ShareTech OT防護設備

OTS-400

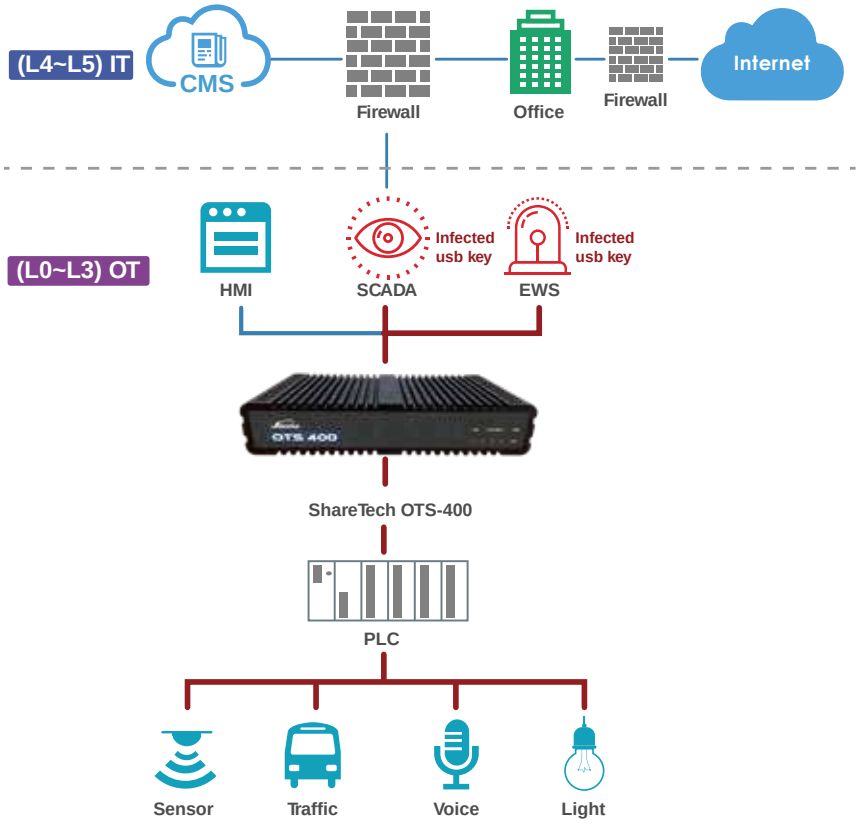
傳統 IT 的安全功能，像是防火牆設備主要是為企業網路安全而設計，以符合商用環境運作為首要目標。但是如果將商用的防火牆設備放置在工業控制系統(ICS)和SCADA網路環境就不一定適合，因為設備無法在嚴苛的工業環境中運作。

為了在PLC、RTU和其他裝置的工作環境，可以部屬一台安全、穩定的防護設備，眾至推出推出第一款OT防護設備OTS-400，適用於ICS、醫療產業、重要基礎設施等領域。

OTS-400硬體採無風扇設計，支援LAN BYPASS模式，可融合企業現有網路架構，內建ICS工業協定埠、內含深度封包檢測(DPI)、應用程式白名單、識別管理者身分、加密流量檢測、Virtual Patch、OPC防護，並能夠識別內容ID，具有保護內容、阻止惡意內容的能力。

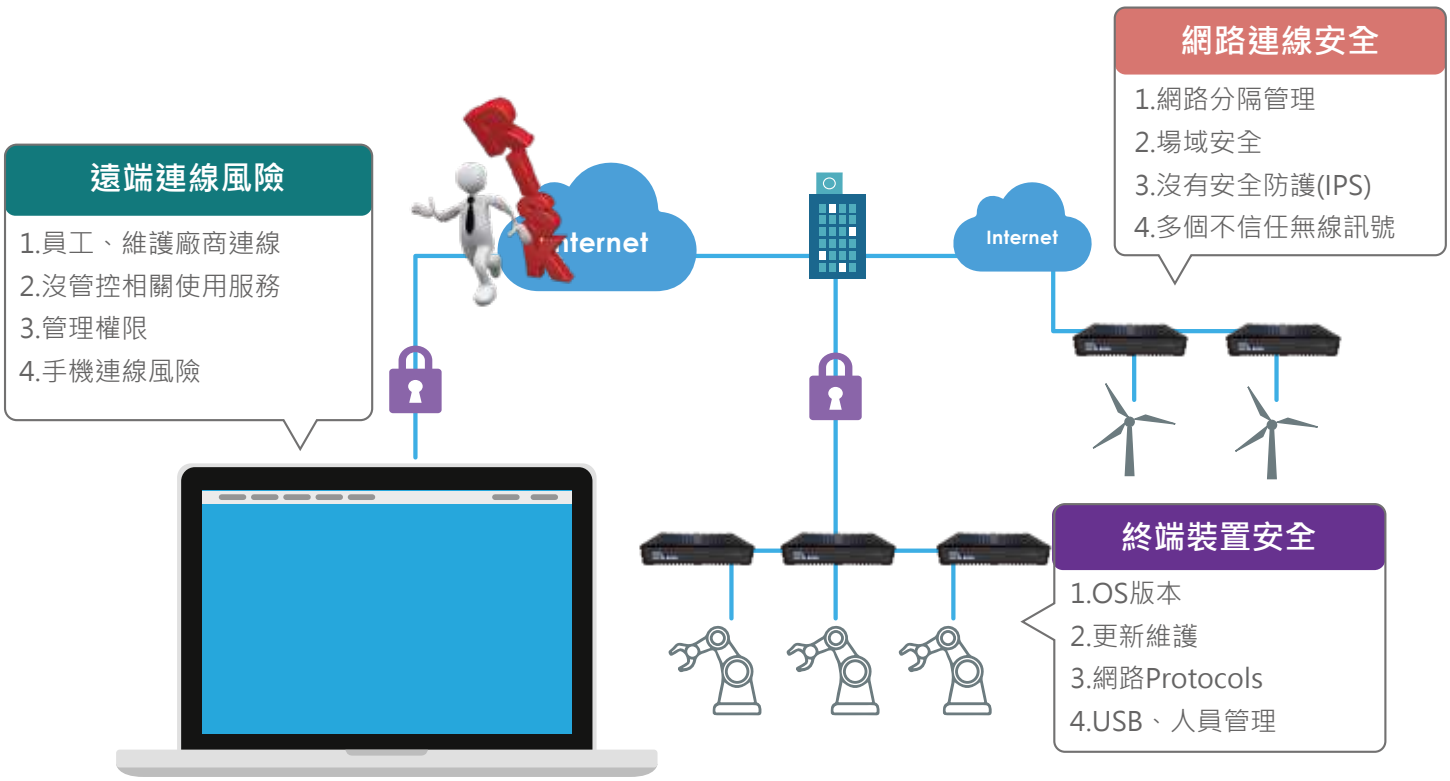
特 點

- 簡易布署、管理、維護
- 提高威脅的明見度
- OPC入侵防禦
- Virtual Patch防護
- 身分識別
- 大數據分析—服務、裝置
- 安全VPN連線
- 3G / 4G USB Module (optional)



OT環境的安全弱點

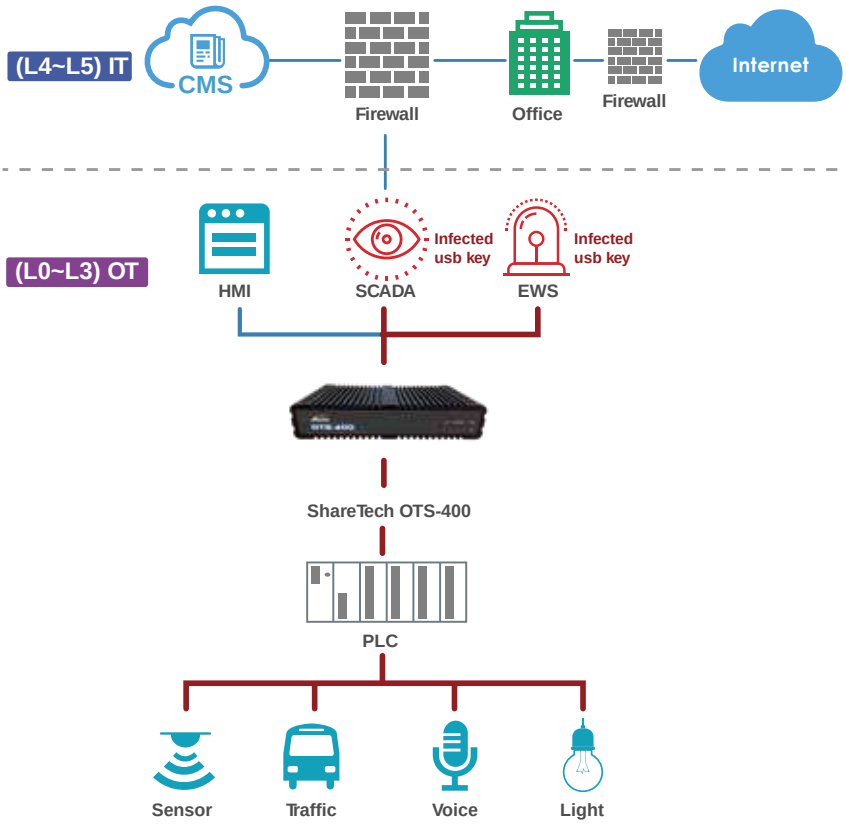
- **OT的灰色地帶：**未知的設備，未知的連線
- **不安全的身分驗證：**來自於設計及實施的缺陷
- **不安全的協議：**資訊無加密
- **缺乏保護的設備：**無可行的保護措施
- **不安全的第三方軟體：**終端管理裝置易受攻擊，可能一開始即受供應鏈的感染。



ShareTech OTS-400特點

將工業控制網路安全區域獨立隔離

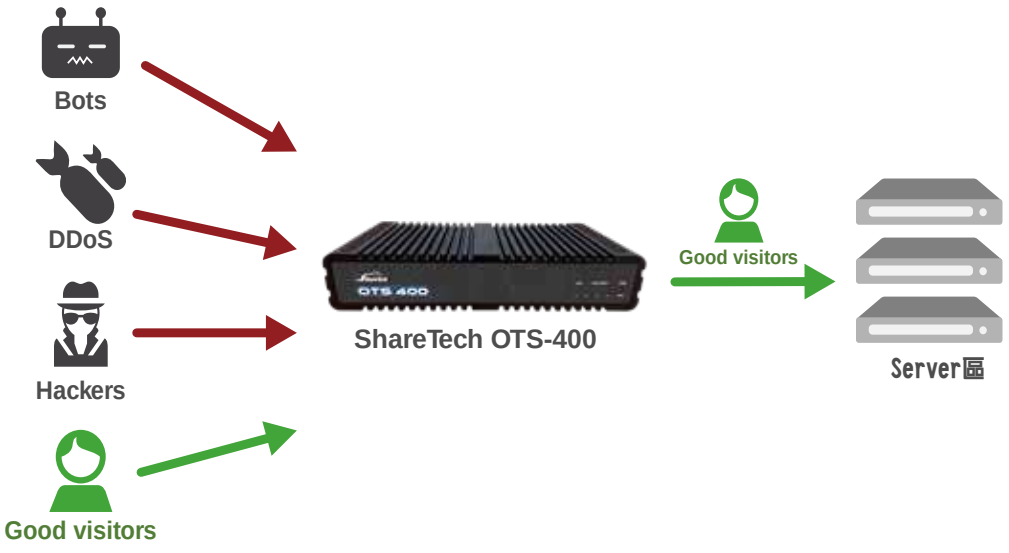
透過ShareTech OTS-400防護設備對工業控制網路安全區域進行隔離防護。工業企業應根據實際的情況，在不同網路邊界間或者各操作機台部署邊界安全閘道，實現安全的訪問控制、阻隔非法的網路連線，嚴格禁止沒有防護的工業控制網路與網際網路相連接。此外，也可以利用虛擬區域隔離、埠禁用的安全配置強化內網的安全。



降低控制機台系統漏洞風險

USB、光碟機、無線等工業主機設置，提供病毒、木馬、蠕蟲、惡意程式攻擊滲透的途徑，如果不能拆除或封閉工業主機上這些不必要的外設介面，讓它有機會對ICS或SCADA系統攻擊，可能會改變設備的生產流程，而遭到入侵的ICS、SCADA和其他OT系統可能會最佳後門途徑，惡意者容易透由路徑擷取內部重要網路資源。

加上多數的工廠操作系統多採用非標準軟體，無法進行及時修補。即使採用標準軟體系統，要進行修補也是很困難，因為OT環境大多採24x7全天服務，要停機更新系統是一項非常重大的任務。OTS-400內建虛擬補丁防護，幫助一些無法上Patch或更新韌體的老舊設備，從外圍阻絕攻擊流量。



監控工控網路傳輸行為，並對病毒與漏洞進行處置

對網路異常行為或攻擊模式都能嚴密監測、及時發現處置、並能完整記錄報告，是工控環境營運能穩定最重要因素。ShareTech OTS-400在一般情況下可以透過流量分析與漏洞掃描，對工控網路中存在的病毒與漏洞進行掃描，且對網路攻擊和異常行為進行識別、告警、通知與記錄所有相關威脅紀錄。當發現傳輸的流量超過平均標準設定值、加密封包有夾帶惡意封包、異常的指令、病毒木馬程式滲透攻擊，都可即時過濾阻隔，降低危害。

隔離感染面，防止威脅擴散

對於透過技術手段，確認威脅的感染面，盡快採取應急的隔離手段。ShareTech OTS系列可以與交換器協防，除了可以對網路進行分區隔離，讓各自生產線獨立運作，避免當其中一個生產線遭受惡意攻擊時，間接影響其他營運。眾至提供的不是只針對單一點進行控管、而是希望能涵蓋整個面進行完整防護，避免災情擴散。

支援工業網路通訊協定

內建業界常用的工業控制協定，例如，EtherCAT 使用TCP/UDP 34980、EtherNet/IP 使用 TCP 44818 UDP 2222，管理者只要選取這一些協議名稱，會自動對應出應該開放的Port 號，至於其他的通訊PORT當然是全部被關閉。

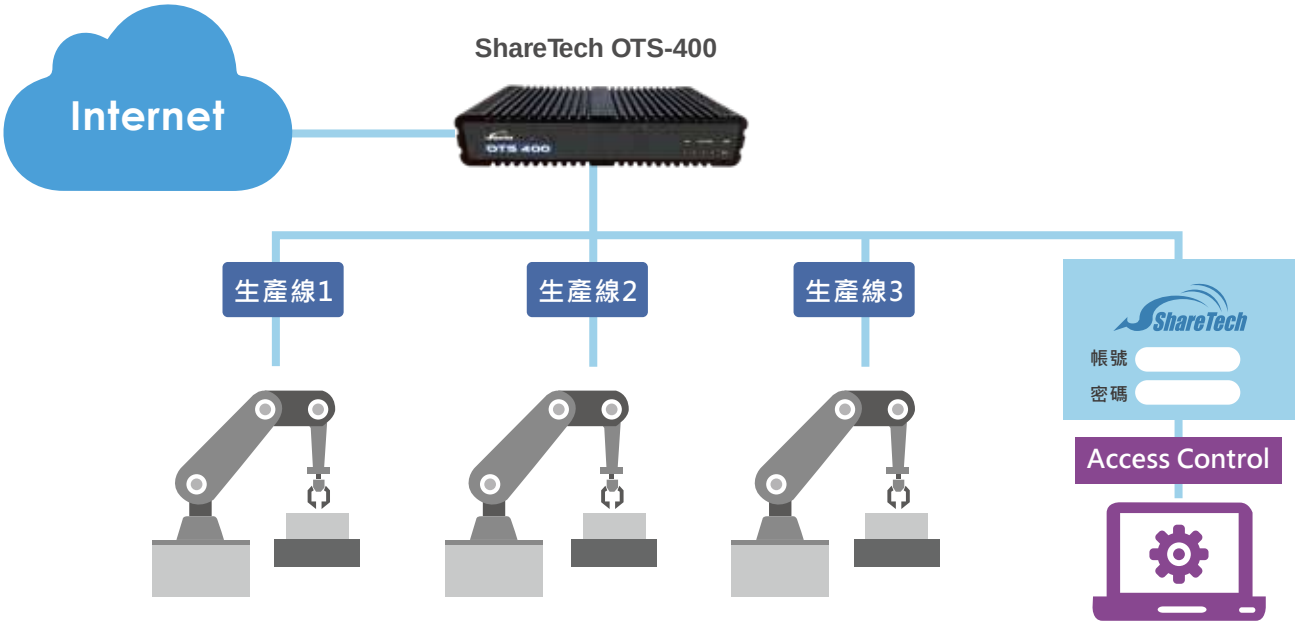
以電腦組裝線為例，若封包夾帶可疑的參數，要求機械手臂執行標準以外動作，OTS-400在接獲數據封包後，將進行封包分析、阻擋，降低電腦廠商蒙受巨額財物損失。

專屬OPC入侵防禦機制

OPC防護是針對OT攻擊防禦最佳解決方案，收集所有IT、OT網路的封包與訊號，並且採用深度封包檢測（DPI）的方式進行比對，分析通訊協定當中的每個層級，掌握出現異常數據的行為。讓管理者可以在與關鍵工控設備連接的網路路徑上，及時偵測到攻擊事件的發生、並依照管理員的設定，中止或阻絕入侵行為，包括自動攔截棄置攻擊封包，並依據設定，留下攻擊的記錄即通知管理者等連續的應變措施。

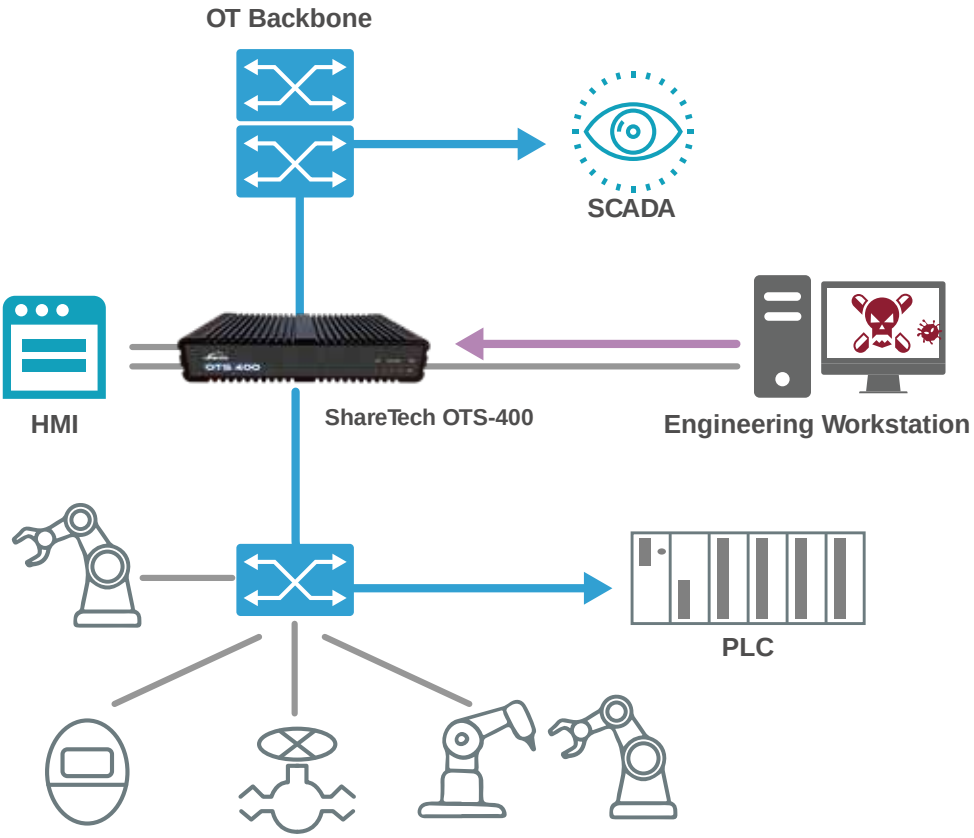
身分識別與存取管理

身分識別與存取管理屬於傳統安全領域，對工業控制系統安全來說也是一個相當重要的層面。在工控環境系統，有些單位為了遠端管理的便利性，使用SSH、Telnet、網頁登入連線模式，如果沒有採取任何安全管理措施，例如：只限定某些特定IP才能存取，或者必須經過身分認證後才能使用服務，否則讓駭客輕易入侵系統管控設備，容易引起大災難。ShareTech OTS-400提供本機使用者/AD/POP3/Radius認證授權機制，可協助館已人員與監控企業內部所有使用者帳號，在確認使用者的ID的有效授權之後，才能允許其使用網路，讓企業可以有效管理網路使用資源。



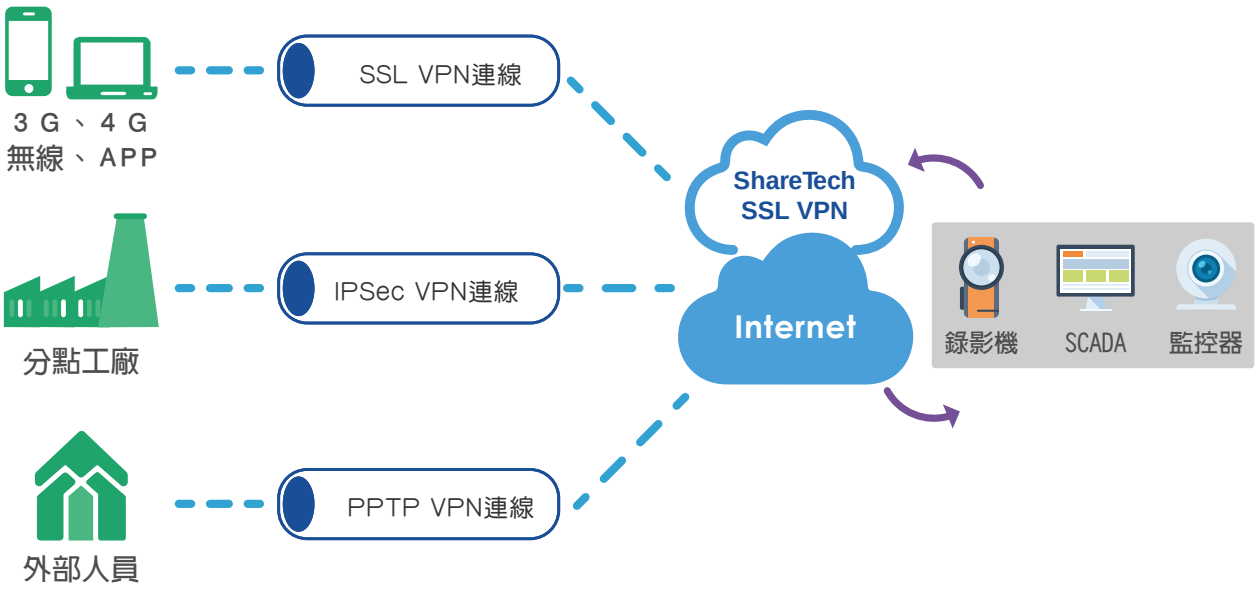
應用程式白名單

由於惡意程式的變種速度太快，如果靠黑名單來做把關可能沒那麼可靠，所以對OT設備的軟體管理權限，應該都用白名單機制來進行控管。在OT場域裡具有極少變動的特性，通常系統在安裝後，應用程式即維持不變。管理者可以決定哪些程式是允許被執行，其餘的程式將被阻擋。當所有程式被允許執行時，應用程式白名單可以過濾內容或限定其頻寬使用量。



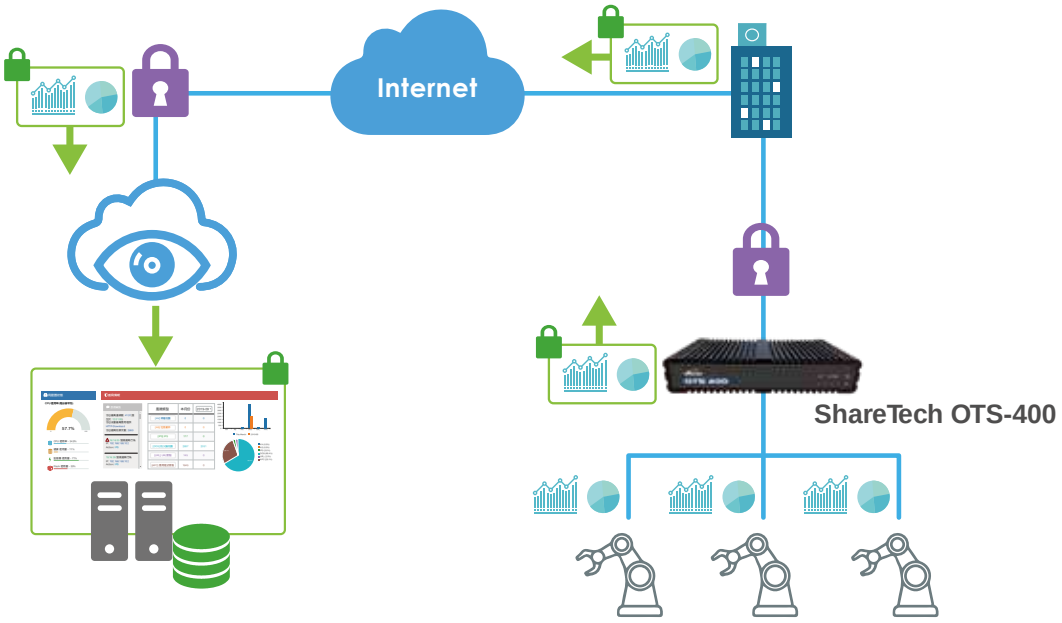
安全遠端連線模式(VPN)

有時候工業企業需要透由遠端進行維護管理，對單位來說應通過遠端認證連線、加密模式確保其連線安全後，才可以允許其操作。ShareTech OTS-400可在網絡邊界使用單向隔離裝置、VPN等方式實現數據單向訪問，並控制訪問時限，並有稽核相關日誌提供日後稽查佐證。目前安全連線支援IPSec、PPTP、L2TP、SSL VPN等連線模式。



威脅情報資訊Dashboard

有效收集OT設備與網路資訊，在ShareTech「戰情室-威脅情報資訊」進行智慧化的分析與檢測，達到即時和準確的資安狀態呈現與保護的效果。



設備災難復原機制

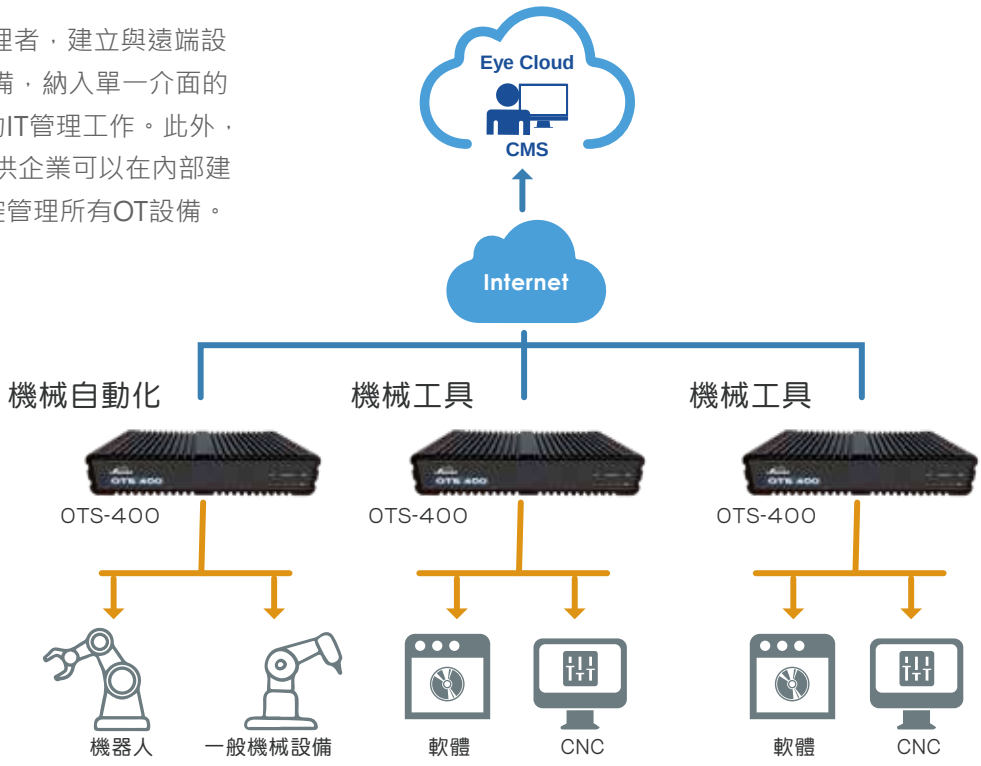
當設備因外在事故無法正常運作時，ShareTech OTS-400硬體支援LAN BYPASS模式，不影響工廠生產營運，如果是硬體損壞無法運作，管理人員透由設備內建USB插槽，平時做好設定檔備份動作，當設備真的無法運作，只要立即更換一台，將原本USB換插到新機上開啟電源，就會自動將原本的設定檔資料帶入，不用5分鐘完成災難救援的服務。

支援3G / 4G USB

OTS-400硬體USB埠口能用來連接3G / 4G USB，最多可同時啟用3個WAN連線進行負載平衡或是備援動作。

支援CMS與雲端管理平台

OTS-400支援CMS功能，可以提供管理者，建立與遠端設備之間的連線，將該單位的OT防護設備，納入單一介面的集中管理架構，以簡化企業整體環境的IT管理工作。此外，亦提供雲端管理平台，ShareTech提供企業可以在內部建置一個私有的雲端管理平台，快速監控管理所有OT設備。



硬體簡介

硬體外觀

- 網路埠：4個GbE埠（4個RJ-45埠）
- Console埠：1個
- USB 2.0：2
- Bypass：1組

效能

- 防火牆吞吐量：1.5 Gbps
- VPN吞吐量：200 Mbps（IPsec AES）
- OPC防護：380Mbps
- 防毒：250Mbps
- 最大連線數：15萬個
- 支援通訊協定：Modbus、DNP3、IEC-104、EtherNet/IP、LanWorks、IEC-61850、BACNet、AXView2.0

安裝方式

- 直立(加購)

尺寸大小

- 外觀：240 x 120 x 50 mm

電源

- 24W Power Adapter

適用環境

- 運作環境溫度：攝氏0度到40度
- 操作濕度：10%~85%，相對濕度，非作業期間