背景資訊

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern,
Germany
Deutschland／Germany
www.pilz.com

2025 年 10 月

保護公司、機械設備及產品

安全與工業資安 – 一站式服務

奧斯菲爾，2025 年 10 月 – **資安事件不再僅影響 IT 系統，而是日益影響生產環境（OT）。工業資安事件不僅包含針對性攻擊，也包含非預期的操縱。在生產中，工業資安的使命是確保工廠與機械設備的可用性，以及機器資料和流程的完整性和機密性。然而，最高的保護目標是功能安全。因為歸根究柢，若公司無法掌控其資料，則公司和員工的安全都處於危險之中：沒有資安就沒有安全，而沒有安全，人員就無法受到保護！**

歐盟已認知到日益嚴峻的威脅態勢，並已據此調整立法：在公司層級，**NIS 2 指令**要求採取措施，例如透過資訊安全管理系統 (ISMS) 確保歐盟內網路資安的高度統一標準。

機械規則 2023/1230
現在規定工廠與機械設備的防破壞保護，並要求對影響功能安全的機器零件採取工業資安措施。

網路韌性法案（CRA）要求具備數位元件的產品採取資安措施。這些產品包含控制器、IO 系統，以及機械設備中使用的其他元件。

公司、機械設備及產品 –

在每個層面，機器製造商和營運商面臨到不同挑戰和不同法律框架。

符合最新技術的資安

儘管立法正將工業資安列為強制要求，仍有許多充分理由應儘早處理此議題並尋求專業建議。若未定期檢視，操作機械設備的既定流程與

條件可能助長操縱行為。例如，機械設備的長使用壽命往往導致相應系統過時，並在某個時間點不再符合現行資安標準。這些系統存在無法再修補的資安漏洞，因為供應商已停止提供資安更新。通常，終端裝置無法實施惡意軟體防護，因為部分裝置過於老舊，其性能會因此受到影響，可能導致生產停機。

逐步提升工業資安

歸根究柢，旨在確保業務營運持續受到保護，但是為達成此目標，公司必須克服各種挑戰：從識別適用的法規要求、偵測與修復系統漏洞，到提升員工的意識和訓練，以及後續執行控制措施。由於資安是個動態目標，因此也有必要定期檢查機械設備的工業資安狀態。重要的是在公司內明確職責，並採用系統化方法建立必要的專業知識。

自動化公司 Pilz
已為這些要求做好準備，並為全球機器製造商與使用者開發出客製化的服務產品組合，可全面涵蓋人員與機器保護的所有層面。Pilz
的專家瞭解當前的法律與標準化要求，並將這些納入其建議中。培訓課程完善了我們的服務，讓公司能夠建立或更新其資安知識。Pilz
產品解決方案也用於實務實施，例如用於提升安全和工業資安的識別進入管理（I.A.M.）系統。

奠定正確的基礎

為了確保自身機械設備的工業資安，機械工程領域的專家需要具備紮實基礎知識 – 特別是法規和適用標準。Pilz
的專家在「工業資安基礎」培訓課程中分享這些專業知識。學員將學習理解機械設備和網路資安情境中的資安威脅、適當保護措施及最佳

實務。因此，即使是資安領域的新手也能瞭解可以採取哪些措施，有效保護機械設備免於機器生產層級的網路攻擊與操縱。

透過「CESA – 自動化資安專家認證」，Pilz 提供為期兩天的專家課程，為參加者提供符合最新標準的深入資安知識，特別是關於 IEC 62443 系列標準（「工業通訊網路 – 網路和系統的 IT 資安」）。此外，培訓涵蓋實務風險降低措施，例如存取控制、使用技術手段和組織措施提升網路資安，以避免資安風險。參與者將學習如何正確應用該標準，並證明其自動化系統符合網路資安要求。通過測驗之後，參與者將獲得全球認可的 TÜV NORD「CESA – 自動化資安認證專家」證書。

將理論付諸實踐

在理論基礎與培訓之上，強化工業資安的下一步是應用結構化的實務流程。操作技術（OT）諮詢服務，可彌補理論基礎與可實行策略之間的差距。透過循序漸進的方法，工業資安服務可識別複雜系統中的漏洞，並制定措施將風險降至最低。結果是全面的資安概念。

提升工業資安的四個步驟

OT 資安程序包含四個步驟：防護需求分析、工業資安風險評估、工業資安概念及工業資安系統驗證。

在防護需求分析期間，公司可識別工廠或機器中個別「資產」的防護要求與其防護目標。第二步驟是風險評估，針對系統整個生命週期的每個子系統，考量所有風險以及發生的可能性。下一步驟是制定詳細的工業資安概念，採用策略與措施防禦並減輕攻擊、操縱與操作者錯

誤所造成的風險。此外，還需制定政策、規則與準則，以確保系統持續安全運作或維持安全架構。最後步驟是工業資安系統驗證，檢查已實施對策的有效性。

確保機器可用性

工業資安服務流程可協助減輕或防止網路攻擊。非預期觸發的資安事件數量也下降。這進而提升機器可用性，最終確保節省成本，，同時維護經濟效益。

這種方法透過適當的資安措施，主要保護機器上的人員。因為資安事件可妨礙安全措施。例如，機械設備前面的光柵可確保操作人員不會進入危險區塊。然而，若攻擊者能影響相關控制器與機構，則安全光柵的保護功能可能無法再獲得保障。資安保障安全！

因此，在機器的實際實施中，將安全與資安一併考量是合理的。因為：沒有資安就沒有安全，而沒有安全，人員就無法受到保護！

明確規範：誰能在機器上做什麼？

機器及其操作人員的安全取決於存取控制 –
無論是人員或網路。入口點必須受到保護以防止未經授權的存取，例如確保任何人都不會在機器運作時處於危險區域內。即使是出於善意的工廠操作或維護（無論在現場或透過網路），也可能產生致命後果。

其明確規範公司內工廠與機械設備的權限和存取的識別進入管理（I.A.M.）是重要要素。這些包含組織措施與規範，以及適當的安全與資安功能。Pilz 的 PITreader

等存取權限系統即為適當的產品元件。這意指使用者可符合有關員工保護、責任保護、最大產能及資料保護的要求。

只有全面的安全與資安方法才能保確保人員和機器獲得全面保護。是否想要應對資安問題以及到何種程度，將不再由公司自行決定。現在已成為法規要求。在工程設計中，工業資安形式的資安不僅是 IT 的任務，更是設計和構造不可或缺的一部分。事後實施資安非常複雜，且通常意味著使用便利性、功能性及生產力會降低。

((字元數：9,784))

((欄位：))

歐盟工業資安立法概述

特別是在歐洲，立法者已透過一系列法律對威脅態勢作出反應。因此，全球最嚴格的要求適用於歐洲。但已與其他國家達成協議，這些法律也將被導入其他國家。因此，工業資安的全球統一指日可待。

NIS 2：公司負有更多義務

NIS（網路與資訊安全）是旨在強化網路資安的歐盟指令。此指令自 2016
年起生效，迄今適用於關鍵基礎設施供應商，包括能源、交通、銀行與金融、衛生、飲用水供應與分配，以及數位基礎架構。這些領域的供應商必須採取「適當的資安防護措施」並通報任何嚴重的網路資安事件。新的 NIS 2 指令（(EU) 2022/2555 ...
有關歐盟內維持高度統一網路資安的措施）要求未來更多公司採取網

路資安風險管理措施。例如，NIS 2 將產業領域擴展至製造 /

生產行業，包含電氣設備的工程與製造商。

要求包含資訊系統的風險分析和資安概念、供應鏈的保護，以及人員安全。存取控制和工廠管理的概念是另一項要求，還有強制性管理訓練。

該指令於 2022
年底由歐洲議會和歐盟理事會通過。與所有歐盟指令一樣，NIS 2
不會立即在各歐盟成員國生效和具有約束力，而是必須由成員國納入其國內法律中。公司明智的做法是盡早處理 NIS

2，並為公司執行全面的資安評估。例如，這包含資訊安全管理系統（ISMS）的建立。在這種情況下，依據資訊安全標準 ISO 27001
進行認證很有幫助。

以風力發電機作為範例的 NIS 2：根據 NIS
2，發電設備（如風力發電機）製造商等機器製造商，未來也必須符合相關要求。進而，風力發電機製造商需要自動化解決方案、控制器或感測器。達到一定規模後，電氣元件製造商也在 NIS 2
的管轄範圍內。而由於 NIS 2 也規定將供應商列入考慮，Pilz
等公司也必須關注安全供應鏈，並對其供應商提出要求。因此 NIS 2
涵蓋整個供應鏈。

新機械規則：沒有資安，就沒有 CE 標章

機械指令 2006/42/EC 在機械設備的功能安全方面具有特殊重要性。

為了將機械設備進口到歐洲，機器製造商始終必須經歷相關合規性評估流程，最後取得 CE 標章。

於 2023 年 6 月重新發佈為機械規則，規範已升級至最新技術水準。由於是規則，因此不必先轉換成國家法律。機器製造商必須於 2027 年 1 月 20 日前調整以符合新要求，並自該關鍵日期起滿足這些要求。

機械規則取代現有的機械指令，與前身不同的是，其將網路資安列為強制要求。機械指令純粹檢驗安全性，而該規則在「基本健康與安全要求 (EHSR)」的「防破壞」項下包含資安保護目標：機器的安全功能不得因意外或故意破壞而受到損害。

這種取得 CE 標章的新途徑為機器製造商和營運商帶來許多新問題，因為他們將需要修訂既有的安全和資安概念。

網路韌性法案：涵蓋整個產品生命週期的資安

除了檢驗公司和機械設備以外，也絕對也有必要直接在裝置（如控制器）中實施資安措施。2022 年 9 月，歐盟委員會提交了旨在提升產品網路資安的規則草案。此網路韌性法案（CRA）針對具備數位元件（硬體與軟體）且能與其他產品通訊的產品製造商。智慧型手機或機器人吸塵器等 B2C 領域的產品、控制器和感測器等 B2B 領域的產品，以及作業系統或機器本身等純軟體產品皆受此影響。

製造商對已被利用漏洞的通報義務自 2026 年 9 月 11 日起適用。自 2027 年 12 月 12 日起，具備數位元件的產品必須滿足 CRA 的要求，才能在歐盟市場上銷售。CRA 是歐盟規則，因此將立即在歐盟成員國生效。

CRA 的影響實際有多大，取決於最終建立的產品分類標準。依據 CRA，只有保能確保適當網路資安等級的產品才能投放到市場 – 且須涵蓋產品的整個生命週期。因此，資安始於產品開發階段。所以多年來，Pilz 也將其開發流程與 IEC 62443-4-1「工業自動化和控制系統的資安 – 第 4-1 部分：安全產品開發生命週期要求」保持一致，並開發出例如可證明安全的 SecurityBridge。

((字元數：6,062))

Pilz – 安全精神

Pilz 是自動化技術產品、系統及服務的全球供應商。身為安全自動化的先驅，Pilz 可為人類、機器及環境創建安全。成立於 1948 年，如今總部位於奧斯菲爾的該家族企業，在全球 42 家子公司與分公司擁有 2500 名員工。

該技術領導者可提供針對機器安全與工業資安的完整自動化解決方案。其中包含感測器、控制與驅動技術，以及用於工業通訊、診斷及視覺化的系統。國際服務範圍具備諮詢、工程設計及訓練，使得產品組合完整。Pilz 解決方案用於機械工程以及許多產業，例如內部物流、包裝、鐵路技術、半導體、氫能或機器人領域等。

www.pilz.com

社群網路上的 Pilz：

在我們的社群媒體平台上，我們提供關於該公司及 Pilz 人員的背景資訊，並報導自動化技術的最新消息。

www.pilz.com/facebook
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

媒體聯絡人：

Martin Kurth

企業與技術媒體部
電話：+49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

技術與企業媒體部
電話：+49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

技術媒體部

電話：+49 711 3409-1067
j.skarman@pilz.de

Eva Gellner-Rössle

技術媒體部

電話：+49 711 3409-7147
e.roessle@pilz.de