7. 經驗學習

- 資安漏洞由系統的遠端存取帳號，於受駭系統上注入勒索軟體，並結合網路犯罪與國家級進階持續性威脅（APT）攻擊。
- 啟用多因素認證、建立垃圾訊息過濾機制、過濾網路流量、定期更新軟體、限制特定資源的存取，以及部署防毒軟體等防護。
- 隔離管道作業及部份 IT 系統，重視第三方的安全專家來調查，知會執法機關及回報包括能源部在內的聯邦政府。
- 建立備份來復原系統。

3.3.3 資通安全供應鏈風險

工業界已承認供應鏈中的風險確定為對大型電子系統(Bulk Electronic Systems. BES)可靠性的潛在威脅。資訊和通訊技術及工業控制系統的供應鏈長而多維，涉及全球多個國家的眾多參與者。在為其營運購買產品和服務時，大型電力系統(Bulk Power Systems, BPS)所有者和營運商通常依賴於供應商和承包商，這些供應商和承包商可能使用多個第三方供應商的產品或技術中使用的組件。惡意行為者可能以供應鏈中的一個或多個供應商為目標，以創建或利用漏洞，利用這些漏洞對大型電子系統資通系統和設備發起資通攻擊。

3.3.3.1 供應鏈風險

資訊和通訊技術以及工業控制系統的供應鏈長而多維，涉及全球多個國家。全球各地的多個實體可以參與單個購買產品的開發，設計，製造和交付。全球供應鏈可以為消費者提供大量收益的機會，但是同時，供應鏈中任何環節的漏洞都可能給最終用戶帶來風險。資通供應鏈風險可能源於假冒產品的插入，未經授權的生產，篡改，盜竊，惡意軟體和硬體的插入以及不良的製造和開發流程。即使是設計良好的產品，也可能在供應鏈中引入了惡意組件，事實證明在部署這些組件之前很難識別它們。

研究顯示在 SCADA 產品上安裝惡意軟體和盜竊項目文件，在防火牆解決方案上插入未經授權的程式碼允許執行遠端程序，並涉嫌將外國目標單位「後門」插入反病毒公司的安全產品，都是已經發生的資通安全事件。同時，經統計供應鏈中引入惡意程式及遠端訪問其系統的供應商員工的風險確定為面臨的兩個最重大的供應鏈風險。供應鏈風險種類如圖 xxx。

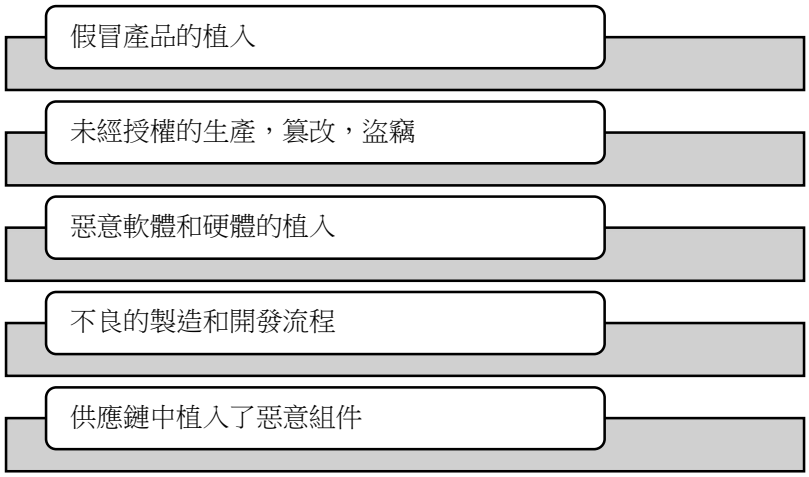

圖 xxx 供應鏈風險

3.3.3.2 解決供應鏈風險的工業標準和最佳實踐

業界針對供應鏈風險，已經提出許多標準和最佳實踐[14]來解決產業中的供應鏈風險。這些標準和最佳實踐可更全面地了解供應鏈風險以及企業為減輕風險可能採取的步驟。相關標準和最佳做法包括以下內容：

一、 場外供應商服務

在政府環境中，如果供應商為涉及不在政府所在地的資訊系統的實體執行部署或服務，則適用聯邦風險與授權管理計畫(FedRAMP[25])標準。(以美國為例)

二、 第三方認證流程

遵循 FedRAMP 和國際標準化組織發布的品質管理和資訊安全管理標準之標準供應商，使用獨立的第三方來評估其對標準的遵守情況。

三、 安全的硬體交付

美國能源部(Department of Energy, DOE)的能源部門控制系統工作組開發了用於能源傳遞系統的資通安全採購程式，該語言確定了硬體交付的控制措施，以幫助減少運輸過程中受到危害的風險。

四、 來源

來源是在供應鏈流程和供應商關係中提供可追溯性的能力。若干標準和準則涉及到出處，參考由 NIST 發布的《聯邦資訊系統國家供應鏈風險管理

[25] FedRAMP: Federal Risk and Authentication Management Program

慣例》(NISTIR 762226)。

五、 威脅建模

威脅建模是用來確保所有產品都具有針對產品目前開發範圍的威脅模型的過程，如國際電工委員會標準 IEC 62443-4-1 中所述。

六、 供應鏈缺陷評估

應變控制措施，以識別和緩解某些產品或服務提供商的供應鏈流程中評估的漏洞或固有弱點的風險是一種重要的風險管理方法，如 NIST SP 800-53 中所述。

七、 外部依存關係識別

美國能源部的資通安全能力成熟度模型(C2M2[27])將供應鏈視為識別和管理外部依存關係的過程。認識依存關係及對營運最關鍵的依存關係，可以提高實體突顯和減輕供應鏈風險的能力。

八、 處理不符合採購流程的提供的產品或服務的政策

當提供的產品或服務不符合其特定供應鏈政策時，實體可以使用控制措施來減輕風險。美國核監管委員會在美國聯邦法規 10 C.F.R.50 部分的附錄 B 中描述了這種方法，以確保品質。

九、 不支持或開源的技術組件

在更新系統或系統組件時，必須考慮不同的過程，以有效減輕遺留或不受支持的系統的風險。請參閱 NIST SP 800-53 關於開源產品，開源群組建立了一套名為「受信任的技術提供者標準(O-TTPS[28])認證計畫」的標準和認證流程，以解決購買者的供應鏈控制問題。

十、 供應商關係

管理供應商的一個重點是如何終止與第三方的關係，以限制丟失產品或服務的營運影響。

3.3.3.3 大型電力系統供應鏈風險

北美電子可靠性公司(North American Electric Reliability Corporation, NERC)提出一套供應鏈標準包括新的可靠性標準，供應鏈標準側重於以下五個安全目標：

[26] NISTIR 7622: https://www.nist.gov/privacy-framework/nistir-7622
[27] https://www.energy.gov/ceser/energy-security/cybersecurity-capability-maturity-model-c2m2-program
[28]https://www.opengroup.org/certifications/o-ttps

軟體完整性和真實性，供應商遠端訪問保護，資訊系統規劃以及供應商風險管理和採購控制。要求執行以下操作：

一、 降低攻擊者利用合法的供應商補丁程序管理流程將受損的軟體更新或補丁交付給大型電子系統資通系統的可能性。

二、 解決與供應商遠端訪問相關的威脅，包括用於在沒有負責單位知道的情況下訪問大型電子系統資通系統的供應商通行碼被盜的威脅及信任的供應商的受損可以追蹤到負責實體的大型電子系統資通系統的不受監視的連接。

三、 解決責任實體可能無意間計畫在其資訊系統內購買和安裝易受攻擊的設備或軟體的風險，或者可能無意間無法預測由於其網路體系結構或技術和供應商過渡期間可能出現的安全問題的風險。

四、 解決責任實體可能與對其資訊系統構成重大風險的供應商簽訂合約的風險，以及責任實體採購的產品未達到最低安全標準的風險。

五、 解決受到威脅的供應商無法向與其連接的責任實體充分通知安全事件和漏洞以及相關事件響應的風險。

針對供應鏈資通安全弱點對大型電力系統（如核電廠）造成的潛在風險，NERC 制定了供應鏈標準要求負責單位採取措施解決與大型電力系統中資通系統供應鏈相關的資通安全風險。NERC 和業界已經對供應鏈風險可能對大型電力系統可靠性產生的潛在影響更深入了解，NATF[29]提出幾個真實事件包括在 SCADA 產品上安裝惡意軟體和盜竊項目文件，在防火牆解決方案上插入未經授權的程式碼允許執行遠端程序，並涉嫌將外國目標「後門」植入反病毒公司的安全產品。APPA[30]和 NRECA[31]將系統的供應商員工的風險確定為成員實體面臨的兩個最重大的供應鏈風險。EPRI 強調，如果供應商提供產品市場的很大一部分，則單個供應商的供應鏈中的損害可能會產生廣泛的影響。

為求解決電力產業所面臨的供應鏈風險，NERC 工作人員建議實體在制定其供應鏈風險管理計劃時採用以下做法：

1. 安全的硬體交付：在大型電力系統上採購和部署的許多資通資產都是配置為執行非常特定的實時功能的硬體設備。這些設備可能擁有可被操縱的程式碼，因而可能導致它們潛在地影響大型電力系統的可靠運行。如果那些設備在運輸中受到損害，如同美國能源部能源部門控制系統工作小組所描述，建立硬體交付控制措施可能有助於降低風險。

[29] NATF = North American Transmission Forum
[30] APPA = American Public Power Association
[31] NRECA = National Rural Electric Cooperative Association

2. 第三方認證流程：包括其供應商的獨立評估或第三方認證過程， NERC 將與利益相關者合作開發一種認證模型，以識別具有強大的供應鏈風險管理實踐能力的供應商。此一認證不僅可以提高提供大型電力系統相關產品和服務的供應商正有效地實施供應鏈資通安全管控措施的信心，而且還有助於遵守建議的可靠性標準。應當制定第三方認證或認證的流程，並提交給 NERC 進行評估。

3. 威脅告知採購語言：應針對其環境的特定風險制定安全規範。並可經由威脅建模來完成，該過程確保所有產品都具有針對該產品開發範圍的威脅模型。如此可以確保適當評估採購任何應用程式或系統的風險與危害組織或大型電力系統的風險。例如，如果正在為中等影響的大型電力系統資通系統籌建新的遠端訪問系統，威脅模型可根據其特定的風險和系統特定的漏洞反應遠端訪問系統對大型電力系統的影響。

4. 解決不受支持或開源技術組件的過程：如果不再有系統或組件的補丁程式來源，則應制定計劃以減輕這些不受支持的系統帶來的潛在風險。購買開源技術時也應實施控制措施，包括持續支持和修補的責任。

5. 使用供應鏈控制來緩解共模漏洞(Common-Mode Vulnerabilities)：供應鏈標準要求擁有高影響力和中等影響力的大型電力系統資通系統開發流程，以確保通過採購流程來管理供應鏈風險。作為最佳實踐，NERC 希望具有中等或較高影響力的大型電力系統資通系統的單位將對低影響力的大型電力系統資通系統應用 CIP-013-1[32]要求供應鏈風險管理計劃。如果將供應鏈安全實踐統一應用於資通資產類型和大型電力系統資通系統影響級別，則可降低共模漏洞的風險。

3.3.3.4 電子門禁管制或監視系統供應鏈風險

電子門禁管制或監視系統（EACMS[33]）定義為「對電子安全外圍設備或大型電力系統資通系統執行電子門禁管制或電子門禁監視的資通資產。」組成 EACMS 的組件通常用於控制對大型電力系統上的關鍵系統（例如 EMS / SCADA 和基於微處理器的繼電器）的訪問，保護和監視。EACMS 組件包括防火牆，路由器，第三層交換機，入侵檢測系統，紀錄監控器和訪問控制系統。

EACMS 可能容易受到供應鏈風險的影響。如果遭到破壞，濫用或無法使用，則 EACMS 組件可能會對大型電力系統的可靠性產生實時影響。供應鏈漏洞帶來的風險在很大程度上取決於 EACMS 的特定配置，部署 EACMS 的位置（即處於低，中或高影響力的大型電力系統資通系統），以及採用某些補償措施的程度。

[32] CIP-013-1 : Cyber Security - Supply Chain Risk Management, NERC
[33] EACMS = Electronic Access Control and Monitor System

如果要在供應鏈中破壞電子門禁管制組成部分，例如，通過引入未經授權的「後門」，惡意行為者可以訪問（或禁止授權用戶訪問）直接影響大型電力系統操作的系統。如果受損的 EACMS 控制著對中度或高度影響的大型電力系統資通系統的電子訪問，則這種損害可能會對大型電力系統的可靠性產生負面影響。

上述供應鏈受損的潛在風險可以通過技術控制得到部分緩解，例如，可以使用嚴格的授權和身份驗證（包括多因素身份驗證），以限制所有者或供應商人員對 EACMS 管理服務進行本地或遠程訪問所帶來的風險。為了保護訪問和通訊的安全，可以採取的其他技術控制措施包括：實施強大的密碼策略；實施基於角色的訪問控制；使用身份驗證，授權和計費服務；實施訪問控制列表；加密遠程訪問會話；並將單獨的安全虛擬局域網用於數據和管理流量。對 EACMS 的體系結構，配置和管理訪問進行測試，驗證和確認還可以幫助確保 EACMS 按設計實施，達到預期的安全控制目標並在定義的 ESP 中保護大型電力系統資通系統。

NERC 希望在採購和配置與 EACMS 相關的各種資通資產類型時，將識別和評估供應鏈漏洞。考慮以下因素

- 確定構成 EACMS 的組件（即特定的資通資產類型）
- 確定每種 EACMS 設備類型的供應商
- 確定每種 EACMS 設備類型執行的功能以保護可靠性（即防火牆，路由器，交換機等）
- 識別並確定優先級：如果每種 EACMS 設備類型都受到威脅（例如，受到威脅的防火牆可能允許未經授權或惡意的流量），則存在的風險; 和知情的潛在緩解情況（例如，記錄系統主要用於事後分析，而不是實時保護）
- 評估每種設備類型帶來的已識別風險
- 制定潛在的策略或建議，以解決和減輕每個已識別的風險

3.3.3.5 實體門禁控制系統

實體門禁控制系統（PACS[34]）定義為「控制，警告或記錄對實體安全邊界的訪問的資通資產。」組成 PACS 的系統通常用於控制和監視對大型電力系統資通系統所在的設施和系統的實體訪問。包括實體入侵檢測系統，紀錄監控器和控制實體訪問的系統。 PACS 資通資產包括身份驗證服務器，通行卡系統和徽章控制系統。

PACS 可能容易受到供應鏈風險的影響。 如果 PACS 組件遭到破壞，誤用或

[34] PACS = Physical Access Control Systems

變得無法使用，則可能會對大型電力系統的可靠性產生即時影響。供應鏈漏洞帶來的風險在很大程度上取決於 PACS 的特定配置，PACS 的部署位置（即，在低，中或高影響力的大型電力系統資通系統上）。根據特定的配置，如果 PACS 受到損害，濫用或變得無法使用，則可能會對大型電力系統的可靠性產生即時影響。考慮到這種潛在的影響，在採購和配置這些系統時，必須考慮供應鏈漏洞。

實體門禁控制的方法包括密鑰卡（電子訪問方式，在資料庫中預先定義卡持有者的訪問權限，權限可能因邊界而異），特殊鎖（不限於「鑰匙」系統鎖，也含遠端操作電磁鎖），安全人員，及其他身份驗證設備（如生物識別，鍵盤，象徵或其他等效設備，用於控制實體訪問）。記錄實體門禁的方法包括計算機紀錄、影片記錄、及手動記錄。執行實體門禁管制的 PACS 資通系統比監視和記錄系統具有更高的風險。PACS 的受損會允許訪問直接影響大型電力系統運行的系統，從而可能使威脅源對大型電力系統的可靠性產生負面影響。對執行監視的資通系統的危害雖然不會帶來很高的風險，但可能會影響快速分析攻擊的能力，並且可能掩蓋即時警報，以阻止正在積極評估可靠性的警報的訪問。受損的 PACS 監視系統也可能會消除該實體檢測對設施及其關聯的大型電力系統資通系統的非法訪問的能力。在進行實體或資通攻擊之前，可能會失去監視未經授權的訪問以及向監視人員發出警報或警報的能力，這可能會延長響應時間並允許威脅行為者成功進行攻擊。破壞紀錄系統的風險將影響主動和潛在攻擊後的取證分析。考慮到受損的 PACS（尤其是受損的訪問控制系統）可能造成的潛在不利影響，在採購和配置這些系統時，識別和評估供應鏈漏洞非常重要。

針對降低 PACS 系統供應鏈風險時，應考慮實體營運環境中的 PACS 因素，確定組成 PACS 的組件（如伺服器、工作站、攝影機和其他監視設備、訪問控制資通資產組件、監控組件、及記錄組件），確定每種 PACS 設備類型的供應商，確定每種 PACS 設備類型為保護可靠性而執行的功能（例如，授權和授予訪問，檢測，響應，監視，記錄等），識別並區分每種 PACS 設備類型所帶來的風險（如果受到損害）（即，受侵害的訪問授權系統可能允許未經授權或惡意的訪問），評估每種設備類型帶來的已識別風險，制定潛在的策略和/或建議，以解決和減輕每個已識別的風險。

3.3.3.6 受保護的資通資產供應鏈風險

受保護的資通資產（PCA[35]）定義為「一個或多個資通資產是在電子安全範圍之內或之上使用通信協定連接的。 受保護的資通資產的影響等級等於同一 ESP 中評價最高的大型電力系統資通系統。」由於 PCA 的資產種類繁多，因此如果由於供應鏈漏洞而使大型電力系統受到損害，則無法明確定義大型電力系統的一般風險。

[35] PCA = Protected Cyber Assets

PCA 是資通資產，可能是典型的資訊技術資產，如工作站，服務器，印表機，掃描儀，以及其他支持控制中心，資料中心，或安全運營中心環境中的操作員和員工作業的外圍設備。根據類型和配置，PCA 可能具有與高或中等大型電力系統資通系統相關的資通資產的相同風險特徵。風險加劇的情況是，這些系統可能與大型電力系統資通系統駐留在相同的網段中，而不是大型電力系統資通系統的一部分。由於 PCA 與大型電力系統資通系統之間的潛在互連性，PCA 的妥協或濫用可能會轉向大型電力系統資通系統。

潛在的風險可以通過技術控制得到部分緩解，一些可以在 CIP 可靠性標準中解決，而其他則可以在政策和程序中解決。 例如，可以使用實施訪問控制列表，入侵防禦系統和惡意軟體防禦工具來限制 PCA 可能影響互連的大型電力系統資通系統的風險。

3.3.4 小結

SolarWinds 攻擊凸顯出供應鏈攻擊！供應鏈攻擊對駭客具有吸引力，因為當常用軟體受到威脅時，攻擊者可能會獲得使用該軟體的所有企業的訪問權限。供應鏈攻擊又可稱為價值鏈攻擊或第三方攻擊。SolarWinds 攻擊是一種新型的攻擊手法，危害極大。即便美國建立網路攻擊防禦系統「愛因斯坦」(Einstein)，但在 SolarWinds 攻擊中都未發生有效防護作用。供應鏈中任何環節的漏洞都可能給最終用戶帶來風險。資通供應鏈風險可能源於假冒產品的插入，未經授權的生產，篡改，盜竊，惡意軟體和硬體的插入以及不良的製造和開發流程。

面對大型電力系統供應鏈風險，NERC 工作人員建議以下做法

- 大型電力系統上採購和部署的許多資通資產都是配置為執行非常特定的實時功能的硬體設備。這些設備可能擁有可被操縱的程式碼，因而可能導致它們潛在地影響大型電力系統的可靠運行，應建立硬體交付控制措施可能有助於降低風險。
- NERC 建議將與利益相關者合作開發一種認證模型，以識別具有強大的供應鏈風險管理實踐能力的供應商。
- 針對其環境的特定風險制定安全規範。並可經由威脅建模來完成，該過程確保所有產品都具有針對該產品開發範圍的威脅模型。如此可以確保適當評估採購任何應用程式或系統的風險與危害組織或大型電力系統的風險。
- 不再有系統或組件的補丁程式來源，則應制定計劃以減輕這些不受支持的系統帶來的潛在風險。購買開源技術時也應實施控制措施，包括持續支持和修補的責任。
- 供應鏈標準要求擁有高影響力和中等影響力的大型電力系統資通系統開發

流程，以確保通過採購流程來管理供應鏈風險。

- 為了保護訪問和通訊的安全，可以採取的其他技術控制措施包括：實施強大的密碼策略；實施基於角色的訪問控制；使用身份驗證，授權和計費服務；實施訪問控制列表；加密遠程訪問會話；並將單獨的安全虛擬局域網用於數據和管理流量。

- 實體門禁控制的方法包括密鑰卡（電子訪問方式，在資料庫中預先定義卡持有者的訪問權限，權限可能因邊界而異），特殊鎖（不限於「鑰匙」系統鎖，也含遠端操作電磁鎖），安全人員，及其他身份驗證設備（如生物識別，鍵盤，象徵或其他等效設備，用於控制實體訪問）。

- 使用實施訪問控制列表，入侵防禦系統和惡意軟體防禦工具來限制受保護的資通資產可能影響互連的大型電力系統資通系統的風險。