，所有來自受信任網路的出站流量*（例如，從區域網路到網際網路）*可通過防火牆*。為回應當前對外連接而發送的對內流量也可通過防火牆。為回應Web瀏覽器啟動的請求，來自Ewon網頁www.ewon.biz的對內流量可自動通過防火牆。

但是，預設情況下會阻止未與出站流量請求明確關聯的任何對內流量。要允許來自網際網路的某些對內流量通過防火牆，必須將防火牆規則配置為允許特定類型的流量從特定來源流向特定目標位址。

雖然防火牆可保護區域網路中的系統（包括機器）和資料免遭未經授權的訪問，但它不能保護通過區域網路發送和接收的網際網路流量的機密性和完整性。*這就是虛擬私人網路或 VPN的價值所在*。VPN技術在兩台機器或兩個網路之間創建隧道。在兩端之間生成一個加密金鑰，創建一個加密的“包裝器”，保護源頭的資料。在通信隧道的另一端，目標閘道“拆封”資料並對其進行解密。

使用網路託管架構

您可以選擇自行在PC上安裝VPN解決方案。然後，您需要安裝和配置軟體，以便建立通信並確保通信安全。這不一定是一項簡單的任務，安全性設置配置錯誤會影響預期用途。我們認為機器製造商應該只關心在其機器上進行的維護活動，而不是IT複雜性。這就是我們設計Talk2M的初衷。有了我們的託管解決方案，使用者無需進行複雜的配置。VPN伺服器配置從PC外包到雲端，技術和安全性配置由我們的專家工程師設置。用戶可以最輕鬆地連接到他們的機器並專注於他們的任務，如圖 3-1 所示。

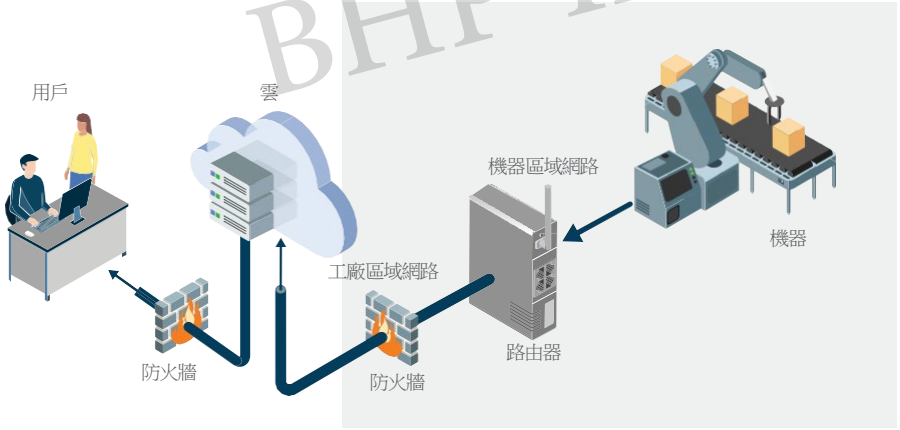


圖 3-1：使用VPN伺服器安全地連接到您的遠端機器。

但是，如果VPN伺服器不是安裝在單台機器(PC)上，而是由雲服務(SaaS)產品中的獨立組織託管，則可以在多個機器製造商之間共用，每個製造商都有一個私人帳戶，並且每個製造商都能夠分別配置其客戶和機器。*與基於硬體閘道或內部軟體應用程式的純物理架構相比，雲端架構本質上具有更好的可擴展性。*

雲端架構允許通過在多個伺服器上分配必要的連接和VPN隧道來實現負載平衡。它還提供冗餘，從而確保發生操作中斷或災難時遠端存取服務的彈性。

瞭解Ewon的“多層”安全方法

遠端連接的主要挑戰之一是平衡PLC工程師或技術人員的需求與IT部門的任務，即確保網路的安全性、完整性和可靠性。多年以來，找到一個雙方都容易接受的解決方案一直是一項挑戰，也是令所有利益相關者感到沮喪和效率低下的根源。維護網路安全對於獲得IT部門的認可至關重要，但用戶不希望解決方案過於複雜、難以實施或會妨礙生產效率。*基於安全性和易用性的雙重考慮，Ewon創建了一個適合終端使用者和IT管理人員的遠端存取解決方案。*

安全性和可靠性是Ewon解決方案的兩個關鍵方面。它們是基於使用多層安全對策的“多層安全性”策略，如圖 3-2 所示。

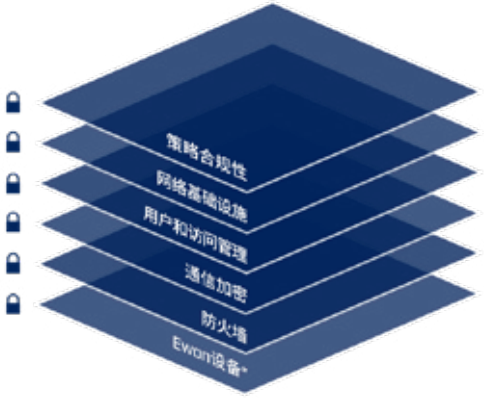


圖 3-2：Ewon的多層防禦策略。

該策略的目標是基於以下眾多出版物、指南、最佳實踐和既定安全標準，保護Talk2M工業雲端伺服器連接和資訊系統的完整性，例如：

- ISO/IEC27001(國際標準組織和國際電子電機委員會)
- 美國國家標準與技術研究院(NIST)《提升關鍵技術設施網路安全框架 1.0 版》
- 開放式Web應用程式安全專案(OWASP)
- 開源安全性測試方法手冊(OSSTMM)

從硬體到策略和程式，安全性是Ewon解決方案的關鍵元件，集成在各個層次。Ewon縱深防禦戰略的不同層次包括以下要素：

- **Ewon**路由器：用戶必須進行身份驗證。機器/區域網路端的流量與廣域網路/用戶端的流量是分離的，使用者只能訪問區域網路中授權的設備。

  具體控制措施包括以下四個關鍵方面

  - 網路隔離：工業路由器通常安裝在機器的控制台中，一端連接機器（區域網路），另一端連接工廠網路（廣域網路）。需要建立連接時，Ewon設備充當所有流量通過的閘道。最初配置Ewon時，設備的安全性設置會限制這兩個網路介面之間的流量。這種網路分離僅允許遠端存取連接到Ewon區域網路的設備；它會阻止訪問網路的其餘部分。
  - 設備認證：Ewon路由器具有與Talk2M不同的存取權限。只有擁有適當憑據和存取權限的用戶才能更改Ewon路由器的安全性設置。同樣，對於提供資料服務的設備，只有獲得授權的使用者才能查看或更改資料。
  - 物理交換機：所有Ewon硬體設備都有一個數位輸入。可以將物理交換機連接到此輸入以啟用或禁用廣域網路埠。終端使用者可保留對是否遠端存取設備的完全本地控制。
  - IP分配和控制：Ewon需要與連接到同一網路的PC是相同類型的設置（IP位址、子網路遮罩和閘道，以及所有可選的代理設置）。Ewon可以配置為通過DHCP自動接收這些設置。但是，如果需要，Ewon也可以配置為使用由IT部門分配和控制的靜態IP位址。

- 防火牆：在eCatcher應用程式中，Talk2M帳戶管理員可以設置過濾和防火牆規則，指示可以遠端存取Ewon背後的哪些設備，乃至可以通過哪些埠（乙太網路、USB或串列）以及可以使用哪些協議訪問它們。Talk2M根據所聲明設備的IP位址、埠、閘道和對Ewon服務的存取權限提供四種不同的防火牆配置。從限制最少的防火牆級別到最安全的級別，分別描述如下：
  - 標準型：允許訪問連接到Ewon網路的所有設備。
  - 高級型：只能訪問明確列出的連接到Ewon區域網路的設備；也可能設有埠限制。
  - 加強型：可以阻止訪問Ewon閘道。
  - 超強型：可以阻止訪問Ewon設備服務，例如HTTP、FTP和SNMP。

當與Talk2M用戶許可權管理相關聯時，管理員可以為特定用戶組自訂遠端存取許可權。

- 加密：遠端用戶和Ewon之間的通信使用傳輸層安全(TLS)進行完全加密，從而確保資料的真實性、完整性和機密性。所有使用者和Ewon單元均使用x.509證書進行身份驗證，而端到端通信使用強對稱和非對稱演算法進行加密。
- 用戶管理及職責：每個Talk2M帳戶可以擁有無數個用戶。管理員可以為需要訪問遠端設備的每個使用者創建唯一識別碼。這使得在需要時更容易授予和撤銷訪問特權。此外，Talk2M帳戶管理員可以限制每個用戶可以訪問哪些機器、可以訪問哪些服務，乃至允許使用哪些埠和哪些協定。例如，管理員可以允許遠端使用者出於監視目的訪問特定設備的web服務，但僅限特定工程師才能用埠進行更改。控制措施包括：

- 基於角色的存取控制(RBAC)，定義了哪些用戶可以訪問哪些機器並允許不同級別的訪問
- 每個使用者的唯一識別碼和個性化密碼要求（最小長度、字母、數位元、特殊字元、到期時間和一次性密碼歷史記錄）
- 多因素身份驗證(MFA)，要求使用者在輸入用戶名和密碼後輸入SMS發送的代碼
- 每個設備的審核日誌和連接日誌，用於查看連線物件、連線時間以及連接時長

- **Talk2M**基礎設施：Ewon在風險管理框架內定期評估Talk2M架構。實施適當的控制措施以實現最大的安全有效性並符合適用的監管要求。

技術內容

Ewon簽約了幾家符合以下要求的一流託管公司：

- 符合要求的託管服務供應商：為了提高可靠性、改進冗餘和減少延遲，Ewon與全球21家領先的託管服務供應商合作。
- 每年365天、每週7天、每天24小時全天候監控：全天24小時監控我們的伺服器網路，以確保最大的可用性和安全性。
- 認證資料中心：相關認證包括Service Organization Control (SOC) 1/2 Statements on Standards for Attestation Engagements (SSAE) 16/International Standard for Assurance Engagements (ISAE) 3402, SOC 2, 和International Organization for Standardization (ISO) 27001/27002/27017/27018。
- 雲安全聯盟(CSA)企業成員：Ewon與作為CSA企業成員的託管合作夥伴合作。

- 策略和程式：Talk2M遠端存取解決方案旨在相容客戶的現有安全性原則。Ewon路由器在通常開放的埠（例如443和1194）上使用對外連接並與大多數代理伺服器相容，旨在最大限度地減少對網路的侵入並在現有防火牆規則內運行。Talk2M帳戶管理員可以自訂密碼策略，使其符合公司策略。他們還可以限制用戶存取權限。Talk2M帳戶管理員還可以查看Talk2M連接報告（審計），以瞭解哪些用戶在何時連接到哪些設備，從而核實是否遵循了公司的遠端存取策略。

為盡可能確保最佳的業務連續性，我們為客戶提供兩種服務：

- Talk2M Free+提供免費、高效的服務，無需簽訂服務級別協定(SLA)
- Talk2M Pro是一種更精細的付費服務，需要簽訂SLA

Talk2M Pro服務保證99.6%的服務可用性。為了提供這兩個級別的服務，我們通過幾個策略和控制目標來加強Talk2M架構，包括：

- 託管服務供應商的SLA：Talk2M Pro服務由一流的託管合作夥伴託管，保證我們的服務具有99.99%的可用性。對於Talk2M Free+服務，我們使用了多個託管服務供應商，通常提供超過99%的可用性。
- 關鍵性能指標：每台伺服器的性能都受到持續監控。
- 伺服器冗餘：供應商的多樣性有助於在出現問題時快速重新路由VPN連接。
- 持續監控：TalK2M服務由值班工程師持續監控。

最後，為了降低網路延遲，資料中心分佈在五大洲（北美、歐洲、亞洲、非洲和澳洲）並不斷擴展到越來越多的地區。事實上，某些基於超小型資料的PLC協定需要低延遲，這些協定對網路中斷更加敏感。Ewon產品連接到地理位置最近的伺服器，以優化連線性能。

未來的解決方案：Ewon Cosy+及其進一步增強的安全性

未來，Ewon Cosy+工業路由器將採用多層安全方法（見圖3-2），並將自己定位為更加重視安全性的絕對行業標杆。
憑藉Cosy+，Ewon將遠端存取解決方案提升到了前所未有的安全水準。這種新方法將高水準的物理安全作為信任鏈的一部分，以滿足最嚴格的物聯網標準。以下是Ewon Cosy+集成的一些高級安全功能：

- 從硬體到雲端有保證的信任鏈：Ewon Cosy+具有內置安全元件(SE)晶片，可保護機密資訊並提供硬體信任根。它還包括防止克隆或偽造的根證書。
- 已實施安全啟動（受控啟動的一種形式）序列，以確保僅執行由Ewon簽名的代碼。同時確保對與T2M雲端伺服器的所有通信進行增強式加密。
- 與Ewon Cosy+相關的所有機密操作均通過金鑰儀式處理。金鑰儀式(KC)是一個控制如何生成和存儲加密物件的會話。
- 數位輸出表明遠端連接處於活動狀態，從而提高了安全性。

遠端存取使用實例

在本章中，您將瞭解以下五個具體實例：

1. 鑄造商
2. 熱成型機製造商(MAAC)
3. 麵包工廠(Bakkersland)
4. 物料搬運(A.G.Stacker)
5. 衛生健康領域的迴旋加速器(IBA)

1. 鑄造商

目前該鑄造商遇到的問題是：產品出口世界各地，現場支援成本高，設備眾多，不方便集中管理，需要有安全性保障。

該鑄造商對比了多家方案，最終選用了HMS的Ewon Cosy閘道配套Talk2M伺服器的方案，該產品的穩定性、聯網方式的靈活性、以及產品基於分層深度防禦的安全設計、帳戶可集中管理的簡單方便性，都成為了用戶最終決策的助推因素。

Ewon Cosy通過基於雲的遠端連接解決方案Talk2M，建立從機器到世界任何地方的安全VPN連接。閘道在區域網路上與PLC和HMI進行無縫通信，並允許從電腦、平板電腦或智慧手機進行遠端連接。Ewon Cosy和Talk2M使連接變得簡單，並且不需要使用者成為IT專家，即可節約時間和成本。

客戶系統架構介紹

客戶使用的西門子S7-1500 PLC以及三菱Q系列PLC，主要是對鑄鐵行業和有色金屬鑄造行業的整體鑄造和造型設備進行控制，但由於客戶設備出口世界各地，導致技術維護成本很高，同時需要對設備進行集中管理和控制。

客戶最終選用了Ewon Cosy閘道與Talk2M帳戶結合的方式，通過對PLC進行遠端存取，技術維護人員無需出差到全球各地進行維護，可進行遠端存取與PLC程式的上下載，這極大地降低了維護成本，通過Ewon提供的Talk2M帳戶，也實現了設備的集中管理與監控。

方案亮點

1. Ewon Cosy模組支援LAN和4G兩種聯網方式並且可以進行冗餘切換，能夠針對不同的工業現場提供靈活的聯網方案。

2. 遍佈全球的Talk2M雲端伺服器保證了用戶對出口到世界各地的設備能夠隨時隨地進行穩定和便捷的遠端存取。

3. Ewon產品基於分層深度防禦的安全設計為用戶遠端存取的安全性保駕護航。

4. Talk2M PRO帳號能夠對遠端連接的使用者和設備進行統一的管理和分配，便於審計追蹤。同時支援多個遠端連接，方便特殊情況下的遠端專家會診。

客戶評價Ewon產品：“自從我們啟用了HMS的Ewon Cosy閘道，我們無需安排大量的現場服務差旅，這幫我們節約了大量的差旅費用和維護成本，同時，Talk2M帳戶便捷的管理方式，讓我們在任意地點都能及時掌控設備運行狀態，和置身現場一樣，迅捷方便！”

2. 熱成型機製造商

MAAC總部位於芝加哥，專門製造熱成型機和其他互補產品。MAAC產品在全球範圍內廣泛使用，並服務於許多行業領域，例如航空航太、醫療和汽車行業。

MAAC很快意識到自動化控制技術將是機械領域成功的關鍵。技術服務總監Leslie Adams長期以來一直是電子自動化的宣導者。Adams表示，“Ewon VPN路由器提供的通信簡直太棒了。通過網際網路連接，我們幾乎可以從任何地方連接到機器。”

Ewon技術提供的安全VPN連接完全集成了IT安全標準。Ewon獨特的遠端存取解決方案使MAAC能夠像公司車間的機器一樣輕鬆靈活地連接到現場的機器。

遠端存取使公司可以隨時連接到機器，並可以訪問PLC、驅動器和HMI設備以及連接到機器子網的任何其他設備，包括IP攝像機。在安裝Ewon路由器之前，MAAC使用電話數據機連接到其機器，但時間延遲是一個大問題。“我對監控機器帶來的的挫敗感還記憶猶新，因為資訊需要很長時間才能通過數據機連接傳輸完成。我們在澳大利亞使用的一台機器，延遲長達15秒，”Adams回憶道。

遠端維護可實現快速高效的故障排除，因而有助於降低客戶支援成本。Leslie評價說：“使用Ewon，我們減少了50-70%的支援成本，同時顯著減少了通常因等待維修技術人員造成的機器停機時間。往返現場耗費的時間相當於浪費了很多金錢。在機場候機和開車前往客戶的工廠會浪費大量時間—我們更願意我們的員工把這些時間用於操作新機器或改進現有系統。這些人不在公司時，他們根本就沒法做重要的事情。”

3. 麵包工廠(Bakkersland)

Bakkersland是荷蘭最大的麵包工廠。Bakkersland的主要擔憂是生產過程中可能出現的機器停機。任何停機情況都可能導致物流過程延遲。

為了避免這種類型的中斷，Bakkersland開展了一個專案：為其每台機器配備一台Ewon工業路由器。Ewon路由器安裝在控制室中PLC旁邊的DIN導軌（用於在設備機架內安裝斷路器和工業控制設備的金屬導軌）上。該架構線上運行，並可通過安全VPN連接讓操作員對機器進行遠端監控。

Bakkersland選擇Ewon Cosy路由器作為其機器的遠端維護系統。Bakkersland技術專家Dennis van Scheijndel解釋了Ewon架構的優勢：“如果發生警報，操作員將能夠明確是特定感測器有髒汙還是由於連接並非完全安全。必要時，供應商將能夠對控制措施進行更改。作為用戶，我們並不是唯一節省時間的人；與此同時，機器製造商也不再需要派工程師前往現場。從中受益的主要是位於國外的供應商。”

4. 物料搬運(A.G.Stacker)

A.G.Stacker是堆垛機和輔助設備製造商。Clarence和Helen Allen於 1996 年創立該公司時，他們的目標是提供創新設備，並提供優於業內任何廠家的客戶支援。如今，考慮到創新和客戶服務，A.G.Stacker即將與Ewon合作開發下一代客戶交互產品。

A.G.Stacker製造的機器已被全球客戶採用。每一台機器都使用複雜的自動化系統，其中包括驅動器、可程式設計控制項和其他最先進的設備。雖然A.G.Stacker擁有一支由高素質工程師、技術人員和培訓師組成的團隊，可說明客戶最大限度地發揮機器的價值，但有時，客戶的實際情況證明瞭在現場進行微調和系統修改是合理的。

有時需要派專人前往客戶現場來調整機器上的自動化設備，無論調整幅度有多麼小。由於臨時乘坐飛機價格高昂，A.G.Stacker想找到一種新的創新方法來解決這個問題。這也是Ewon派上用場的時候。

Ewon提供一種快速、簡單且安全的遠端連接方法。A.G.Stacker電氣/IT技術人員Kennedy Larramore解釋道：“即使我們分配了三名技術人員來支援我們的客戶，但‘移動的技術人員’對於我們的客戶和A.G.Stacker而言都是價格高昂的。基本上，我們的員工可以更好地利用往返現場所耗費的時間，而且客戶現場停機時間的成本也非常高。此外，我們經常遇到客戶難以描述其確切問題。”

“我們首先在我們的機器上提供Ewon設備作為選項。但在看到Ewon的免費Talk2M解決方案和現場設備的強大功能後，我們決定將Ewon集成到我們製造的所有機器中。”Larramore先生補充道。

5. 衛生健康領域的迴旋加速器(IBA)

IBA致力於為癌症診斷和治療開發高精度解決方案，例如迴旋加速器。IBA選用Ewon和Talk2M技術在全球範圍內提供遠端售後服務。

“最重要的是，我們的目標是能夠在客戶出現故障或有任何疑問時為他們遠端解決問題，”IBA客戶服務專案經理PatrickDelcour解釋說，“使用Talk2M，我可以在三秒鐘內完成登錄，並從澳大利亞墨爾本網站轉到比利時根特網站。”

根據指示燈和顯示器狀態提供的資訊，從控制室為客戶解決故障。“但是，來自控制室的回饋資訊非常分散。”Delcour先生說。使用Ewon之前，客戶的操作人員必須在出現問題時撥打IBA熱線。

Talk2M解決方案徹底改變了IBA的工作方式。Talk2M兼具易用性和連線性，同時提高了回應效率。“點擊三下，我就連接上了，”Delcour先生如是說。使用者完全感受不到與防火牆或代理相關的複雜性。

與Talk2M建立連接後，Ewon區域網路端的所有IP位址都將對用戶可見且可被用戶訪問。只需點擊幾下，用戶就可以連接到PLC和IP攝像機，或在控制PC上啟動遠端桌面應用程式來控制本地PC並啟動HMI。

如需查看有關如何使用Ewon的更多示例，請訪問**www.ewon.biz/customers**。

只需5個簡單步驟即可啟動並運行Ewon Cosy

在本章中，瞭解如何：

- 創建並設置您的Talk2M帳戶
- 配置您的Ewon Cosy
- 連接到遠端機器

如果您還沒有Ewon Cosy但想瞭解更多資訊，請訪問www.ewon.biz/zh/contact查找您所在國家/地區的經銷商資訊。

按照以下步驟操作：

1. 下載、安裝並啟動**eCatcher**。
   eCatcher是一款免費工具，用於在Talk2M虛擬私人網路絡(VPN)中啟動遠端存取並連接到所有連接到Ewon的設備。您可以從Ewon網站https://ewon.biz/zh/technical- support/pages/all-downloads上下載eCatcher。啟動安裝嚮導後，按照說明完成設置並啟動eCatcher。

2. 在登錄頁面上，點擊“創建免費帳戶”，創建您的帳戶。
   創建一個唯一的帳戶名稱，輸入您的姓名和電子郵箱並創建一個密碼。您還必須通過點擊發送到您電子郵箱的連結來啟動您的帳戶。

點擊“檢查可用性”以驗證您是否選擇了唯一的帳戶名稱。

3. 登錄**eCatcher**並按一下“添加”按鈕添加您的**Ewon**。
   此步驟如圖6-1所示。按照設置嚮導繼續操作。選擇您的Ewon Cosy版本（乙太網路、Wi-Fi或行動網路網路）。配置可通過插入Ewon的預配置U盤/SD卡或通過Ewon的Web介面完成。

可以通過與Ewon連接到同一區域網路（或直接插入乙太網路埠）的Web瀏覽器訪問Ewon的Web介面。訪問此Web介面的最簡單方法是啟動“eBuddy”程式，該程式會自動檢測連接到同一區域網路的多個Ewon。找到Ewon後，只需按右鍵Ewon並選擇“在瀏覽器中打開”。

在此步驟中，您可以更改區域網路的IP位址（預設為10.0.0.53）並通過DHCP或靜態IP位址定義廣域網路。出現提示時，將U盤/SD卡插入您的PC以保存配置。完成後，關閉eCatcher應用程式。

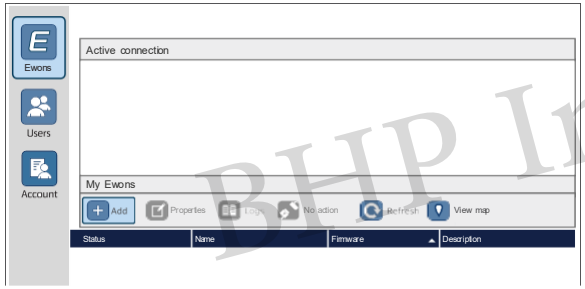


圖 6.1：在eCatcher中添加Ewon

4. 打開**Ewon Cosy**，連接網際網路並插入**U盤/SD卡**。
將廣域網路乙太網路線纜插入廣域網路埠（如圖6-2所示），相應埠旁邊將會出現一個琥珀色的閃光燈。Ewon上的每個埠旁邊都會顯示一個數位。預設情況下，1 代表區域網路埠，4代表網際網路埠。

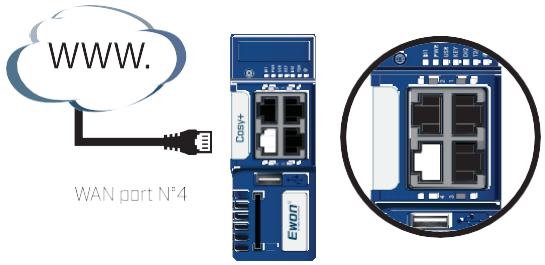


圖 6-2：識別Ewon上的網際網路。

當PWR指示燈呈綠色且USR指示燈呈綠色閃爍時（如圖6-3所示），將配置好的U盤/SD卡插入Ewon Cosy。USR指示燈將開始快速呈琥珀色閃爍，表示已檢測到有效的設定檔。

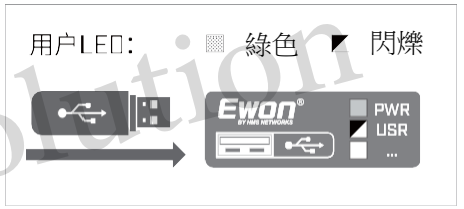


圖 6-3：插入USB且檔載入成功時的LED模式。

如果USR指示燈變為綠色常亮，則表示檔載入成功。您可以移除U盤或SD卡，您的Ewon Cosy將立即重新啟動。如果USR指示燈變為紅色，則表示您的配置有誤。所述模式如圖6-4所示。

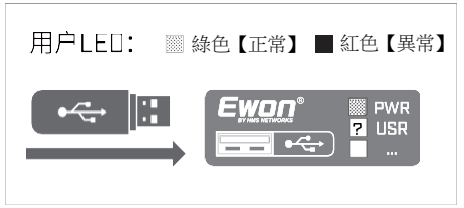


圖 6-4：等到用戶指示燈變為綠色常亮（載入成功）或紅色（配置有誤）

提醒

建立Talk2M連接可能需要幾分鐘時間。在設置過程結束時，Talk2M指示燈應亮起。請參閱圖6-5。

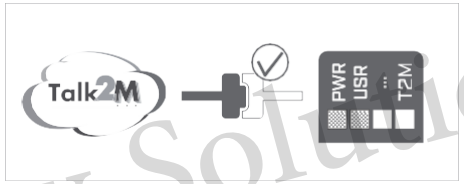


圖 6-5：Talk2M指示燈亮起，表示設置過程已完成。

5. 電腦連接到網際網路後，啟動**eCatcher**。
Ewon Cosy的狀態必須為“線上”。只需突出顯示您的Ewon設備，然後按一下“連接”按鈕。

通過eCatcher連接到Ewon後，如果您已將乙太網路設備插入Ewon Cosy的區域網路埠並且它們位於同一子網中，您可以使用Ping指令檢查其IP位元址的網路連接情況。

給選擇工業遠端存取解決方案的用戶的建議：

1. 請特別注意安全方面（請參閱第3章）。
2. 確保您可以輕鬆管理您的連接以及誰有許可權在何時訪問哪些機器。能夠通過集成式審核系統跟蹤以前的訪問記錄也很重要。
3. 必須對所有連接進行保密和加密。
4. 在工廠內定義網路訪問架構：機器供應商無許可權訪問您的整個區域網路。只接受對外連接。然後，您不需要打開更多埠，也不需要固定IP位元址。
5. 通過適當的SLA確保供應商的雲端架構能夠保證您有存取權限。事實上，最糟糕的情況莫過於陷入困境，因為您的雲系統依賴於一個不可用的資料中心。要以2021年發生在法國的事情為戒。
6. 選擇一個基於不斷發展的、經驗證的解決方案開發的解決方案，最好是開放原始程式碼解決方案。
7. 確保您的供應商繼續更新固件和程式。
最糟糕的莫過於供應商純粹出於投機而進入市場，並在幾年後退出市場。
8. 群組的穩定性：確保您的供應商健全發展且能夠盈利。

2G：于1991年首次向公眾發佈，基於GSM且啟用了SMS文本消息等移動設備數位資料服務的第二代無線通訊技術。另請參閱全球移動通信系統(GSM)和短信(SMS)。

3G：于1998年首次向公眾發佈，為無線語音電話、行動網際網路接入、固定無線網際網路接入、視頻通話和移動電視技術提供2兆比特每秒(Mbps)或更高資料傳輸速率的第三代無線通訊技術。

4G：于2008年首次向公眾發佈，為行動通信（例如，行動車輛通信）提供100Mbps峰值資料傳輸速率，同時為低移動性通信（例如，行人通信）提供1千兆比特每秒(Gbps)峰值資料傳輸速率的第四代無線通訊技術。

高級加密標準**(AES)**：一種用於加密敏感網路流量和資料的對稱分組加密演算法。AES是DES和3DES的替代加密演算法。另請參閱資料加密標準(DES)。

應用程式設計發展介面**(API)**：一套規則和規範，供軟體程式遵循以進行相互通信，且充當不同軟體程式之間的介面並促進它們之間的交互。

憑證授權**(CA)**：頒發數位憑證並由證書上指定的主體證明公開金鑰所有權的實體。

資料加密標準**(DES)**：開發於二十世紀七十年代初期，但由於其金鑰大小較小（56位），目前被視為不安全的對稱式金鑰密碼編譯演算法。

DB9：一種用於RS232串列電腦連接且以其特有的D形金屬遮罩層和兩排共九針的平行線而得名的常用電連接器。另請參閱RS232。

DF1：一種用於與大多數Allen Bradley RS232介面模組進行通信且面向位元組的非同步協定。另請參閱RS232。

信封加密**(EVP)**：OpenSSL加密函數的高級介面。另請參閱OpenSSL。

安全有效載荷封裝**(ESP)**：IPsec協定套件的一部分，負責保證原始資料的真實性、完整性和機密性。

乙太網路：一種控制如何通過區域網路傳輸資料的網路通訊協定。從技術角度而言，這屬於IEEE 802.3協議。該協議隨著時間的推移不斷發展和改進，目前可以以1 GB每秒的速度傳輸資料。

乙太網路線纜（交叉）：一種帶有RJ45連接器且將兩台電腦設備直接連接在一起的雙絞線銅纜。

乙太網路線纜（直通）：一種帶有RJ45連接器且通常通過集線器或交換機將區域網路中的電腦設備連接在一起的雙絞線銅纜。另請參閱區域網路(LAN)。

檔案傳輸通訊協定**(FTP)**：一種用於在網路中的用戶端和伺服器之間傳輸電腦檔的標準網路通訊協定。

防火牆：一種旨在防止未經授權訪問私人網路絡或防止通過私人網路絡進行未經授權訪問的網路安全系統。防火牆可以作為硬體和軟體或兩者的組合來實現。網路防火牆經常用於防止未經授權的用戶訪問連接到網際網路的私人網路絡。

全球移動通信系統**(GSM)**：歐洲通信標準協會(ETSI)為2G協定制定的無線通訊標準。另請參閱 2G。

基於雜湊的訊息驗證碼**(HMAC)**：一種使用加密散列函數和秘密加密金鑰的訊息驗證碼。

超文字傳輸協定安全**(HTTPS)**：通過網際網路中的Web瀏覽器進行安全通信且使用安全通訊端層(SSL)協定進行加密的協定。另請參閱安全通訊端層(SSL)。

人機介面**(HMI)**：製造或程式控制系統中的使用者介面。

工業**PLC**：一種用於通過所謂的“連續處理”來控制工業過程的特殊電腦。此類控制器用於自動化工業過程。一個動作觸發另一個動作，另一個動作又觸發另一個動作，這取決於各種參數、條件等。這些自動機廣泛用於裝配線和機器控制。

網際網路服務供應商**(ISP)**：為客戶提供網際網路存取權限的組織。

IP攝像機：通過快速乙太網路連接聯網的攝像機。IP攝像機通過網際網路或網路連接將其信號發送到主要伺服器或電腦顯示器。它主要用於IP監控、閉路電視(CCTV)和數位攝像。IP攝像機即將在很大程度上取代模擬攝像機，因其具有數位變焦和通過網際網路進行遠端監控的功能。

網際網路協定**(IP)**：TCP/IP通信套件的主要通信協定，用於跨網路邊界（路由器）和網際網路進行路由。另請參閱傳輸。

區域網路**(LAN)**：一種連接建築物、工廠、實驗室、學校或其他相對較小區域中的電腦和設備（包括機器）的電腦網路。

機器對機器**(M2M)**：直接發生在兩台機器之間的有線或無線通訊。

Modbus：一種最初由Modicon（現為Schneider Electric）發佈的用於其PLC的串列通信協定。另請參閱PLC。

多因素身份驗證**(MFA)**：一種僅在提供至少兩種形式的身份驗證後才授予存取權限的存取控制。

網路延遲：通過網路進行資料通信時發生的任何類型的延遲。稍微有延遲的網路連接稱為低延遲網路。延遲時間較長的網路連接稱為高延遲網路。

物件連結和嵌入**(OLE)**：一種允許將文檔嵌入並連結到其他物件的Microsoft專用技術。

OEE（整體設備效率）：是一種用於評估製造運營效率和減少生產機器停機時間從而提高生產效率的措施。

OpenSSL：對SSL和TLS協議的開放原始程式碼實現。另請參閱安全通訊端層(SSL)和傳輸層安全(TLS)。

原始設備製造商**(OEM)**：生產可由其他製造商行銷的零件和設備的公司。

外網管理：一種用於管理聯網設備的專用通信通道，例如遠端監控和配置。外網通信通道獨立於內網通信通道，因此不依賴於設備的運營通信通道（例如，網路連接）。

封包交換：在通信網路中使用的一種方法，其中資料以由報頭和有效載荷組成的資料形式傳輸到其目標位址。網路硬體根據報頭中的資訊通過最佳可用路徑將各個資料路由到目標位址，然後在目標位址以正確的順序重新組裝資料。

Ping：一種用於測試主機（例如，IP網路中的設備或機器）的可訪問性的實用程式。

過程現場匯流排**(PROFIBUS)**：自動化技術中的一種現場匯流排通信標準。

PLC：一種堅固耐用且適用於控制製造過程的工業電腦。

公開金鑰基礎設施**(PKI)**：一組用於創建、管理、分發、使用、存儲和撤銷數位憑證並管理公開金鑰（也稱為非對稱）加密的角色、策略和程式。

公共交換電話網**(PSTN)**：由國家、地區和本地電話運營商運營的所有全球電路交換電話網絡。

RJ45：用於連接語音和資料設備的標準通信網路介面。

基於角色的存取控制**(RBAC)**：一種基於分配給組織內單個使用者的指定角色來控制對電腦或網路資源的訪問的方法。

RS232：一種串列資料傳輸通信標準。

RS485：由電信工業協會和電子工業聯盟(EIA/TIA)定義的標準序列介面。也稱為TIA485 和EIA485。

安全散列演算法**(SHA)**：由美國國家標準與技術研究院(NIST)發佈的一系列加密散列函數。

安全通訊端層**(SSL)**：一種用於保護電腦網路通信的加密協定。

傳輸控制協議**(TCP)**：網際網路協定套件的主要協定之一，TCP作為該套件的兩個原始元件之一，是對網際網路協議(IP)的補充，因此整個套件通常被稱為“TCP/IP”。TCP確保將位元組流從一台電腦上的程式可靠有序地傳送到另一台電腦上的另一個程式。TCP是萬維網、電子郵件、遠端系統管理和檔案傳輸等主要網際網路應用程式所基於的協定。另請參閱網際網路協定(IP)。

虛擬私人網路絡**(VPN)**：用於使用加密連接和資料封裝在公共網路（例如，網際網路）中安全地擴展私人網路絡（例如，區域網路）的技術。另請參閱區域網路(LAN)。

廣域網路**(WAN)**：在很長的地理距離上延伸的一種通信或電腦網路。

無線數據機：一種繞過電話系統直接連接到無線網路的數據機，通過它可以直接訪問由網際網路服務供應商(ISP)提供的網際網路連接。

服務級別協定**(SLA)**：服務供應商和客戶之間涉及所提供服務的品質、性能、可用性和責任等特定方面的一種正式承諾。

網際網路協議安全**(IPsec)**：一套用於驗證並加密通過網路發送的資料的網路通訊協定。

網路隔離：將網路拆分為兩個區域網路、將不安全的電腦保留在第一個網路中並將您想要保護的電腦移動到第二個遮罩網路。

短信**(SMS)**：一種文本消息服務。

西門子多點介面**(MPI)**：一種基於EIA485（以前稱為RS485）標準且用於將PC、控制台和其他設備連接到Siemens SIMATIC S7 PLC的專有序列介面。另請參閱RS485 和PLC。

簡單網路管理協定**(SNMP)**：用於收集和組織網路中管理的設備相關資訊的標準網際網路協定。

使用者身份模組**(SIM)**：一種用於存儲在移動設備上識別和驗證使用者所用的國際移動用戶身份(IMSI)號碼及其關聯金鑰的積體電路(IC)。

監視控制和資料獲取**(SCADA)**系統：一種使用電腦、網路資料通信和圖形化使用者介面(GUI)進行高級過程監督管理的控制系統架構。

入侵偵測系統**(IDS)**：一種監控網路或系統是否存在惡意活動的硬體設備或軟體應用程式。

網路位址轉譯**(NAT)**：將一個IP位址映射到另一個IP位址的方法，例如：將一個專用IP位址映射到一個公共IP位址。

傳輸層安全**(TLS)**：一種用於保護電腦網路通信的加密協定。

通用序列匯流排**(USB)**：一種行業標準，定義了用於電腦與週邊設備之間的連接、通信和電源的電纜、連接器和通信協定。

虛擬網路計算**(VNC)**：一種用於通過向遠端PC發送鍵盤敲擊和滑鼠移動來遠端連接和控制另一台PC的圖形桌面共用系統。

X.509：一種定義了公開金鑰證書格式的加密標準。

司騰達股份有限公司

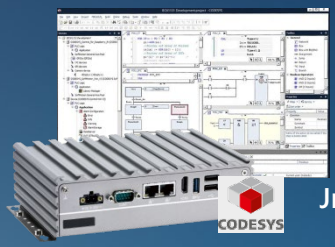
自動化工業與跨國遠端連線的最佳選擇

Ewon Cosy131
VPN 遠端連線

Ewon Flexy205
VPN+IOT 物聯網模組

Anybus X-Gateway

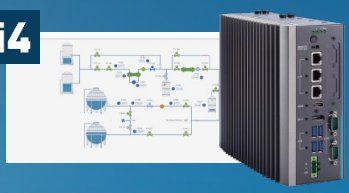
CODESYS SoftPLC



Jmobile HMI/SCADA IPC

工業 4.0 數位工廠與
工業物聯網解決方案

i4-SCADA IPC



WAGO750 Remote IO
EtherCAT / PROFINET

SIEMENS ET 200SP
PROFINET Remote Io

MR JET 系列
EtherCAT 伺服馬達

eSMART Web HMI
Esmart04/07/10

司騰達股份有限公司

台北營業所：235602 新北市中和區中山路 2 段 299 號 5 樓之 1
Tel：(02)-2242-1625　Fax：(02)-2242-1605

台中營業所：40760 台中市西屯區廣福路 186 號
Tel：(04)-2451-0611　Fax：(04)-2451-0612

E-mail：sales@bhp.com.tw

Line ID：@bhp.tw

司騰達股份有限公司
BHP Industry Solution

LINE

官網

了解更多產品詳細資訊請上官網查詢
www.bhp.com.tw