SKKYNET

宏虹 HONGHONG

在不暴露網路的情況下訪問您的數據

WHITE PAPER

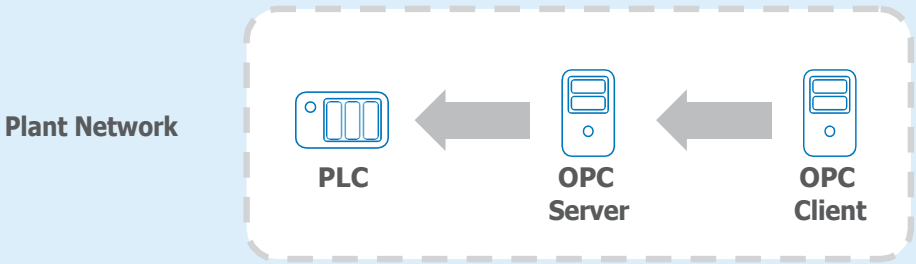
工業物聯網和工業 4.0 的安全遠端訪問

工業物聯網和工業4.0帶來了根本的安全挑戰。一方面，在首次設計工業系統時，從未考慮過在工廠網路之外的連接，因為當時還沒有這種需求。
另一方面，IIoT和工業4.0需要與工業連接
系統，無論是從公司 IT 網路內部還是通過互聯網從遠端位置。這種訪問工業數據的需求提出了一個問題：在允許遠端訪問數據的同時，保持任務關鍵型系統所需的高級別安全性的最佳方法是什麼？

傳統用戶端-伺服器體系結構

這一基本問題凸顯了對IIoT和工業4.0的新型安全設計方法的需求。到目前為止，大多數控制系統的架構，例如工廠和管道中使用的控制系統，都假設它們在安全的範圍內運行。防火牆、DMZ，有時甚至是氣隙已被用於確保沒有人可以從外部訪問工廠網路。

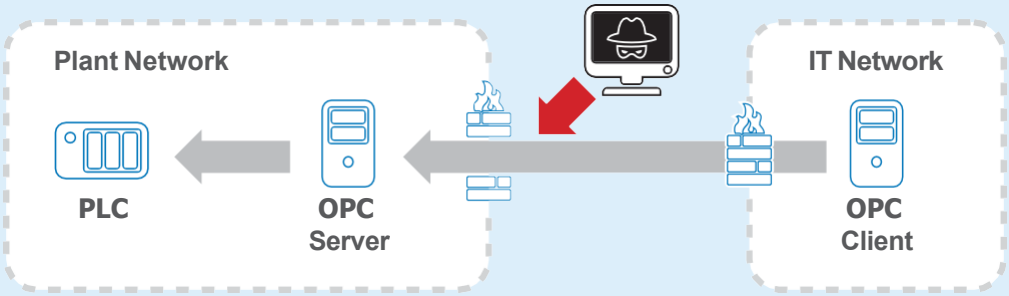
在此週邊工廠網路通常使用 OPC 等工業協定將 PLC 和其他設備連接到 SCADA 系統、HMI 和其他用戶端。在這個自給自足的世界中，OPC伺服器連接到PLC以收集其數據。然後，歷史資料庫、HMI 或 SCADA 控制面板等 OPC 用戶端連接到 OPC 伺服器以訪問該數據。只要網路與外界關閉，該過程及其數據就是安全的。



從其他位置訪問

傳統架構在 工廠的安全範圍內運行良好。但是，當有人想從另一個位置訪問工廠數據時會發生什麼？

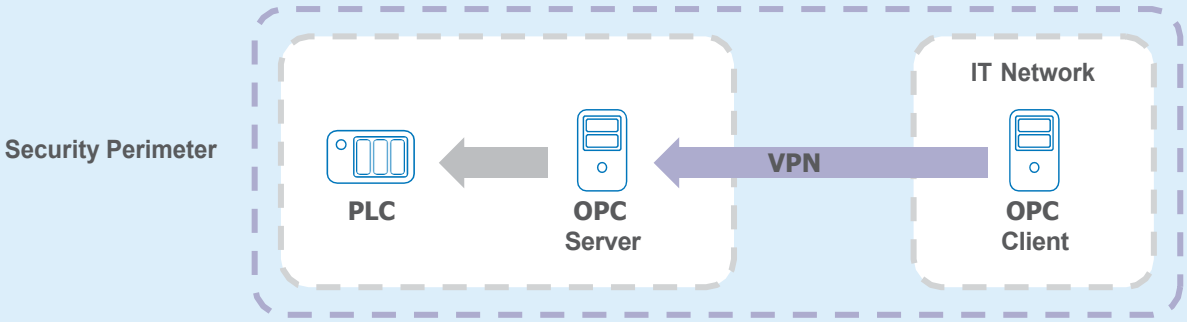
將遠端 OPC用戶端放在工廠外部（例如，在IT網路上）並連接到工廠內的OPC伺服器需要在工廠網路上 打開防火牆埠。這使網路受到 攻擊，並且是一個嚴重的安全問題。



為什麼不使用 VPN？

可能想到的一種解決方案是使用VPN（虛擬專用網路）。但是，VPN實際上並不能解決安全問題。VPN 有效地將安全邊界擴展到 工廠網路之外，以包括 IT 網路 。

這會將攻擊面擴展到兩個網路。更糟糕的是，VPN上的安全漏洞將使兩個網路上的所有系統都受到 攻擊。VPN不僅僅是共享過程數據，而是共用整個網路。



對美國Target連鎖店的高度宣傳攻擊就是一個很好的例子。獲得對公司系統的VPN訪問許可權的承包商是網路釣魚攻擊的受害者。通過訪問承包商的系統，

攻擊者找到了必要的 VPN 憑據，然後進入目標系統。他很快就找到了客戶 記錄和信用卡號碼的方法，並度過了一天。

同樣，VPN不會保護工業系統免受WannaCry攻擊。該病毒通過電子郵件到達，然後卸載了攻擊網路上所有電腦的“蠕蟲”。登錄到VPN的任何受攻擊的計算機都會自動感染所有其他計算機。

Microsoft開發人員Clemens Vasters詳細研究了將VPN用於工業應用的缺點。在一篇題為《物聯網：VPN是假朋友嗎？Vasters說：“VPN提供了一個虛擬化和私有（隔離）的網絡空間。安全隧道是
一種機制，用於實現進入該空間的適當保護路徑，但空間本身根本不安全。

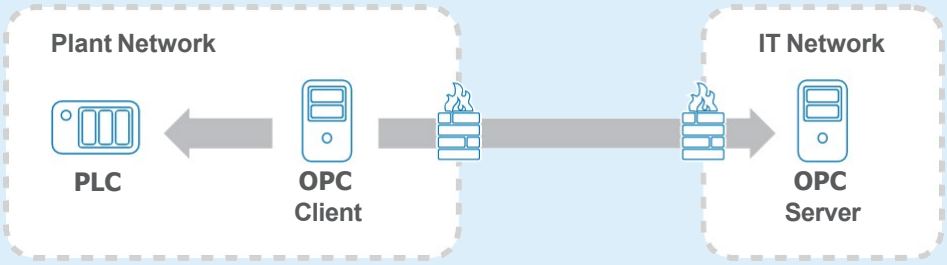
已建立的 VPN 空間完全是一個功能。對鏈路層上方的所有協定和流量透明。

為什麼不反轉連接？

打開防火牆埠的問題是由於 與工廠的入站連接造成的。如果有一種方法可以使連接出站而不是入站連接，則可以克服此漏洞。那麼為什麼不切換客戶端和伺服器位置呢？在用戶端/伺服器關係中，連接始終由客戶端啟動，因此要建立出站連接，您可以將用戶端放在工廠內，向外連接到 IT 網路上的 OPC 伺服器。

這將提供出站連接，但不提供數據。客戶端必須從伺服器獲取其初始數據值和更新。如果伺服器不在工廠網路上且未連接到數據源，則無法提供該 資訊。

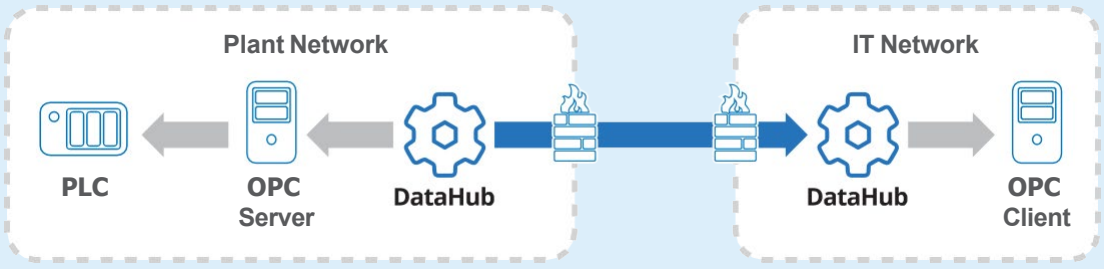
儘管簡單地切換伺服器和用戶端的位置是行不通的，但建立出站連接仍然是最安全的方法。還有其他方法可以做到嗎？



不同類型的出站連接

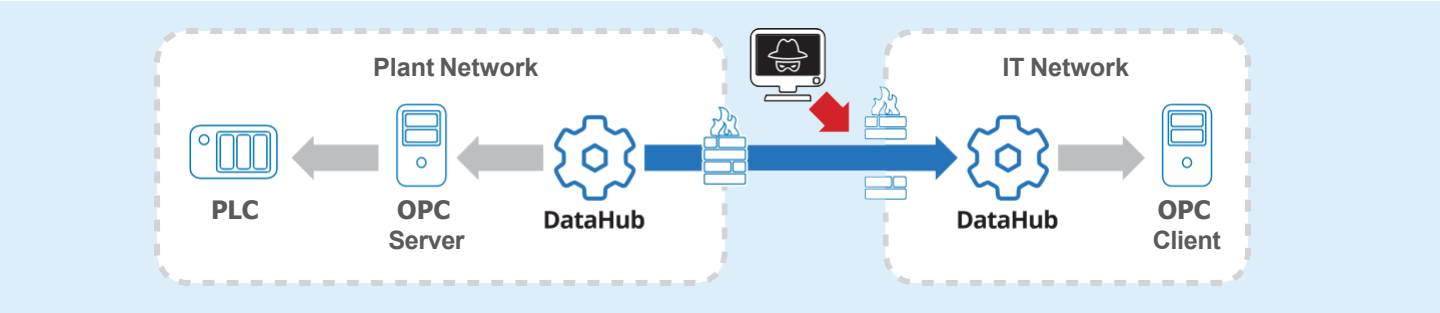
Cogent DataHub® 在連接方式上非常靈活 。當一個數據中心連接到另一個數據中心時，任何一個都可以啟動連接，並且 任何一個都可以配置為受信任的權威
數據源。（我們所說的“權威”是指
在網路上斷開連接/重新連接時具有正確數據的連接。

分配受信任數據源以及建立連接的人員的能力解決了用戶端/伺服器問題，因為現在數據的權威源也可以啟動
連接。因此，通過將一個 DataHub 放在工廠網路上，將另一個 DataHub 放在遠端位置，您可以從工廠網路建立出站連接，並且仍然保持數據的正確許可權。



與傳統伺服器/客戶端關係的根本區別是Skkynet為IIoT和工業4.0提供的安全設計軟體和服務的基礎。僅使用 DataHub 進行出站連接可使所有工廠防火牆保持關閉，並保護工廠網路免受攻擊。

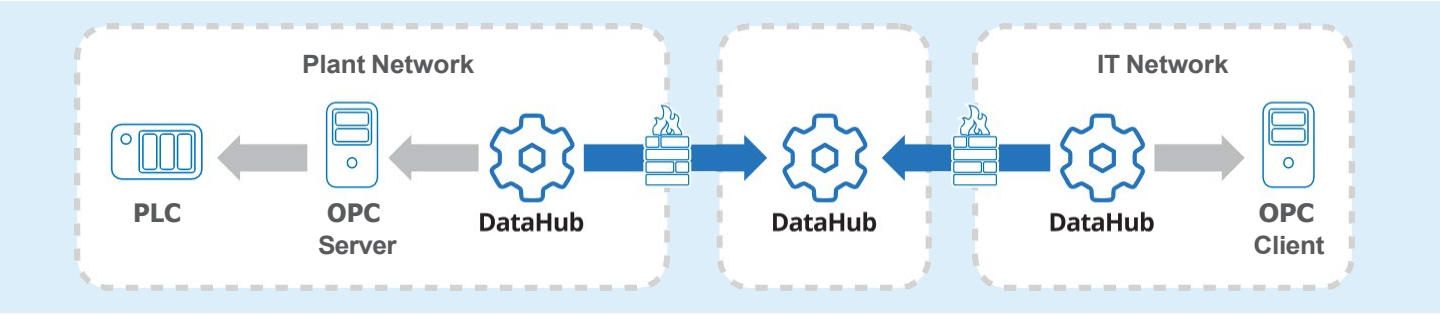
根據您的安全要求，這可能就是所有需要的。但這個故事還有更多。儘管工廠網路受到保護，但遠端位置現在必須打開防火牆，使其受到攻擊。



理想情況下，所有連接，無論是來自工廠網路、IT 網路還是任何其他遠端用戶端，都應僅出 站。這將鎖定兩個網路上的防火牆 ，不會提供攻擊面。

安全中間件

伺服器和客戶端系統可以通過在中間放置另一個 DataHub 來保護，該資料中心接受傳入連接並代理源和使用者之間的數據交換。



這樣，工廠和IT網路都只建立出站連接。同時，由於從源到使用者的通信鏈上的每個數據中心 都是單獨配置的，因此鏈中的每個環節
成為可信的權威數據源。因此，如果有的話
部分網路出現故障，用戶端收到通知，當重新建立連接時，它會使用來自源的最新可信數據進行更新。

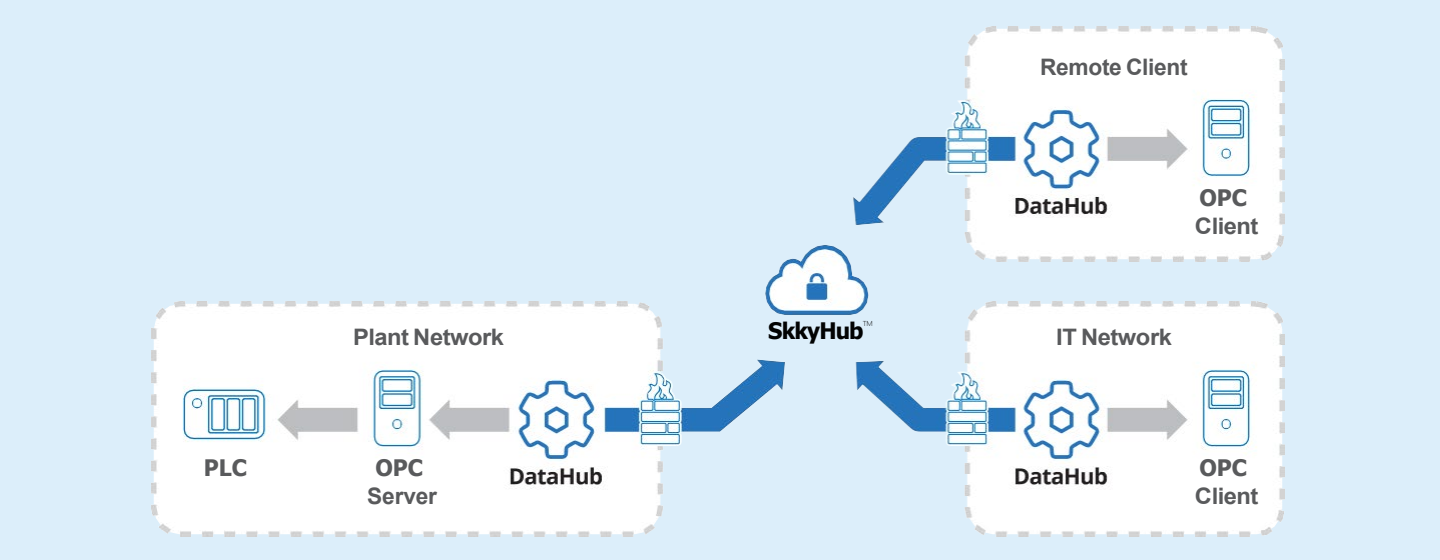
隨著工廠和IT網路上的所有防火牆都關閉，系統的潛在攻擊面現在已經轉移到中間的DataHub，從而降低了安全問題的複雜性。中央數據中心現在可以託管在安全的 DMZ 計算機上，該計算機可以配置為管理安全風險。DMZ 可以在公司網路或私有雲系統上運行。

雲服務

作為使用本地 DMZ的替代方法， SkkyHubTM 服務在雲中運行的 DMZ中提供完全託管的 DataHub。借助 SkkyHub，工廠數據可以安全地與遠端使用者共享，從而消除了第三方連接到本地 DMZ或工廠網路的不確定性。

事實上，SkkyHub服務甚至可以完全取代本地 DMZ，節省資源併為工廠和IT網路提供安全的出站連接。

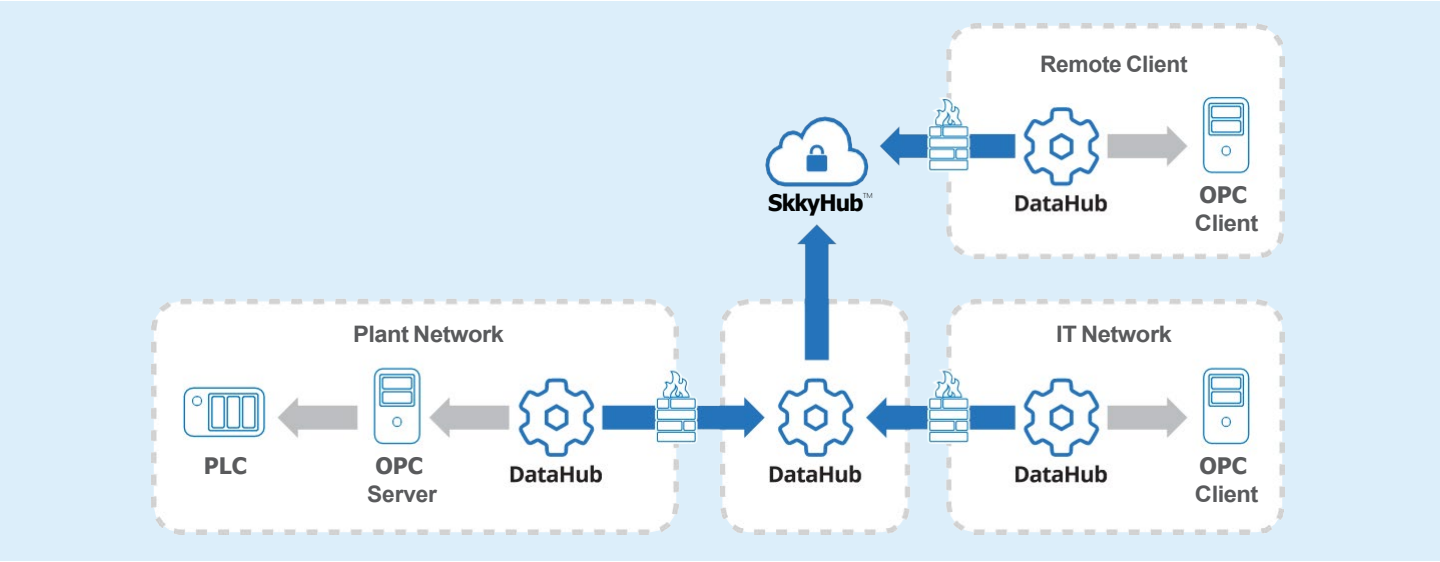
SkkyHub服務提供安全的數據連接和集成，使幾乎任何工業系統或嵌入式設備都可以輕鬆連接和聯網。它接受來自DataHub的入站連接，並提供內置的基於 Web的人機介面，允許使用者從幾乎任何地方監控或控制他們的過程或設備，無需程式設計。



混合雲

最後，還可以將基於DMZ的本地解決方案與SkkyHub相結合，以創建混合雲服務。

通過 DMZ 伺服器提供強大的本地網路，以及與雲的安全出站連接，以便遠端存取資料。如果互聯網連接中斷，IT網路將保持連接。



共用您的數據，而不是您的網路

以下四種方法中的任何一種：與DataHub建立安全的出站連接，或者在混合雲中使用DMZ或SkkyHub，或兩者兼而有之，提供對過程控制數據的相同，基於DataHub的安全訪問，沒有VPN 並且工廠網路上沒有開放的防火牆埠。

這 DataHub和SkkyHub安全設計架構可讓您共享數據，而不是網路。這就是如何保持關鍵任務系統的安全，同時全面參與工業物聯網和工業4.0。