TLP:CLEAR

調整網絡安全風險平衡：「設計安全」和「預設安全」的原則和方法

發佈日期：**2023**年**4**月**13**日

網絡安全和基礎設施安全局

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

目錄

概述：設計漏洞

科技幾乎融入了日常生活的方方面面。面向互聯網的系統連接著直接影響著我們經濟繁榮、生計甚至健康等關鍵系統，從個人身份管理到醫療保健。僅舉一個例子，網絡漏洞已導致全球範圍內的醫院取消手術並轉移患者照護。關鍵系統中的不安全技術和漏洞可能會招致惡意網絡入侵，從而導致嚴重的潛在安全[1]風險。

對技術製造商來說，現在比以往任何時候都需要將「設計安全」和「預設安全」作為產品設計和開發流程的重點。一些供應商在推動軟件保障行業向前發展方面取得了長足進步，而另一些供應商則落後了。編寫機構強烈鼓勵每個技術製造商以這樣一種方式構建他們的產品，即防止客戶必須不斷地對其系統進行監控、例行更新和損害控制，以減輕網絡入侵。我們鼓勵製造商承擔改善其客戶安全結果的責任。過去，技術製造商一直依賴於修復客戶部署產品後發現的漏洞，要求客戶自費應用這些補丁。 只有結合「設計安全」實踐，我們才能打破創建和應用修復程序的惡性循環。

為實現這種高標準的軟件安全，編寫機構鼓勵製造商優先考慮將產品安全融合作為功能和上市速度的關鍵先決條件。隨著時間的推移，工程團隊將能夠建立一種新的穩態節奏，在這種節奏中，安全性真正融入設計之中，並且需要較少的維護。

反映這一觀點，歐盟在《網絡彈性法案》中強調了產品安全的重要性，強調製造商應在產品的整個生命週期實施安全措施，以防止製造商將有漏洞的產品引入市場。

為了創造一個技術和相關產品對客戶來說更安全的未來，編寫機構敦促製造商改進他們的設計和開發計劃，只允許向客戶提供「設計安全」和「預設安全」的產品。「設計安全」的產品是指將客戶安全作為核心業務目標，而不僅僅是一個技術功能的產品。「設計安全」的產品在開發開始之前就以該目標為出發點。「預設安全」的產品是那些「開箱即用」的安全產品，幾乎或完全不需要更改配置，並且無需額外費用即可獲得安全功能。這兩個原則共同將保持安全的大部分負擔轉移給了製造商，並減少了客戶因配置錯誤、補丁速度不夠快或許多其他常見問題而成為安全事件受害者的可能性。

網絡安全和基礎設施安全局 **(CISA)**、國家安全局 **(NSA)**、聯邦調查局 **(FBI)** 和以下國際合作夥伴[2]提供本指南中的建議，作為技術製造商確保其產品安全的路線圖：

[1] 編寫機構認識到，「安全」一詞根據其使用的上下文具有多種含義。 在本指南中，「安全」是指提高技術安全標準以保護客戶免受惡意網絡活動的侵害。

[2] 以下簡稱「編寫機構」。

- 澳洲網絡安全中心 **(ACSC)**
- 加拿大網絡安全中心 **(CCCS)**
- 英國國家網絡安全中心 **(NCSC-UK)**
- 德國聯邦資訊安全辦公室 **(BSI)**
- 荷蘭國家網絡安全中心 **(NCSC-NL)**
- 新西蘭計算機應急響應小組 **(CERT NZ)** 和新西蘭國家網絡安全中心 **(NCSC-NZ)**

編寫機構承認許多私營部門合作夥伴在推進「設計安全」和「預設安全」方面的貢獻。本產品旨在推動國際間有關關鍵優先事項、投資和決策的對話，這些對話是實現技術在設計和預設情況下安全、可靠和有彈性的未來所必需的。 為此，編寫機構徵求有關各方對此產品的反饋，並打算召開一系列聆聽會議，以進一步完善、明確和推進我們的指南，以實現我們的共同目標。

有關產品安全重要性的更多資訊，請參閱 CISA 的文章，《 不安全技術的代價以及我們能做些什麼》。

「設計安全」

「設計安全」是指技術產品的構建方式可以合理地防止惡意網絡行為者成功訪問設備、數據和連接的基礎設施。軟件製造商應執行風險評估，以識別和列舉對關鍵系統的普遍網絡威脅，然後在產品藍圖中包含保護措施，以應對不斷變化的網絡威脅情況。

安全資訊技術 **(IT)** 開發實踐和多層防禦（稱為深度防禦），亦被建議用來防止對手活動危害系統或未經授權獲取敏感數據。 編寫機構建議製造商在產品開發階段使用定制的威脅模型來解決系統面臨的所有潛在威脅，並考慮到每個系統的部署過程。

編寫機構敦促製造商對其產品和平台採取整體安全方法。 「設計安全」的開發需要軟件製造商在產品設計和開發過程的每一層投入大量資源，這些資源不能在以後「附加」。 它需要製造商最高業務主管的強有力領導，使安全作為業務優先事項，而不僅僅是一項技術功能。業務領導者和技術團隊之間的這種協作從設計和開發的早期階段延伸到客戶部署和維護。我們鼓勵製造商作出艱難的權衡和投資，包括那些對客戶「不可見」的，例如遷移到消除廣泛漏洞的編程語言。他們應該優先考慮保護客戶的功能、機制和工具的實施，而非那些看似有吸引力但會擴大攻擊面的產品功能。

沒有單一的解決方案可以結束惡意網絡行為者利用技術漏洞的持續威脅，「設計安全」的產品將繼續受到漏洞的影響； 但是，大量漏洞是由相對較小的根源子集造成的。 製造商應制定書面路線圖，以使其現有產品組合與更多「設計安全」實踐保持一致，確保僅在特殊情況下才會出現偏差。

編寫機構承認，為客戶承擔安全結果的責任並確保這種水平的客戶安全可能會增加開發成本。

然而，在開發新技術產品和維護現有產品的同時投資於「設計安全」實踐，可以顯著改善客戶的安全態勢並降低遭受攻擊的可能性。「設計安全」原則不僅加強了客戶的安全態勢和開發者的品牌聲譽，而且長期來看降低了製造商的維護和補丁成本。

下面列出的「對軟件製造商的建議」部分提供了一個建議的產品開發實踐和政策清單，供製造商考慮。

「預設安全」

「預設安全」是指產品開箱即可抵禦普遍的漏洞利用技術，無需額外付費。 這些產品可以抵禦最普遍的威脅和漏洞，而終端用戶無需採取額外的措施來保護它們。 「預設安全」產品旨在讓客戶敏銳地意識到，當他們偏離安全預設值時，除非他們實施額外的補償控制，否則他們會增加遭受攻擊的可能性。

- 安全配置應該是預設基線。「預設安全」產品會自動啟用保護企業免受惡意網絡行為者侵害所需的最重要的安全控制措施，並提供可使用和進一步配置安全控制措施的能力，無需額外費用。
- 安全配置的複雜性不應是客戶的問題。 組織的 **IT** 人員經常因安全和運營責任而超負荷，從而導致有限時間來了解和實施強大的網絡安全態勢所需的安全影響和緩解措施。 通過優化安全產品配置，即確保預設路徑，製造商可以通過確保他們的產品按照「預設安全」標準安全地製造、分銷和使用，來幫助他們的客戶。

「預設安全」產品的製造商不會為實施額外的安全配置收取額外費用。 相反，他們將這些包含在基礎產品中，就像所有新車都配有安全帶一樣。 安全不是奢侈的選擇，而是更接近每個客戶應該期望的標準，而無須爭議或支付更多費用。

對軟件製造商的建議

本聯合指南為向製造商提供建議，以製定書面路線圖來實施和確保 **IT** 安全。 編寫機構建議軟件製造商實施以下各節概述的策略，以通過「設計安全」和「預設安全」原則來承擔其客戶的安全結果。

軟件產品安全原則

我們鼓勵技術製造商採用優先考慮軟件安全的戰略重點。 編寫機構制定了以下三個核心原則，以指導軟件製造商在開發、配置和交付其產品之前將軟件安全納入到其設計流程。

1. 安全的責任不應只由客戶承擔。 軟件製造商應對客戶購買的安全結果負責，並相應地改進其產品。
2. 採用徹底的透明度和問責制。 軟件製造商應該以提供安全可靠的產品為榮，並根據自己的能力在其他製造商群體中脫穎而出。 這可能包括共享他們從客戶部署中了解到的資訊，例如採用強化身份驗證機制預設。 還包括確保漏洞公告和相關的常見漏

洞和暴露 (CVE) 記錄完整且準確的堅定承諾。 但是，要提防將 CVE 視為負面指標的誘惑，因為這些數字也是健康的代碼分析和測試社區的標誌。

3. 建立組織結構和領導來實現這些目標。 雖然技術專業知識對於產品安全至關重要，但高級管理人員是在組織中實施變革的主要決策者。對於軟件製造商來說，高管層承諾將安全作為產品開發的一個關鍵要素進行優先考慮，這需要與組織的客戶建立合作夥伴關係，以了解：
    a. 產品部署場景指導，以及定制的威脅模型
    b. 遵循「預設安全」原則的安全控制措施的建議實施方式
    c. 根據公司規模定制的資源分配策略，以及用「設計安全」實踐取代遺留開發實踐的能力
    d. 需要保持開放的溝通渠道以獲取有關產品安全問題的內部和外部反饋（例如員工和客戶反饋）。 應在內部論壇（例如全員大會或午餐會議）以及外部產品營銷和客戶參與中強調軟件安全
    e. 衡量客戶部署內的有效性。 高級行政領導將想知道「設計安全」和「預設安全」的投資在哪些方面通過減緩安全補丁的速度、減少配置錯誤和最小化攻擊面來幫助客戶。

為了實現這三個原則，製造商應該考慮幾種操作策略來改進他們的開發流程。

定期與公司行政領導召開會議，以推動組織內「設計安全」和「預設安全」的重要性。 應制定政策和程序來獎勵那些開發遵守這些原則的產品的生產團隊，其中可以包括對實施出色的軟件安全實踐的獎勵，或工作階梯和晉升標準的獎勵。

強調軟件安全對業務成功的重要性。 例如，考慮指派一個堅持商業和 IT 實踐的軟件安全負責人或軟件安全團隊，以直接將軟件安全標準與製造商責任聯繫起來。 製造商應確保他們的產品擁有穩健、獨立的產品安全測評和評估程序。

在開發過程中使用定制的威脅模型，以優先考慮最關鍵和影響最大的產品。 威脅模型考慮到產品的具體使用情況，並使開發團隊能夠強化產品。 最後，高層領導應將交付安全產品作為產品卓越和質量的關鍵因素，對團隊進行責任追究。

「設計安全」策略

安全軟件開發框架 (SSDF)，也稱為國家標準與技術研究院 (NIST) SP 800-218，是一套核心的高級安全軟件開發實踐，可以整合到軟件開發生命週期的每個階段 （SDLC）。 遵循這些做法可以幫助軟件生產商更有效地發現和消除已發佈軟件中的漏洞，減輕利用漏洞的潛在影響，並解決漏洞的根本原因以防止未來再次發生。

編寫機構鼓勵使用「設計安全」策略，包括參考 SSDF 實踐的原則。 軟件製造商應制定書

面路線圖，以在其產品組合中採用更多「設計安全」的軟件開發實踐。 以下是非盡錄的說明性路線圖最佳實踐：

- 內存安全編程語言（**SSDF PW.6.1**）：盡可能優先使用內存安全語言。 編寫機構承認其他內存特定的緩解措施，如地址空間佈局隨機化 **(ASLR)**、控制流完整性 **(CFI)** 和模糊測試對遺留代碼庫有幫助，但不足以被視為「設計安全」，因為它們不能充分防止漏洞利用。 現代內存安全語言的一些示例包括 **C#**、**Rust**、**Ruby**、**Java**、**Go** 和 **Swift**。 閱讀 **NSA** 的內存安全資訊表來了解更多。
- 安全硬件基礎：納入能夠支持細粒度內存保護的架構功能，例如能力硬件增強型 **RISC** 指令 **(CHERI)** 所描述的可以擴展傳統硬件指令集架構 **(ISA)** 的架構功能。 如需更多資訊，請瀏覽劍橋大學的 **CHERI** 網頁。
- 安全軟件組件 **(SSDF PW 4.1)**：從經過驗證的商業、開源和其他第三方開發人員處獲取和維護安全的軟件組件（例如，軟件庫、模塊、中間件、框架），以確保消費者軟件產品的強大安全性。
- 網絡模板框架（**SSDF PW.5.1**）：使用實現用戶輸入自動轉義的網頁模板框架，以避免網頁攻擊，例如跨站腳本。
- 參數化查詢（**SSDF PW 5.1**）：使用參數化查詢而不是在查詢中包含用戶輸入，以避免 **SQL** 注入攻擊。
- 靜態和動態應用程式安全測試（**SAST/DAST**）（**SSDF PW.7.2**、**PW.8.2**）：

  使用這些工具來分析產品源代碼和應用程式行為，以檢測容易出錯的做法。 這些工具涵蓋了從內存管理不當到容易出錯的數據庫查詢構造（例如，未轉義的用戶輸入導致 **SQL** 注入）等問題。 **SAST** 和 **DAST** 工具可以被納入開發流程，並作為軟件開發的一部分自動運行。 **SAST** 和 **DAST** 應補充其他類型的測試，例如單元測試和集成測試，以確保產品符合預期的安全要求。 當發現問題時，製造商應執行根本原因分析，以系統地解決漏洞。
- 代碼審查（**SSDF PW.7.1**、**PW.7.2**）：努力確保提交到產品中的代碼經過其他開發者的同行審查，以確保更高的質量。
- 軟件材料清單 **(SBOM)**（**SSDF PS.3.2**、**PW.4.1**）：納入**SBOM**[3] 的創建，以提供對進入產品的軟件集的可見性。
- 漏洞披露計劃（**SSDF RV.1.3**）：建立漏洞披露計劃，允許安全研究人員報告漏洞並在此過程中獲得法律上的安全港。 作為其中的一部分，供應商應建立流程以確定已發現漏洞的根本原因。 此類流程應包括確定採用本文中的任何「設計安全」實踐（或其他類似實踐）是否會防止漏洞的引入。

[3] 一些編寫機構正在探索其他方法，來獲得圍繞軟件供應鏈的安全保證。

- **CVE** 完整性：確保已發布的 **CVE** 包括根本原因或常見弱點枚舉 **(CWE)**，以便對軟件安全根本原因進行全行業分析。 雖然確保每個 **CVE** 都是正確和完整的可能需要額外的時間，但它允許不同的實體發現有利於所有製造商和客戶的行業趨勢。 有關管理漏洞的更多資訊，請參閱 **CISA** 的利益相關者特定 **SVCC** 指南。
- 深度防禦：設計基礎架構，使單個安全控制被破壞不會導致整個系統被破壞。 例如，確保嚴格規定用戶權限並使用訪問控制列表可以降低受破壞帳戶的影響。 此外，軟件沙盒技術可以隔離漏洞以限制對整個應用程式的破壞。
- 滿足網絡性能目標 **(CPG)**：設計滿足基本安全實踐的產品。 **CISA** 的網絡安全績效目標概述了組織應實施的基本、基線網絡安全措施。 此外，有關加強組織態勢的更多方法，請參閱英國的網絡評估框架，該框架與 **CISA** 的 **CPG** 有相似之處。 如果製造商未能滿足 **CPG**，例如不要求所有員工進行防網絡釣魚的多因素身份驗證，那麼他們就不能被視為提供「設計安全」的產品。

編寫機構認識到這些變革是組織態勢的重大轉變。 因此，它們的引入應根據關鍵性、複雜性和業務影響進行優先排序。 這些做法可以引入到新軟件中，並逐步擴展到覆蓋其他使用情況和產品。 在某些情況下，某種產品的關鍵性和風險狀況可能值得加速採用這些實踐。 在其他情況下，可以將實踐引入遺留代碼庫，並隨時間進行修復。

「預設安全」策略

除了採用「設計安全」開發實踐外，編寫機構還建議軟件製造商在其產品中優先考慮「預設安全」的配置。 這些製造商應該努力更新產品，以便在產品更新時符合這些實踐。 例如：

- 消除預設密碼：產品不應帶有普遍共用的預設密碼。為消除預設密碼，編寫機構建議產品要求管理員在安裝和配置期間設置一個強密碼。
    - 對特權用戶強制執行多因素身份驗證 **(MFA)**。 我們觀察到許多企業部署是由未使用 **MFA** 保護的帳戶的管理員管理的。鑑於管理員是高價值目標，產品應該讓 **MFA** 選擇退出而不是選擇加入。 此外，系統應定期提示管理員註冊 **MFA**，直到他們在其帳戶上成功啟用它。 荷蘭的**NCSC**有與 **CISA** 類似的指導，請查閱他們的成熟認證資訊單張了解更多資訊。
- 單點登錄 **(SSO)**：**IT** 應用程式應通過現代開放標準實施單點登錄技術。 這方面的示例包括安全斷言標記語言 **(SAML)** 或 **OpenID**連接**(OIDC)**。此功能應預設提供，無需額外費用。
- 安全日誌：為客戶提供高質量的審計日誌，不收取額外費用。 審計日誌對於檢測和升級潛在的安全事件至關重要。 在調查疑似或已確認的安全事件期間亦甚為重要。 考慮最佳做法，例如將安全資訊和事件管理 **(SIEM)** 系統與使用協調世界時 **(UTC)**

、標準時區格式和強大的文檔技術的應用程式編程接口 **(API)**更易於整合。

- 軟件授權配置文件：軟件供應商應提供有關授權配置文件角色及其指定使用情況的建議。 製造商應包括一個明顯的警告，通知客戶如果他們偏離了建議的配置文件授權，就會增加風險。 例如：醫生可以查看所有患者記錄，但醫療調度員對安排預約所需的地址資訊的存取權限有限。
- 前瞻性安全優於後向兼容性：向後兼容的遺留功能往往包含在產品中，並且經常在產品中啟用，儘管這會給產品安全帶來風險。 將安全性置於向後兼容性之上，使安全團隊能夠刪除不安全的功能，即使這意味著會導致重大更改。
- 跟踪並縮減「加固指南」的大小：縮減為產品製作的「加固指南」的大小，並努力確保隨著軟件新版本的發布，尺寸會越來越小。將「加固指南」的組件整合為產品的預設配置。 編寫機構認識到，縮短加固指南是與現有客戶持續合作的結果，包括許多產品團隊的努力，包括用戶體驗 **(UX)**。
- 考慮安全設置對用戶體驗的影響：每個新設置都會增加最終用戶的認知負擔，應該結合所帶來的商業利益進行評估。 理想情況下，一個設置不應該存在； 相反，最安全的設置應該預設集成到產品中。 當配置是必要的時候，預設選項應能夠廣泛地對抗常見威脅。

編寫機構承認這些變化可能會對軟件的使用方式產生操作影響。 因此，客戶的意見對於平衡操作和安全考慮至關重要。 編寫機構認為，制定書面路線圖和行政支持，將這些想法優先納入組織最關鍵的產品中，是轉向安全軟件開發實踐的第一步。 雖然客戶的意見很重要，但編寫機構觀察到一些客戶不願或不能採用改進標準（通常是網絡協議）的重要案例。 對於製造商來說，重要的是要為客戶創造有意義的激勵措施，讓他們保持最新，並不允許他們無限期地存在漏洞。

加固與鬆散指南

加固指南的產生可能是由於缺乏從開發之初就嵌入到產品架構中的產品安全控制。 因此，加固指南也可以成為對手查明和利用不安全功能的路線圖。 許多組織通常不知道強化指南，因此他們的設備配置設置處於不安全的狀態。 一種被稱為鬆動指南的倒置模型應該取代這種加固指南，並解釋用戶應該進行哪些更改，同時列出由此產生的安全風險。

編寫機構建議軟件製造商通過提供鬆散指南轉向「預設安全」方法，而不是開發列出保護產品方法的強化指南。 這些指南以通俗易懂的語言解釋決策的商業風險，並可以提高組織對惡意網絡入侵風險的認識。 安全權衡應由客戶的高級管理人員決定，平衡安全與其他業務需求。

給客戶的建議

編寫機構建議組織讓他們的供應技術製造商對其產品的安全結果負責。 作為其中的一部分，編寫機構建議組織高管將購買「設計安全」和「預設安全」產品的重要性放在首位。 這可以通過制定政策要求 **IT** 部門在購買製造商軟件之前評估其安全性，以及授權 **IT** 部門在必要時推回來體現。 應授權 **IT** 部門製定採購標準，強調「設計安全」和「預設安全」實踐（本文檔中概述的那些以及組織製定的其他實踐）的重要性。 此外，在採購決策中執行這些標準時，**IT** 部門應該得到執行管理層的支持。 接受與特定技術產品相關風險的組織決策應正式記錄在案，由高級業務主管批准，並定期提交給董事會。

支持組織安全態勢的關鍵企業 **IT** 服務，例如企業網絡、企業身份和存取管理以及安全運營和響應能力，應被視為關鍵業務功能，對其提供的資金與其對組織任務成功的重要性保持一致。組織應制定計劃，升級這些功能，以採用「設計安全」和「預設安全」實踐的製造商。

在可能的情況下，組織應努力與他們的主要 **IT** 供應商建立戰略夥伴關係。 這種關係包括組織多個級別的信任，並提供解決問題和確定共同優先事項的工具。 安全應該是這種關係的一個關鍵要素，組織應該努力在關係的正式（例如，合同或供應商協議）和非正式方面加強「設計安全」和「預設安全」實踐的重要性。 組織應該期望其技術供應商對其內部控制狀況以及採用「設計安全」和「預設安全」實踐的路線圖保持透明。

除了將「預設安全」作為組織內的優先事項外，**IT** 領導者還應與業內同行合作，了解哪些產品和服務最能體現這些設計原則。 這些領導者應協調他們的請求，以幫助製造商確定他們即將推出的安全計劃的優先級。 通過合作，客戶可以幫助向製造商提供有意義的意見，並為他們創造優先考慮安全性的激勵措施。

在利用雲端系統時，組織應確保他們了解與其技術供應商的責任共擔模式。 也就是說，組織應該清楚供應商的安全責任，而不僅僅是客戶的責任。組織應該優先考慮那些對其安全狀態、內部控制和在責任共擔模式下履行自己義務的能力透明的供應商。

免責聲明

本報告中的資訊按「原樣」提供，僅供參考。 **CISA** 和編寫機構不認可任何商業產品或服務，包括任何分析對象。 任何通過服務標誌、商標、製造商或其他方式對特定商業實體或商業產品、流程或服務的提及，並不構成或暗示 **CISA** 和編寫機構的背書、推薦或偏袒。 本文件是 **CISA** 的聯合倡議，並不自動作為監管文件。

資源

CISA

- 軟體組件清單 (SBOM) 指南
- CISA 跨行業網絡安全績效目標
- 技術互通性指南
- CISA和 NIST的防禦軟件供應鏈
- 不安全技術的代價及我們能夠採取的措施|CISA
- 停止推卸網絡安全責任：為什麼公司必須將安全納入科技產品中（foreignaffairs.com）
- CISA利益相關者特定漏洞分類 (SSVC) 指南
- CISA的抗釣魚多重身份驗證資訊單張
- 面向小企業的網絡安全指南|CISA

NSA

- NSA 的內存安全網絡安全資訊表
- NSA的ESF 確保軟件供應鏈安全：供應商的最佳做法

FBI

- 理解和應對 SolarWinds 供應鏈攻擊：聯邦的觀點
- 網絡威脅—應對和報告
- FBI 的網絡安全策略

國家標準與技術研究所 (NIST)

- NIST 的數字身份指南
- NIST 的網絡安全框架

- NIST 的安全軟件開發框架（SSDF）

澳洲網絡安全中心（ACSC）

- ACSC 的物聯網製造商守則指南

英國國家網絡安全中心（UK）

- 英國的網絡評估框架
- 英國 NCSC 的安全開發與部署指南
- 英國 NCSC 的漏洞管理指南
- 英國 NCSC 的漏洞披露工具包
- 劍橋大學的 CHERI
- 再見，感謝所有的位元組—NCSC.GOV.UK

加拿大網絡安全中心（CCS）

- CCS 的防範軟件供應鏈攻擊指南
- 網絡供應鏈：風險評估方法
- 加拿大網絡安全中心提供的CONTI勒索軟件指南

德國聯邦資訊安全辦公室**(BSI)**

- BSI Grundschutz綱要（模組CON.8）
- 國際標準IEC 62443第4-1部分
- 2022年德國IT安全狀況報告
- BSI網站應用安全的最佳實踐

荷蘭國家網絡安全中心

- NCSC-NL成熟身份驗證資訊單張

其他

- 複雜系統如何失敗
- 複雜系統故障的新觀點