*從OT與IT的差別

解讀工控系統資訊安全防護指南

鄭春光

民國108年9月23日

大綱

一、 OT與IT的差別
二、專屬的ICS系統在資訊安全上的困境
三、工業控制系統通用性防護參考資源
四、解讀工控系統資訊安全防護指南
五、總結

*IT與OT的差別

*幾十年來，我們將計算機和資料網路稱為資訊技術(IT; information technology)；工業控制系統(ICS; industrial control system)的操作和程序控制，則通稱為營運技術(OT; operational technology)。OT採用專屬軟硬體架構，在隔離和獨立的網路中執行，目標與要求和IT完全不同。但這些已開始發生變化。連網環境日益普及，形成了物聯網及工業物聯網，而使得兩個世界的系統出現了彼此連接的可能性。工業控制系統從單機走向互聯，從封閉走向開放，從自動化走向智慧化。

* ICS廠商為降低成本、即時存取與系統自動化等需求，原本是以專屬軟體、硬體和通訊協定所開發；現在開始運用通用的網路系統來連接企業與外部的網路，使用市售的現成軟、硬體來組建ICS系統，以便降低產品製造與維運的費用，並且提高生產力。

* ICS系統採用這樣的開放、通用性的架構之後，雖然縮短了OT與IT之間的差異，卻也帶來過去所不曾出現的安全性弱點，和IT系統一樣，受到病毒、蠕蟲、木馬等惡意軟體的嚴重威脅。

* OT與IT的區隔日益模糊，但本質上的差異仍然存在，要強化關鍵基礎設施的網路安全，應從了解OT與IT之間的差別開始做起。

*為何傳統資訊安全產品不能解決工控安全問題？

*工控系統具獨特性，IT資安產品係針對IT需求開發
*傳統防火牆不理解、不支援工控協議
*傳統防火牆不適應工業網路對即時性的要求
*傳統防火牆不支援OPC協議的動態埠分配
*防毒軟體通常得不到及時更新
*系統漏洞無法及時修復

*專屬的ICS系統在資訊安全上的困境(1)

*由於系統必須持續運作，若要停機來執行安全更新，相當困難，也可能會因此耗費許多成本，而且有些ICS系統一旦關機、重新啟動，在系統無法運作的期間，可能會導致重大損失。

*工業系統的生命週期高達15~20年或更久，但這些系統設計製造之初，往往並未將資訊安全的需求考量在內，系統資源僅供控制用，機器只要穩定運行就會儘量不更新或延後更新，使得內部系統充滿漏洞，風險極高，以往採用的實體隔離為基本保護策略，使得ICS的韌體與軟體難以替換，更新修補程式也很少有機會安裝

*ICS所連接的網路設備，防禦能力可能也不足，無法偵測與處理惡意型態的流量，或是大型正常流量。但資料交換區很可能是關鍵問題，功能越智慧就越難進行隔離。

*專屬的ICS系統在資訊安全上的困境(2)

*ICS韌體與軟體之很難更新，因為套用修補程式，以及防毒軟體的定義檔之前，均需經過測試、批准安裝、排程執行與驗證等流程，以確保系統能夠安全、持續地進行相關作業控制。

*ICS技術支援服務通常由外部廠商來提供，而這些系統在建置部署時，通常只會套用產品出廠預設的組態。

*使用者在系統執行工程作業、各種操作、技術支援等工作時，通常是以遠端登入的方式進行，這也意味著ICS有可能出現連線不安全，以及非法連線的情況。

*ICS設備的操作手冊大多可公開取得，因此能拿到相關資料的人士，不只是ICS系統的合法使用者，也包括有意發動攻擊者。

*IT系統與ICS系統的主要差別

分類	IT系統	ICS系統
性能要求	非實時性； 響應(respond)必須是持續性的； 需要高吞吐量； 高的延遲和抖動是可接受的。	實時性(real time)； 實時響應； 一定程度的吞吐量是可接受的； 高的延遲和抖動是不可接受的。
可用性要求	重新啟動是可以接受的； 根據系統操作要求，可用性的不足通常是可以容忍的。	由於生產過程可用性要求，類式重新啟動這樣的響應是不能接受的； 根據可用性要求，需要冗餘系統； 斷電要提前數天/數週進行計畫和確定時間表； 高可用性要求進行完全徹底的測試。
風險管理要求	首先保證數據機密性和完整性； 故障容忍不是第一重要，瞬間停機不是主要風險； 主要風險來自商業動作的延遲或中斷。	首先保證人身安全其次才是保護生產過程； 第一重要的是故障容忍，甚至瞬間停機也是不能接受的； 主要風險是監管違規，環境破壞，人、財、物的損失。
體系結構的資訊安全焦點	主要是保護IT資產，以及在這些資產中儲存或傳輸的資訊； 中央伺服器需要更多保護。	主要目標是保護現場系統如PLC、DCS等； 對中央伺服器的保護也很重要 。

分類	IT系統	ICS系統
非預期後果	傳統IT系統有資訊安全解決方案。	一定要測試資訊安全工具(ICS系統的離線測試，以確保他們不會影響到正常的ICS操作。
時間關鍵相互作用	很少關鍵緊急事件； 限制訪問控制可以透過對資訊安全要求的程度來實現。	對人員和其他緊急事件的響應是非常關鍵的； 對ICS系統的訪問要控制，但不應阻礙或干擾到人機互動。
系統操作	使用典型的操作系統； 應用自動化工具進行系統的直接升級。	不同的或者專用的操作系統，通常沒有內在的資訊安全能力； 更改軟體要非常慎重，通常由軟體供應商進行因為涉及到特定的控制算法以及可能會修改相應的硬體和軟體。
資源限制	系統有足夠的資源以支持諸如來自第三方的資訊安全解決方案。	系統支持固定的工業生產過程，因而沒有足夠的內存(RAM)或資源支持資訊安全能力。
通信	標準的通信協議； 主要是有線網路，局部可能會有無線通信能力； 典型的IT網路規程。	很多專用的和標準的通信協議； 多種類型的通信媒介包括了有線和無線(無線電和衛星)； 網路結構複雜(現場層、控制層、管理層等)。

分類	IT系統	ICS系統
變更管理	軟體變更多樣性，並且有著很好的資訊安全策略和規程，過程是自動進行的。	軟體更新要進行測試並且逐步布置到系統中，以確保控制系統的可維護。ICS的斷電要進行計畫和確定時間表，ICS也可能在使用沒有技術支持的操作系統(舊版本)。
技術支持	允許多樣化的服務。	技術支持只有供應商獨立進行。
部件(assembly unit)生命週期	一般是3到5年	一般15到20年
部件訪問	通常是本地，並且易於訪問。	通常是分離的，遠端的，並且需要其他的實體媒介才能夠進行訪問。

*工業控制系統通用性防護參考資源

- *美國國家標準暨技術研究院-- NIST SP800-82 r2 Guide to Industrial Control Systems (ICS) Security
- *國際電工協會 (International Electrotechnical Commission)--IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
- *北美電力可靠度協會(NERC)提出之The critical infrastructure protection cybersecurity standards (*CIP Version 5*)
- *美國核子管理委員會(NRC)提出之REGULATORY GUIDE 5.71 (New Regulatory Guide) CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES
- *行政院資通安全處--關鍵資訊基礎設施資安防護建議
- *中國大陸「工業控制系統信息安全防護指南」
- *中國大陸GB/T 33009.1「工業自動化和控制系統信息安全集散控制系統(DCS)第1部分：防護要求」

*解讀《工業控制系統資訊安全防護指南》

- 工業控制系統資訊安全事關經濟發展、社會穩定和國家安全。近年來，隨著工業化和資訊化融合的不斷深入，工業控制系統從單機走向互聯，從封閉走向開放，從自動化走向智慧化。在生產力顯著提高的同時，工業控制系統面臨著日益嚴峻的資訊安全威脅。
- 應對新的工控安全形勢，提升工業企業工控安全防護水準，中國大陸工業和信息化部(工信部)編制本《指南》，指導工業企業開展工控安全防護工作。
- 以當前工業控制系統面臨的安全問題為出發點，注重防護要求的可執行性，從管理、技術兩方面明確工業企業工控安全防護要求。
- 《指南》堅持企業的主體責任及政府的監管、服務職責，聚焦系統防護、安全管理等安全保障重點，提出了11項防護要求，並做了具體官方解讀。

指南重點

文件要求在工業主機上採用經過離線環境中充分驗證測試的防毒軟體或應用程式白名單軟體，只允許經過工業企業自身授權和安全評估的軟體運行。解讀：工業控制系統對系統可用性、即時性要求較高，工業主機如MES伺服器、OPC伺服器、資料庫伺服器、工程師站、操作員站等應用的安全軟體應事先在離線環境中進行測試與驗證，其中，離線環境指的是與生產環境實體隔離的環境。驗證和測試內容包括安全軟體的功能性、相容性及安全性等。

文件要求通過工業控制網路邊界防護設備對工業控制網路與企業網或互聯網之間的邊界進行安全防護，禁止沒有防護的工業控制網路與互聯網連接。解讀：工業控制網路邊界安全防護設備包括工業防火牆、工業網閘、單向隔離設備及企業定制的邊界安全防護閘道等。工業企業應根據實際情況，在不同網路邊界之間部署邊界安全防護設備，實現安全存取控制，阻斷非法網路訪問，嚴格禁止沒有防護的工業控制網路與互聯網連接。

文件要求原則上嚴格禁止工業控制系統面向互聯網開通HTTP、FTP、Telnet等高風險通用網路服務。解讀：工業控制系統面向互聯網開通HTTP、FTP、Telnet等網路服務，易導致工業控制系統被入侵、攻擊、利用，工業企業應原則上禁止工業控制系統開通高風險通用網路服務。

文件要求在工業控制網路部署網路安全監測設備，及時發現、報告並處理網路攻擊或異常行為。解讀：工業企業應在工業控制網路部署可對網路攻擊和異常行為進行識別、警報、記錄的網路安全監測設備，及時發現、報告並處理包括病毒木馬、埠掃描、暴力破解、異常流量、異常指令、工業控制系統協定封包偽造等網路攻擊或異常行為。

文件要求對靜態存儲和動態傳輸過程中的重要工業資料進行保護，根據風險評估結果對資料資訊進行分級分類管理。解讀：工業企業應對靜態存儲的重要工業資料進行加密存儲，設置存取控制功能，對動態傳輸的重要工業資料進行加密傳輸，使用VPN等方式進行隔離保護，並根據風險評估結果，建立和完善資料資訊的分級分類管理制度。

文件要求在選擇工業控制系統規劃、設計、建置、運維或評估等服務商時，優先考慮具備工控安全防護經驗的企業單位，以合約等方式明確服務商應承擔的資訊安全責任和義務。解讀：工業企業在選擇工業控制系統規劃、設計、建置、運維或評估服務商時，應優先考慮有工控安全防護經驗的服務商，並查核其提供的工控安全合約、案例、驗收報告等證明資料。在合約中應以明文條款的方式約定服務商在服務過程中應當承擔的資訊安全責任和義務。

文件要求以保密協定的方式要求服務商做好保密工作，防範敏感資訊外泄。解讀：工業企業應與服務商簽訂保密協定，協定中應約定保密內容、保密時限、違約責任等內容。防範工藝參數、設定檔、設備運行資料、生產資料、控制指令等敏感資訊外泄。

*(一)安全軟體選擇與管理

1. 在工業主機上採用經過離線環境中充分驗證測試的防病毒軟體或應用程式白名單軟體，只允許經過工業企業自身授權和安全評估的軟體運行。

解讀：工業控制系統對系統可用性、實時性要求較高，工業主機如MES伺服器、OPC伺服器、資料庫伺服器、工程師站、操作員站等應用的安全軟體應事先在離線環境中進行測試與驗證，其中，離線環境指的是與生產環境實體隔離的環境。驗證和測試內容包括安全軟體的功能性、相容性及安全性等。

2. 建立防毒和惡意軟體入侵管理機制，對工業控制系統及臨時接入的設備採取病毒查殺等安全預防措施。

解讀：工業企業需要建立工業控制系統防病毒和惡意軟體入侵管理機制，對工業控制系統及臨時接入的設備採用必要的安全預防措施。安全預防措施包括定期掃描病毒和惡意軟體、定期更新病毒碼、查殺臨時接入設備(如臨時接入USB、可攜式終端等外部設備)等。

*(二)配置和補丁管理

1.做好工業控制網絡、工業主機和工業控制設備的安全配置，建立工業控制系統配置清單，定期進行配置稽核。

解讀：工業企業應做好虛擬區域網隔離、埠禁用等工業控制網絡安全配置，遠端式控制制管理、默認帳戶管理等工業主機安全配置，口令策略合規性等工業控制設備安全配置，建立相應的配置清單，制定責任人定期進行管理和維護，並定期進行配置核查稽核。

2.對重大配置變更制定變更計劃並進行影響分析，配置變更實施前進行嚴格安全測試。

解讀：當發生重大配置變更時，工業企業應及時制定變更計劃，明確變更時間、變更內容、變更責任人、變更審批、變更驗證等事項。其中，重大配置變更是指重大漏洞補丁更新、安全設備的新增或減少、安全域的重新劃分等。同時，應對變更過程中可能出現的風險進行分析，形成分析報告，並在離線環境中對配置變更進行安全性驗證。

3.密切關注重大工控安全性漏洞及其補丁發布，及時採取補丁升級措施。在補丁安裝前，需對補丁進行嚴格的安全評估和測試驗證。

解讀：工業企業應密切關注CNVD、CNNVD等漏洞庫及設備廠商發布的補丁。當重大漏洞及其補丁發布時，根據企業自身情況及變更計劃，在離線環境中對補丁進行嚴格的安全評估和測試驗證，對通過安全評估和測試驗證的補丁及時升級。

*(三)邊界安全防護

1.分離工業控制系統的開發、測試和生產環境。

解讀：工業控制系統的開發、測試和生產環境需執行不同的安全控制措施，工業企業可採用實體隔離、網絡邏輯隔離等方式進行隔離。

2.通過工業控制網絡邊界防護設備對工業控制網絡與企業網或網際網路之間的邊界進行安全防護，禁止沒有防護的工業控制網絡與網際網路連接。

解讀：工業控制網絡邊界安全防護設備包括工業防火牆、工業網閘、單向隔離設備及企業定製的邊界安全防護網關等。工業企業應根據實際情況，在不同網絡邊界之間部署邊界安全防護設備，實現安全訪問控制，阻斷非法網絡訪問，嚴格禁止沒有防護的工業控制網絡與網際網路連接。

3.通過工業防火牆、網閘等防護設備對工業控制網絡安全區域之間進行邏輯隔離安全防護。

解讀：工業控制系統網絡安全區域根據區域重要性和業務需求進行劃分。區域之間的安全防護，可採用工業防火牆、網閘等設備進行邏輯隔離安全防護。

*(四)實體和環境安全防護

1.對重要工程師站、資料庫、伺服器等核心工業控制軟硬體所在區域採取訪問控制、視頻監控、專人值守等實體安全防護措施。

解讀：工業企業應對重要工業控制系統資產所在區域，採用適當的實體安全防護措施。

2.拆除或封閉工業主機上不必要的USB、光碟機、無線等介面。若確需使用，通過主機外設安全管理技術手段實施嚴格訪問控制。

解讀：USB、光碟機、無線等工業主機外設的使用，為病毒、木馬、蠕蟲等惡意代碼入侵提供了途徑，拆除或封閉工業主機上不必要的外設介面可減少被感染的風險。確需使用時，可採用主機外設統一管理設備、隔離存放有外設介面的工業主機等安全管理技術手段。

*(五)身份認證

1.在工業主機登錄、應用服務資源訪問、工業雲平臺訪問等過程中使用身份認證管理。對於關鍵設備、系統和平臺的訪問採用多因素認證。

解讀：用戶在登錄工業主機、訪問應用服務資源及工業雲平臺等過程中，應使用口令密碼、USB-key、智慧卡、生物指紋、虹膜等身份認證管理手段，必要時可同時採用多種認證手段。

2.合理分類設置帳戶權限，以最小特權原則分配帳戶權限。

解讀：工業企業應以滿足工作要求的最小特權原則來進行系統帳戶權限分配，確保因事故、錯誤、篡改等原因造成的損失最小化。工業企業需定期稽核分配的帳戶權限是否超出工作需要。

3.強化工業控制設備、SCADA軟體、工業通信設備等的登錄帳戶及密碼，避免使用默認口令或弱口令,定期更新口令。

解讀：工業企業可參考供應商推薦的設置規則，並根據資產重要性，為工業控制設備、SCADA軟體、工業通信設備等設定不同強度的登錄帳戶及密碼，並進行定期更新，避免使用默認口令或弱口令。

4.加強對身份認證證書資訊保護力度，禁止在不同系統和網絡環境下共用。

解讀：工業企業可採用USB-key等安全介質存儲身份認證證書資訊，建立相關制度對證書的申請、發放、使用、吊銷等過程進行嚴格控制，保證不同系統和網絡環境下禁止使用相同的身份認證證書資訊，減小證書暴露後對系統和網絡的影響。

*(六)遠端訪問安全

1.原則上嚴格禁止工業控制系統面向網際網路開通HTTP、FTP、Telnet等高風險通用網絡服務。

解讀：工業控制系統面向網際網路開通HTTP、FTP、Telnet等網絡服務，易導致工業控制系統被入侵、攻擊、利用，工業企業應原則上禁止工業控制系統開通高風險通用網絡服務。

2.確需遠端訪問的，採用數據單向訪問控制等策略進行安全加固，對訪問時限進行控制，並採用加標鎖定策略。

解讀：工業企業確需進行遠端訪問的，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。採用加標鎖定策略，禁止訪問方在遠端訪問期間實施非法操作。

3.確需遠端維護的，採用虛擬專用網絡(VPN)等遠端接入方式進行。

解讀：工業企業確需遠端維護的，應通過對遠端接入通道進行認證、加密等方式保證其安全性，如採用虛擬專用網絡(VPN)等方式，對接入帳戶實行專人專號，並定期稽核接入帳戶操作記錄。

4.保留工業控制系統的相關訪問日誌，並對操作過程進行安全稽核。

解讀：工業企業應保留工業控制系統設備、應用等訪問日誌，並定期進行備份，通過稽核人員帳戶、訪問時間、操作內容等日誌資訊，追蹤定位非授權訪問行為。

*(七)安全監測和應急預案演練

1.在工業控制網絡部署網絡安全監測設備，及時發現、報告並處理網絡攻擊或異常行為。

解讀:工業企業應在工業控制網絡部署可對網絡攻擊和異常行為進行識別、報警、記錄的網絡安全監測設備，及時發現、報告並處理包括病毒木馬、埠掃描、暴力破解、異常流量、異常指令、工業控制系統協議包偽造等網絡攻擊或異常行為。

2.在重要工業控制設備前端部署具備工業協議深度包檢測功能的防護設備，限制違法操作。

解讀：在工業企業生產核心控制單元前端部署可對Modbus、S7、Ethernet/IP、OPC等主流工業控制系統協議進行深度分析和過濾的防護設備，阻斷不符合協議標準結構的數據包、不符合業務要求的數據內容。

3.制定工控安全事件應急響應預案，當遭受安全威脅導致工業控制系統出現異常或故障時，應立即採取緊急防護措施，防止事態擴大，並逐級報送直至屬地省級工業和資訊化主管部門，同時注意保護現場，以便進行調查取證。

解讀：工業企業需要自主或委託協力廠商工控安全服務單位制定工控安全事件應急響應預案。預案應包括應急計劃的策略和規程、應急計劃培訓、應急計劃測試與演練、應急處理流程、事件監控措施、應急事件報告流程、應急支援資源、應急響應計劃等內容。

4.定期對工業控制系統的應急響應預案進行演練，必要時對應急響應預案進行修訂。

解讀：工業企業應定期組織工業控制系統操作、維護、管理等相關人員開展應急響應預案演練，演練形式包括桌面演練、單項演練、綜合演練等。必要時，企業應根據實際情況對預案進行修訂。

*(八)資產安全

1.建設工業控制系統資產清單，明確資產責任人，以及資產使用及處置規則。

解讀：工業企業應建設工業控制系統資產清單，包括資訊資產、軟體資產、硬體資產等。明確資產責任人，建立資產使用及處置規則，定期對資產進行安全巡檢，稽核資產使用記錄，並檢查資產運行狀態，及時發現風險。

2.對關鍵主機設備、網絡設備、控制組件等進行冗餘配置。

解讀：工業企業應根據業務需要，針對關鍵主機設備、網絡設備、控制組件等配置冗餘電源、冗餘設備、冗餘網絡等。

*(九)數據安全

1.對靜態存儲和動態傳輸過程中的重要工業數據進行保護，根據風險評估結果對數據資訊進行分級分類管理。

解讀：工業企業應對靜態存儲的重要工業數據進行加密存儲，設置訪問控制功能，對動態傳輸的重要工業數據進行加密傳輸，使用VPN等方式進行隔離保護，並根據風險評估結果，建立和完善數據資訊的分級分類管理制度。

2.定期備份關鍵業務數據。

解讀：工業企業應對關鍵業務數據，如工藝參數、設定檔、設備運行數據、生產數據、控制指令等進行定期備份。

3.對測試數據進行保護。

解讀：工業企業應對測試數據，包括安全評估數據、現場組態開發數據、系統聯調數據、現場變更測試數據、應急演練數據等進行保護，如簽訂保密協議、回收測試數據等。

*(十)供應鏈管理

1.在選擇工業控制系統規劃、設計、建設、運維或評估等服務商時，優先考慮具備工控安全防護經驗的企事業單位元，以合同等方式明確服務商應承擔的資訊安全責任和義務。

解讀：工業企業在選擇工業控制系統規劃、設計、建設、運維或評估服務商時，應優先考慮有工控安全防護經驗的服務商，並核查其提供的工控安全合同、案例、驗收報告等證明材料。在合同中應以明文條款的方式約定服務商在服務過程中應當承擔的資訊安全責任和義務。

2.以保密協議的方式要求服務商做好保密工作，防範敏感資訊外泄。

解讀：工業企業應與服務商簽訂保密協議，協議中應約定保密內容、保密時限、違約責任等內容。防範工藝參數、設定檔、設備運行數據、生產數據、控制指令等敏感資訊外泄。

*(十一)落實責任

通過建立工控安全管理機制、成立資訊安全協調小組等方式，明確工控安全管理責任人，落實工控安全責任制，部署工控安全防護措施。

解讀：工業企業應建立健全工控安全管理機制，明確工控安全主體責任，成立由企業負責人牽頭的，由資訊化、生產管理、設備管理等相關部門組成的工業控制系統資訊安全協調小組，負責工業控制系統全生命週期的安全防護體系建設和管理，制定工業控制系統安全管理制度，部署工控安全防護措施。

*總結

- 隨著乙太網技術在工業控制網絡中的應用，以及兩化深入融合的持續推進，未來的工業控制系統將會融入更多的新興資訊技術和安全技術。
- OT與IT的區隔日益模糊，但本質上的差異仍然存在，強化關鍵基礎設施的網路安全，應從了解OT與IT之間的差別開始做起。
- 網路安全在OT與IT的融合過程裡面，扮演著不可或缺的角色，但是技術支援與管理作業仍是各自進行。然而，OT的應用只要牽涉到現場設備與系統的監控，就會與業務或企業系統產生關連性。
- 針對IT系統安全性的管制作法，未必能適用於OT系統的網路安全防護。採用舊有技術，也是現行使用的ICS系統面臨的眾多挑戰之一，比起晚近發展起來的IT系統，已長期使用的工業控制設備，幾乎沒有任何安全性功能。
- ICS安全性的目標設定上，實務上，無法做到百分之百防護。我們所要努力的方向，主要是降低風險、減緩衝擊，以及具有備援的運作模式。
- ICS特別重視系統的可用性，在看待各種ICS安全性的措施時，不只是要留意該如何防禦，同時，還要具備快速復原(Resilience)的能力，使系統儘快恢復運作。


Thank
you!

*單向通信100%安全？

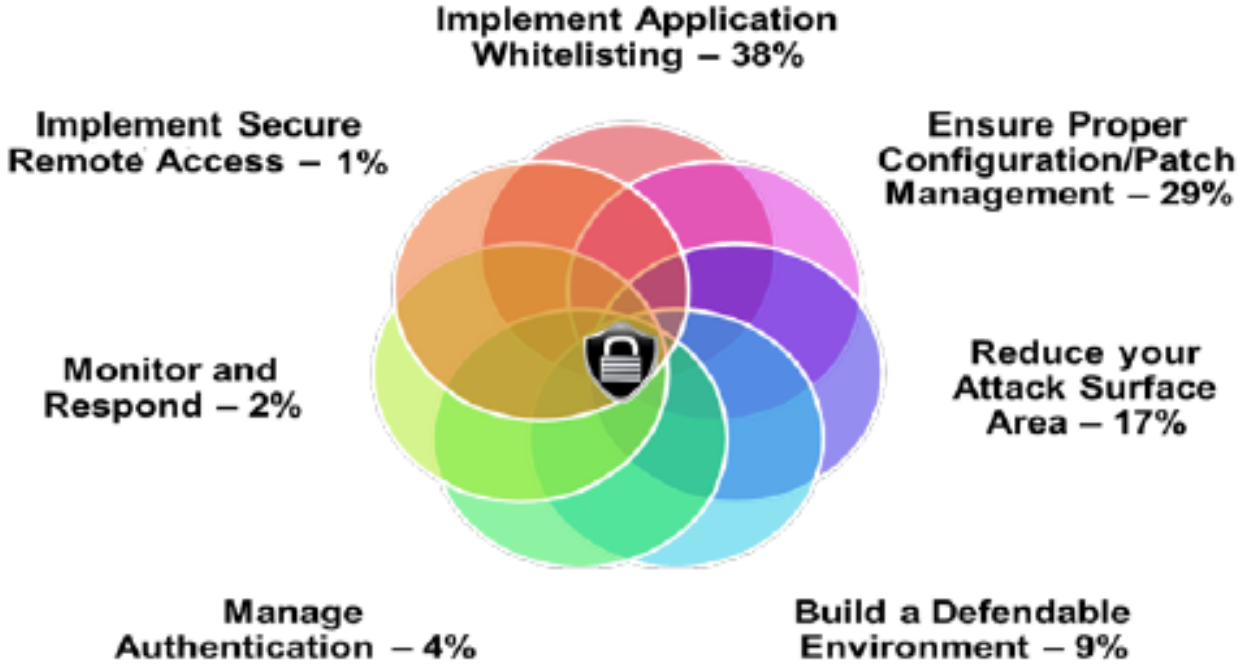
ICS系統允許以單向通訊方式與其他安全區域聯接。但是，這種聯接方式是很不嚴密的，其安全程度高低取決於單向通信的實現方式。

*方式一為限制發起方方式，即通信只能由某一方發起，然後雙方可以互相通信。(防火牆)

*方式二為限制負載流方式，即在方式一基礎上，對方只能發送控制信號，不能發送資料或應用資訊。(防火牆+限制資訊流)

*方式三最嚴格，僅允許一方發送資訊，不允許另一方發送任何資訊。(光纖單向網閘)

Seven Strategies to Defend ICSs



Percentage of ICS-CERT FY 2014 and FY 2015 Incidents Potentially Mitigated by Each Strategy