*本節及本文件其他章節所載資料及統計數據摘自我們委託弗若斯特沙利文編製的報告，以及各種政府官方出版物及其他公開出版物。我們委託弗若斯特沙利文就**[編纂]**編製獨立行業報告－弗若斯特沙利文報告。*

*本公司、聯席保薦人、**[編纂]**、**[編纂]**、**[編纂]**、**[編纂]**、**[編纂]**、**[編纂]**或參與**[編纂]**的任何其他各方(弗若斯特沙利文除外)或其各自的董事、高級職員、員工、顧問或代理並未獨立核實官方政府出版物以及有關資料及統計數據，且不對該等資料及統計數據的準確性或完整性發表任何聲明。*

中國工業網絡安全市場

工業網絡安全的定義

工業網絡安全，也稱為工業控制系統網絡安全，指運用系統化的風險管理方法、技術控制手段及分層防禦措施，專門設計的全面防禦體系。其核心目標在於保護工業生產流程中所有相關IT與OT資產(包括網絡、系統、數據、應用程序及設備)免受攻擊，確保工業生產環境的可靠性、完整性、機密性與可用性，並有效抵禦網絡攻擊、破壞活動及未經授權存取等安全威脅。工業控制系統是能源和電力等關鍵信息基礎設施的核心，支撐著國計民生和關鍵基礎設施的安全穩定運行。因此，工業網絡安全具有區別於傳統信息安全的獨特特點和戰略意義。其已被納入國家戰略安全框架，是實現網絡強國和製造強國目標的重要基石。

工業網絡安全防護範圍廣泛，主要涵蓋工業控制系統的網絡安全，以及其他工業生產活動中涉及的網絡相關設備與場景所需的安全防護。現已形成涵蓋現場至管理的完整產品與服務體系。工業網絡安全產品可根據其主要功能分為四大類：

- ***防護隔離產品：***

該等產品構成了工業環境的基礎防禦框架，包括部署於IT/OT邊界或內部OT區域之間的工業防火墻與工業網關。此類產品實施嚴格存取控制與協議過濾，並能透過深度解析工業協議，實時檢測異常指令、非法操作或已知漏洞攻擊。

- ***檢測評估產品：***

該等產品透過分析異常網絡流量、主動掃描系統或識別系統弱點，為外部入侵和內部漏洞提供全面覆蓋，從而對目標環境提供整體性的安全評估。此類典型產品包括網絡入侵檢測、漏洞掃描系統、配置合規性檢查系統等。

- ***監測審計產品：***

該等產品主要包括網絡流量審計平台、日誌審計系統和數據庫審計系統。通過持續監測關鍵網絡和設備的運行狀態及通信行為，該等工具能即時識別可疑的訪問嘗試、異常活動和潛在風險，將碎片化的警報和日誌轉化為可理解、可操作的事件線索，從而實現主動的威脅識別、快速響應以及事後閉環分析。

- ***管理平台產品：***

核心為工業安全趨勢感知平台，其可彙集來自運營站點的安全數據，並將工業威脅情報與資產發現功能相整合，提供集中管理、統一日誌分析、整合威脅警報及其他功能，為企業提供可視化、集中的安全運營能力。

中國工業網絡安全行業的發展

中國工業網絡安全行業的發展歷經三個不同階段：

初始階段(2010年前)：該期間，中國工業企業對網絡安全的認知尚淺，普遍採用物理隔離的部署模式，即氣隙防禦。安全投入主要聚焦於確保系統的可靠性與實體安全，普遍認為只要系統不連接外部網絡便不會遭受網絡攻擊。因此，市場上幾乎沒有針對工業協議與工業網絡環境的本土化專業安全產品。安全需求基本上呈現分散被動狀態，行業發展緩慢。

認知覺醒與探索期(2010年至2015年)：震網(Stuxnet)病毒事件徹底打破「物理隔離即安全」的觀點，促使中國工業界對工業網絡安全風險的深刻認知。政府與行業開始研究制定符合國情的工業網絡安全標準規範，例如國家級等級保護制度開始延伸至工業網絡系統領域，引導企業開展初步風險評估與邊界防護探索。安全供應商嘗試整合傳統IT安全技術與工業協議，推出具備初步流量監控與邊界防護功能的解決方案。市場需求最初由電力、石油、石化等關鍵基礎設施行業所驅動。

快速發展階段(2016年至今)：在強勁的國家戰略與法律法規驅動下，此階段成為行業爆發期。《中華人民共和國網絡安全法》與《關鍵信息基礎設施安全保護條例》的頒佈將工業網絡安全提升至國家戰略高度，使合規成為市場的主要驅動力。尤其是，網絡安全等級保護制度2.0全面實施後，工業控制系統被納入強制合規範圍，大幅加速了安全產品的部署。與此同時，隨著工業互聯網、智能製造等新興技術與產業深度融合，攻擊面擴大與實際威脅加劇促使企業構建系統化的深度防禦能力，從而推動市場的快速增長。

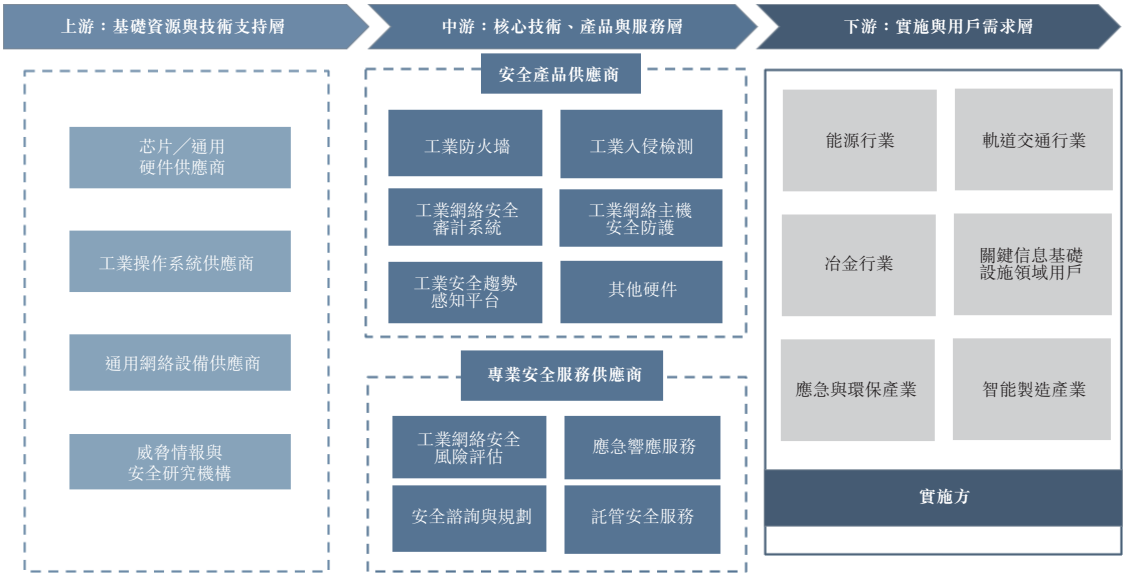
中國工業網絡安全產業鏈

中國工業網絡安全產業鏈的運作模式為高度政策驅動的生態系統。上游領域提供芯片與威脅情報等基礎支持；中游領域交付核心產品與服務；下游領域則以關鍵基礎設施為主要需求來源，系統集成商推動解決方案的定製化實施。整體趨勢呈現向合規導向、操作規範化及自主可控的方向發展。

產業鏈上游作為基礎支撐與技術源頭，主要由提供核心底層技術、通用硬件及關鍵支持服務的供應商構成，包括芯片、通用網絡設備及操作系統(硬件和軟件)供應商，其中特別強調自主可控性與本土化能力。

中游是產業鏈的核心價值創造層，包括安全產品製造商與解決方案供應商，主要提供兩大類功能：安全產品與專業服務。產品層面，該等供應商提供針對工業網絡環境的專用安全產品，例如工業防火墻、工業入侵檢測系統、工業網絡安全審計系統及工業主機安全產品。服務層面，該等供應商提供工業網絡安全風險評估、等級保護合規性評估、應急響應、託管安全營運及人員培訓。

下游涵蓋工業網絡安全解決方案的終端用戶，以及負責實施安全措施的實體。下游客戶主要集中於關鍵信息基礎設施領域及廣泛的智能製造企業，包括對系統穩定性與營運連續性要求極高的行業，例如電力(發電、輸電、配電)、石油化工、軌道交通、冶金、水利及核工業。



資料來源：弗若斯特沙利文

中國工業網絡安全市場

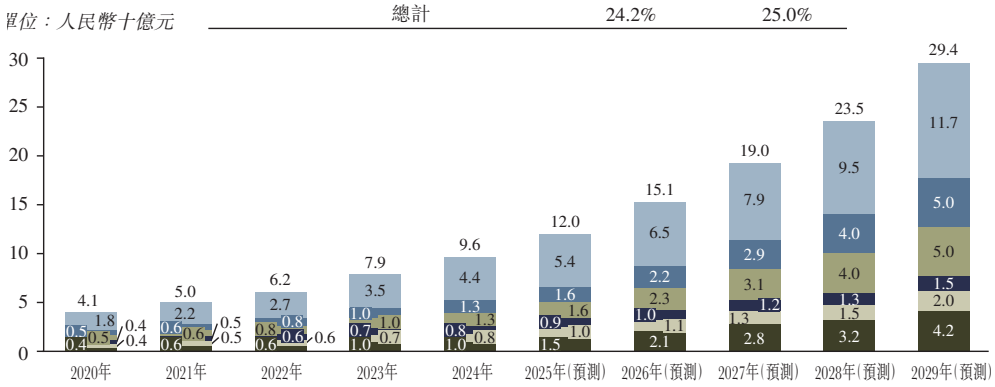
中國工業網絡安全市場的整體規模保持穩定增長。2020年，市場規模為人民幣41億元，至2024年已躍升至人民幣96億元，2020年至2024年的複合年增長率為24.2%。展望未來，預計2029年市場規模將達人民幣294億元，2024年至2029年的複合年增長率預估為25.0%。

從細分市場來看，能源領域工業網絡安全市場規模於2020年達人民幣18億元，2024年增至人民幣44億元，2020年至2024年的複合年增長率為24.7%。預計到2029年將增至人民幣117億元，2024年至2029年的複合年增長率為21.7%，顯示市場穩定擴張趨勢。

智能製造領域工業網絡安全市場規模於2020年達人民幣4億元，2024年增至人民幣13億元，2020年至2024年的複合年增長率為26.2%。受新興領域活力的驅動，該市場規模預計於2024年至2029年以30.7%的複合年增長率增長，於2029年達到人民幣50億元。軌道交通領域的工業網絡安全市場規模於2024年達到人民幣13億元。預計到2029年將達到人民幣50億元，2024年至2029年的複合年增長率預計為30.3%，保持穩定增長趨勢。

中國工業網絡安全市場規模(2020年至2029年(預測))

複合年增長率	2020年至2024年	2029年(預測)
能源	24.7%	21.7%
智能製造	26.2%	30.7%
軌道交通	27.9%	30.3%
冶金	18.5%	12.9%
應急與環保	19.3%	20.2%
其他	24.5%	33.0%
總計	24.2%	25.0%



資料來源：弗若斯特沙利文、專家評論

中國工業網絡安全市場的驅動因素

- ***重大網絡安全事件驅動***

多年來，全球工業領域重大安全事件頻發，例如美國核電廠遭蠕蟲攻擊、另一座美國核設施遭受網絡攻擊、伊朗核電廠的震網(Stuxnet)病毒事件、烏克蘭因惡意代碼引發停電，以及WannaCry勒索病毒全球爆發，造成重大的經濟損失與安全威脅。該等事件暴露了工業系統的網絡安全漏洞，尤其在支撐國家穩定關鍵層面的國家重要基礎設施領域。此類事件的發生威脅著社會福祉與國家安全。

- ***攻擊數量與嚴重程度不斷攀升***

CNVD的數據顯示，2021年至2024年，中國工業網絡安全漏洞的數量逐年增加，2024年高風險漏洞的佔比同比上升。勒索軟件、高級持續性威脅及其他針對能源、製造業等關鍵行業的攻擊事件頻發，導致生產中斷、經濟損失及安全風險，迫使企業增加安全投入。

- ***工業網絡安全是保障公共福祉的核心***

現代社會的正常運行高度依賴電力、供水、交通及醫療等關鍵基礎設施的穩定運行。該等系統的調度、監控與自動化運作都由工業控制系統精密掌控。一旦遭受網絡攻擊或發生安全故障，後果可能從服務中斷、日常生活不便，到大規模停電、斷水、交通癱瘓，甚至危及生命安全，直接影響民眾基本生活秩序與社會穩定。因此，保障工業網絡系統的安全等同於守護城市運轉的生命線，是維護公共安全、確保民眾日常生活延續的基石。

- ***企業的工業網絡安全意識提升***

近年來，隨著工業自動化與智能化的趨勢，企業逐步展開信息化轉型。隨著工業網絡系統複雜度持續增加、設備聯網程度提升，針對工業領域的勒索軟件與高級持續性威脅威脅已成常態，促使企業工業網絡安全意識逐步提升。企業已開始將安全視為保障業務連續性的關鍵投資，並逐步部署及完善工業網絡安全體系。

- ***工業網絡系統的固有漏洞***

工業網絡安全市場的需求亦直接源於工業網絡系統本身固有的內生漏洞。當前，大量正在運行的工業網絡系統存在大量歷史遺留問題：仍在運行過時的操作系統，採用設計時未考量安全性的易受攻擊的協議，且其「穩定至上」的核心原則使許多傳統IT安全措施無法適用。這種固有缺陷直接決定了安全防護必須聚焦於彌補該等漏洞，以確保生產連續性與物理安全。

- ***新技術整合***

憑藉低延遲與高帶寬的特點，5G網絡加速了工業設備的廣泛互聯，在提高生產效率的同時大幅擴大了網絡攻擊面。AI技術雖廣泛應用於工業控制流程優化與故障預測，卻也衍生出了模型劫持、數據中毒等新型安全風險。與此同時，新技術的引入打破了傳統工業網絡系統的封閉性，使原本孤立的系統暴露於更複雜的網絡環境中，而傳統靜態防護機制難以應對智能化與自動化背景下的高級持續性威脅。

- ***政策法規驅動合規***

工業網絡安全的發展主要受國家強制性合規要求驅動。國家通過立法手段，將工業網絡安全從傳統的企業建議性指導直接提升為企業的法律義務。以《中華人民共和國網絡安全法》、《網絡安全等級保護2.0》及《關鍵信息基礎設施安全保護條例》為核心的監管框架，強制要求關鍵信息基礎設施運營商同步規劃、建設並實施與工業系統相銜接的安全措施。此機制有效消除了企業的觀望態度，形成了持續且不可逆的剛性市場需求。此外，行業主管部門發佈的細則與評估要求，進一步推動了安全投資的標準化與落實。

中國工業網絡安全市場趨勢

- ***技術融合推動安全系統邁向智能化與主動化***

AI、5G、雲計算、工業物聯網及區塊鏈等新興技術正與工業網絡安全深度融合。人工智能廣泛應用於威脅檢測、異常行為分析及自動化應對，實現從靜態防禦向動態感知、智能分析與主動應對模式的轉變。同時，5G技術催生基於工業物聯網的新型安全防護架構。未來，工業安全防護將實現從被動防禦到主動智能防禦的根本性轉變，推動安全架構向「雲邊端」協同、實時感知及自適應防護演進，助力構建更智能、更韌性、更可信的工業安全保障體系。

此外，隨著工業系統變得日益複雜，數據可視化技術已成為工業網絡安全運營的核心能力。其以圖形和動態的方式直觀呈現網絡拓撲和風險動態，顯著提高了安全運營效率和決策能力。

- ***數據資產化與工業網絡安全升級***

數據已成為工業企業最具價值的戰略資源，涵蓋生產流程參數、設備運行狀態、供應鏈信息和客戶數據等關鍵內容。數據資產的重要性不僅體現在其對生產優化、智能決策和商業模式創新的支持作用上，也體現在其成為網絡攻擊者的首要目標。

未來，工業網絡安全解決方案將更側重於助力客戶實現數據資產的可發現性、可管理性、可保護性和可追溯性。通過將數據安全技術與工業場景需求深度融合，這些解決方案將在釋放數據價值的同時，幫助企業鞏固安全底線。

- ***企業更積極選擇工業網絡安全防護***

下游客戶的行業滲透率全面加速，標誌著市場將從點對點突破階段邁向全面覆蓋階段。過去安全投資不足的各類場景中，工業網絡安全市場份額將迎來快速增長。這源於企業日益認知到，唯有深度融合自身業務場景與流程的安全解決方案才能有效運作，從而催生出對定製化專業安全產品與解決方案的龐大需求。企業將更積極地構建工業網絡安全防護體系。

- ***市場集中度不斷提高***

隨著市場對安全解決方案的專業性、完整性及認證要求的顯著提高，市場准入門檻大幅提高。這使得具備完整產品線、系統化解決方案能力及權威行業認證的領先供應商能持續擴大優勢。中國工業網絡安全市場正加速向龍頭企業集中，行業競爭格局將逐步從初期的分散競爭轉向生態聚合。

- ***國際化進程啟動***

隨著「一帶一路」倡議的深入實施及全球數字化轉型加速，中國工業網絡安全行業的國際化進程已正式啟動。中國企業正逐步突破國內市場框架，初期以中亞、東盟等地理鄰近且產業合作緊密的區域為切入點，透過輸出成熟安全解決方案參與當地能源、交通、製造等關鍵基礎設施建設；未來將進一步拓展至中東、南美等新興市場，滿足其日益增長的工業網絡安全防護需求。中國供應商將憑藉在IT/OT融合與工業互聯網場景中積累的實踐經驗與技術創新，開發符合國際市場需求的產品。

- ***物聯網與工業網絡安全的整合***

隨著工業物聯網設備在各類工業場景中的大規模部署，傳統的OT環境與IT系統正在加速融合。大量異構終端正在接入工業網絡，顯著擴大了攻擊面，並持續增加對工業網絡安全應用的需求。工業網絡正逐步將物聯網特有的輕量級安全機制融入其整體保護架構，並通過統一的安全管理平台實現對大量物聯網設備的可視化監控、行為分析及風險響應。

中國工業網絡安全市場競爭格局

中國工業網絡安全市場的整體競爭格局高度分散，市場集中度較低。這是由於工業網絡安全領域涵蓋的行業和場景極其廣泛，各行業在工藝流程、協議標準和合規要求方面存在顯著差異。

當前，市場競爭正轉向生態聚合及服務化轉型。供應商之間的競爭不再局限於單個產品的性能比較，而是聚焦於提供行業專屬深度解決方案的能力，即深度整合安全產品與特定行業業務流程的能力，以及提供安全運營服務的能力，例如基於雲或本地的7×24小時管理安全和應急響應服務。

在中國，工業網絡安全供應商主要分為三類：(1)進入工業網絡安全領域的傳統安全供應商；(2)專業的工業網絡安全供應商；及(3)涉足安全服務的工業自動化供應商。

	傳統安全供應商	**專業工業網絡安全供應商**	**工業自動化供應商**
核心背景	在IT網絡安全領域擁有深厚的專業經驗。具備成熟、通用的安全產品組合。擁有龐大且多元化的客戶群。	專注於保護工業控制系統。精通工業協議。了解行業專屬合規與監管要求。	主要專注於工業自動化。
技術優勢	標準IT安全技術	支持廣泛的複雜工業通信協議。有效檢測並應對新出現的威脅。	深深嵌入生產和控制環境。
解決方案能力	主要提供傳統的網絡和終端安全產品。	基於深厚的行業專業知識構建解決方案。交付端到端架構。	缺乏全面、獨立的安全防護能力。
主要挑戰	對OT系統了解有限	在大規模擴張方面仍有改進空間。	缺乏深厚的網絡安全專業知識。

資料來源：弗若斯特沙利文

在中國工業網絡安全市場，前五大公司的總市場份額為30.4%，相對分散。其中，在2024年中國工業網絡安全市場排名第一的公司，市場份額為6.7%。其亦為前三大供應商中唯一一家專業的工業網絡安全供應商。

2024年中國工業網絡安全公司排名(按收益計)

排名	品牌	收益	市場份額
		人民幣百萬元	*%*
1	本公司	643.9	6.7%
2	公司A[1]	634.3	6.6%
3	公司B[2]	602.1	6.2%
4	公司C[3]	544.5	5.6%
5	公司D[4]	501.4	5.2%

資料來源：弗若斯特沙利文，專家評論

進入壁壘

- ***技術壁壘***

新進入工業網絡安全行業的企業不能僅僅依靠傳統的IT安全方法來應對複雜的工業環境，而必須將安全能力與生產運營深度融合。這要求供應商不僅要精通IEC61850、Modbus和DNP3等工業協議的深度解析技術，能夠基於業務邏輯識別異常命令，還要圍繞確保生產連續性設計防護理念。其需要實施輕量級、高可用性的嵌入式部署，以防止安全措施影響控制實時性能。尤其是在對接主流控制系統時，供應商必須精準匹配系統的架構特點與運行習慣，以確保策略協調和穩定運行。

1 公司A是一家上海證券交易所上市公司，成立於2014年，總部位於中國北京，主要從事提供網絡安全產品和服務。

2 公司是B一家深圳證券交易所上市公司，成立於1996年，總部位於中國北京，主要從事網絡安全技術和管理安全服務。

3 公司C是一家成立於2014年的私營公司，總部位於中國北京，主要從事工業控制系統網絡安全。

4 公司D是一家深圳證券交易所上市公司，成立於1995年，總部位於中國北京，主要從事綜合網絡安全解決方案。

- ***用戶信任壁壘***

工業系統的零容錯特性意味著客戶對新供應商的容忍度極低。在選擇網絡安全供應商時，工業企業優先考慮安全產品的可靠性、穩定性以及供應商的實際操作經驗，而非價格。新的安全產品在獲得客戶認可之前，必須經過長時間的現場運行和驗證。因此，擁有大量成功行業案例和7×24小時現場應急響應服務系統的成熟供應商，本身就具有强大的競爭壁壘。對於供應商而言，其積累的經驗和客戶群是難以複製的無形資產，這降低了客戶的信任成本，並確保了業務的連續性。

- ***生態壁壘***

工業網絡安全解決方案的成功交付不再取決於單一產品的優劣，而是資源整合能力的體現。領先的供應商需要與主流工業自動化巨頭建立技術兼容性合作，以確保其產品能夠無縫集成到複雜的工業網絡設備中。同時，供應商必須與大型系統集成商建立穩定的渠道合作夥伴關係，利用後者的工程實施能力和行業覆蓋能力，高效交付解決方案。此外，積極參與國家和行業安全標準的制定，能夠影響市場規範和技術路線，進一步構成難以逾越的生態和監管壁壘。

- ***行業經驗壁壘***

在工業網絡安全領域，深厚的經驗積累和獨特的行業專長形成難以複製的核心進入壁壘。企業必須長期深耕特定行業場景，全面了解不同行業的工藝流程、控制邏輯、設備特性和運作習慣，才能準確識別潛在的風險點，並設計出安全適用的防護策略。對OT環境的深刻理解通常是通過多年的項目實踐、與客戶組織的密切合作以及大量實戰攻防演練逐漸積累。此外，工業網絡安全事件具有低頻率和高風險的特點，使得經驗複用和案例積累尤為關鍵。新進入者由於缺乏實際場景驗證和故障處理經驗，在部署過程中容易導致系統中斷或性能下降，從而失去客戶信任。

- ***認證壁壘***

更具挑戰性的是行業專屬認證。例如，要進入電力行業、核工業和軌道交通等核心領域，供應商必須獲得行業主管部門頒發的專業產品認證和入網許可。該等認證涉及漫長的週期和極其嚴格的審核標準，不僅考驗企業的產品性能和安全合規性，也間接驗證了新進入者的資金實力和抗風險能力。只有擁有多年行業經驗的專業供應商，才能持續投入資源以維持該等高門檻資質。

中國能源領域工業網絡安全市場

能源領域的工業網絡安全特指在電力、石油石化和天然氣等能源及公共事業的生產、傳輸、分配和消費環節中，保護核心運營系統免受網絡攻擊、內部威脅和設備故障影響的專業安全體系。其核心目標是確保能源供應和公共服務的高可用性，以及數據和指令的完整性。

鑒於能源行業直接關係到國民經濟、民生和國家安全，其對系統穩定性的要求在所有工業領域中最為嚴苛。因此，能源領域的工業網絡安全解決方案必須具備零容忍和高可靠性的特點。

- ***電網***

電力行業是中國工業網絡安全建設中成熟度最高且投資規模最大的領域。其應用場景覆蓋電力行業、輸電、變電、配電和調度控制的全過程。

在調度控制中心，安全重點在於保護電力二次系統和WAMS，以防惡意指令影響電網的平衡和穩定。工業網絡防火墻、網絡網關和安全審計系統的部署屬於標準配置。在發電廠，核心在於保護DCS，以確保機組運作指令的完整性，避免因攻擊導致的物理損壞或環境事故。

隨著智能電網的發展，大量分佈式電源和智能終端已接入，使得配電自動化和AMI的安全成為新的重點。這需要將安全保護擴展至現場RTU和終端設備，以應對新型IT/OT融合風險。

- ***石油石化***

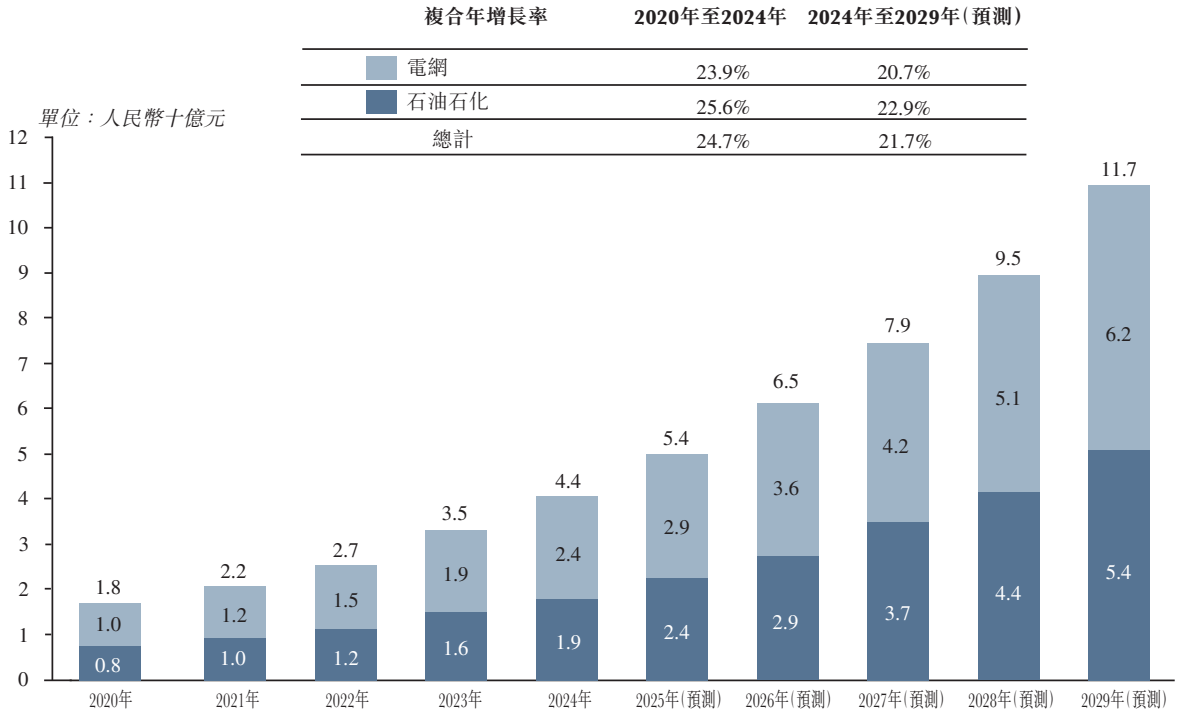
工業網絡安全在石油石化行業的應用場景主要集中在勘探開發、管道運輸、煉油和化工等過程工業環節。

長輸管道的SCADA系統是該領域的關鍵應用。安全重點在於保護RTU的通信安全性和控制指令的可靠性，防止第三方惡意篡改數據流量或引發安全事故。在一體化煉化廠，大量DCS控制著高溫高壓的化學反應過程。安全防護必須注重系統間的邊界隔離和主機加固，以防止因網絡病毒或未經授權操作而導致生產中斷、泄漏或爆炸。

中國能源領域工業網絡安全市場

中國能源領域的工業網絡安全市場涵蓋電網與石油石化兩個子行業，持續保持擴張態勢。總體而言，2020年的市場規模為人民幣18億元，於2024年飈升至人民幣44億元，2020年至2024年的複合年增長率為24.7%，預計到2029年將達到人民幣117億元，2024年至2029年的複合年增長率為21.7%。具體而言，於2020年及2024年，電網行業的市場規模分別為人民幣10億元及人民幣24億元，預計到2029年將達到人民幣62億元，2024年至2029年的複合年增長率為20.7%；而石油石化行業的增長表現更為突出，其市場規模從2020年的人民幣8億元增至2024年的人民幣19億元，2020年至2024年的複合年增長率為25.6%，預計到2029年將達到人民幣54億元。2024年至2029年的複合年增長率為22.9%。

中國能源領域工業網絡安全市場規模(2020年至2029年(預測))



資料來源：弗若斯特沙利文、專家評論

中國能源領域工業網絡安全市場趨勢

- ***安全架構集中化***

能源企業正在加快建設綜合安全運營平台，以實現安全系統集中管理。傳統分散的工業網絡安全產品將統一匯聚數據與事件至中央工業安全態勢感知平台，實現資產可視化、集中威脅預警及統一指揮調度。該趨勢的實現高度依賴於AI智能防禦技術的深度融合。

- ***AI驅動的安全運營***

AI賦能的安全運維將成為未來的核心增長動力。通過對海量工業網絡流量和運行日誌進行異常行為分析(ABA)，AI技術能夠快速識別針對能源系統的高級持續性威脅(APT)攻擊和內部運營風險。這將安全響應從傳統的「事後補救」模式提升至具有「事中阻斷與事前預警」特點的預測性安全運維水平。這種集中化和智能化顯著提升了能源企業安全團隊的效率和威脅處理能力。

- ***操作化能力建設***

根據國家對關鍵基礎設施提出的戰鬥準備、敢於響應和定期運行的要求，實用防禦能力建設已成為能源工業網絡安全的必然趨勢。這要求企業將安全防護從靜態的合規檢查轉為動態對抗與持續運行。能源企業將加大對工業網絡安全範圍和攻防演習的投入，以驗證現有安全系統的有效性。這種注重實踐的趨勢推動安全運營的深化：企業不僅需要購買產品，還需要專業的MSSP服務，以提供持續的威脅情報分析、漏洞管理和應急響應。安全運營的成熟度已成為衡量能源企業安全防護水平的關鍵指標。

- ***加速行業滲透***

隨著行業滲透和市場成熟的加速，能源領域行業專屬安全解決方案的可複製性顯著增強。例如，變電站或輸油管道的標準化安全架構能夠快速部署到類似設施中。這種產品化和模塊化的複製極大提高解決方案的交付效率，從而增強供應商的成本控制能力。對於能源企業而言，這意味著在滿足日益嚴格的合規要求的同時，其可通過採購標準化、高度集成的解決方案來優化安全投資的成本效益。市場將青睞不僅具備技術領先優勢，且在項目實施和長期運營中表現出高效率和低總體擁有成本的供應商。

中國能源領域工業網絡安全市場競爭格局

中國能源領域工業網絡安全市場是整個工業網絡安全市場中進入門檻最高且專業性最強的細分市場。其競爭格局具有兩個核心特徵：高度依賴資質和專業分層競爭。鑒於能源安全對國家安全和民生至關重要，市場准入門檻極高。目前，競爭焦點已從最初的產品性能比拼，轉向系統化、實用化和生態化綜合能力的較量。

按2024年收益計算，本公司位居行業首位，市場份額為8.4%，成為能源領域工業網絡安全市場的領軍企業。

2024年中國能源領域工業網絡安全公司排名(按收益計)

排名	品牌	收益	市場份額
		人民幣百萬元	*%*
1	本公司	368.9	8.4%
2	公司C	317.4	7.3%
3	公司D	269.8	6.2%

資料來源：弗若斯特沙利文、專家評論

中國智能製造工業網絡安全市場

智能製造領域的工業網絡安全指在深度網絡物理集成環境下，為保障智能製造系統整個智能生產流程免受內外部威脅而建立的一體化主動防護體系。其目標不僅包括傳統的可用性，更著重數據機密性與系統完整性，以確保生產不中斷、數據不外洩、決策無謬誤。

- ***智能工廠領域***

作為智能製造的核心單元，智能工廠的工業網絡安全直接關乎生產運營的連續性與穩定性。在高度整合的工廠環境中，各類生產設備、控制系統與信息系統深度融合，共同構成工廠的「數字神經中樞」。該系統面臨多重安全挑戰：既需防範來自企業信息網絡的滲透風險，又需確保生產線控制器與工業機器人等關鍵設備的安全運行。

在實際防護中，智能工廠建立分區分域的安全體系，在不同層級間部署相應防護措施，形成縱深防禦結構。同時，借助統一的安全管理平台，實現對整體網絡安全狀況的實時監控與智能分析，確保安全事件的快速響應與處置。

中國智能製造工業網絡安全市場趨勢

- ***安全理念深化邁向內在整合***

從智能工廠建設初期階段，安全架構便已納入整體規劃，與生產流程同步設計與實施。安全能力不再作為外部附加組件存在，而是作為核心模組嵌入工業互聯網平台、製造執行系統及底層控制器中，實現從設備層到平台層的全面覆蓋。

- ***保護對象擴展至核心數據***

隨著工業數據成為關鍵生產要素，保護重點從傳統設備可用性延伸至數據全生命週期安全。企業正構建涵蓋數據採集、傳輸、儲存及使用全鏈路的安全防護體系，並採用加密傳輸、存取控制及數據去敏感化等技術手段，確保核心流程參數、產品質量數據及設備運行狀態等敏感信息的安全。尤其在研發設計及生產流程等關鍵環節，企業正透過數據血統追蹤及操作行為分析等技術建立完善的防洩漏機制。

中國智能製造工業網絡安全市場競爭格局

智能製造領域作為中國工業網絡安全市場第二大子領域，近年來在製造業加速數智化轉型驅動下，需求持續增長。根據2024年的收益數據，該領域已形成以專業工業網絡安全供應商為主導，傳統網絡安全企業正積極拓展市場版圖的競爭格局。本公司以6.4%的市場份額位居該市場第二，是少數專注工業網絡安全領域且實現規模化增長的專業供應商之一。

2024年中國智能製造工業網絡安全公司排名(按收益計)

排名	品牌	收益	市場份額
		人民幣百萬元	*%*
1	公司C	94.4	7.2%
2	本公司	85.1	6.4%
3	公司A	61.5	4.7%

資料來源：弗若斯特沙利文、專家評論

中國軌道交通工業網絡安全市場

中國軌道交通工業網絡安全市場主要指由確保軌道交通控制系統安全穩定運行的相關技術、產品及服務所構成的市場，其主要涵蓋兩部分：城市軌道交通與國家幹線鐵路(含常規鐵路與高速鐵路)。國家幹線鐵路工業網絡安全市場是伴隨鐵路信息化與智能化發展而快速增長的專業領域，其特點在於能在不干擾鐵路信息系統控制迴路及不影響行車安全的前提下，實現可部署、可協作、可追溯的系統級防護。

作為軌道交通運行的「大腦與神經中樞」，軌道交通控制系統的工業網絡安全主要肩負保障列車運行控制、調度指揮及運營管理等各類系統的可靠性、保密性與完整性的任務。其目標在於防止因網絡攻擊、系統故障或操作失誤導致的運行中斷、安全事故或資料外洩。

- ***列車運行控制安全***

作為軌道交通的「交通控制大腦」，列車運行控制系統透過控制中心、地面設備與車載裝置的協同運作，確保列車安全運行。該系統必須保障控制指令精準傳輸、防止信號干擾與竄改，並維持列車定位與速度等關鍵數據的實時可靠性。實際防護上，採用信號加密與設備認證等安全機制，再結合冗餘設計原則，確保系統在發生故障時仍能維持安全狀態。

- ***綜合監控系統安全***

作為軌道交通的「運營樞紐」，綜合監控系統集供電、環境、設備等多個子系統於一體，負責全線設備的集中監控與管理。該系統必須確保監控數據的完整性與可用性，並保障在緊急情況下能迅速響應。通過建立分區防護架構、實行身份認證與訪問控制，及完善安全審計機制，其為軌道交通的正常運行提供了可靠保障。

中國軌道交通工業網絡安全市場趨勢

- ***合規要求及標準體系的持續完善***

市場發展將繼續受到政策與合規性的雙重驅動。例如，《城市軌道交通綜合監控系統工程技術規範》等文件明確規定，系統應按照三級網絡安全等級保護標準進行設計、建設和驗收。隨著國家對關鍵信息基礎設施保護的加強，相關標準體系、法律及法規將日益嚴格及完善，為市場提供持續的推動力。

- ***加快本地化建設***

受地緣政治及供應鏈安全影響，軌道交通關鍵控制系統的軟硬件國產化替代趨勢正在加速推進。在新建線路中，操作系統、安全芯片、工業控制防火墻及安全可編程邏輯控制器等國產產品的佔比不斷提升。

中國能源數智化綜合解決方案市場概覽

能源數智化市場

能源數智化是能源產業應對能源轉型、提升系統效率、保障能源安全與推進可持續發展的關鍵策略。通過深度融合新興信息技術，其系統化地重構傳統能源產業的基礎設施建設、生產方式、管理機制和價值鏈，實現數智化的協同跨越。

其中，智能以數字化和網絡化為基礎；透過AI能力，可對多源異構數據進行實時感應、識別和分析，並自主解決問題。其感知、認知和解決問題的能力可應用於多個場景，促進生產力的飛躍，並推動產業向高端化、智能化及綠色化轉型。目前，聚焦於能源生產端的智能控制產品，具備實時狀態感知、風險預警和流程優化等核心能力，已成為行業數字化轉型的關鍵推動力。

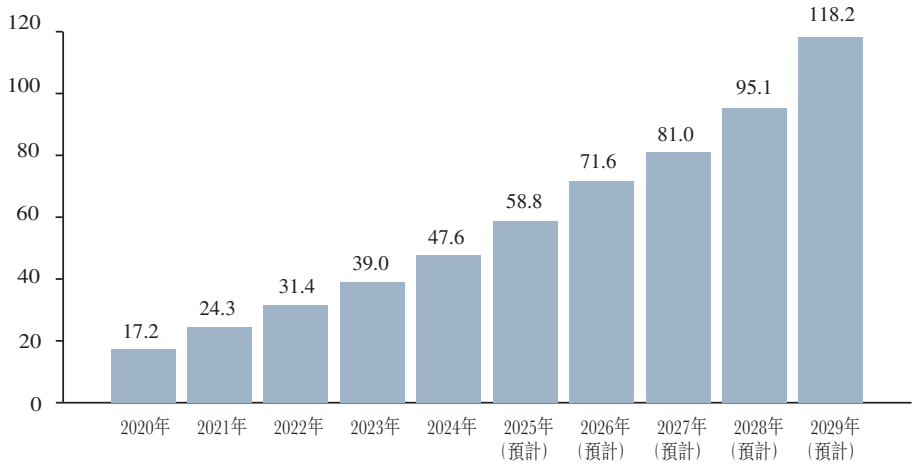
近年來，隨著「雙碳」目標的深入推進和新電力系統的加速建設，能源產業正經歷著前所未有的技術革命。同時，專為工業場景、特殊環境及綠色轉型需求而設計的後備電源解決方案及其集成智能管理系統，因其與電力可靠性、低碳運營及能源效率等行業重點高度契合，正經歷著市場需求的持續增長。數智化轉型已成為推動產業升級的核心引擎。

中國能源數智化綜合解決方案的市場規模已從2020年的人民幣172億元穩步增長至2024年的人民幣476億元，2020年至2024年的複合年增長率為17.4%，預計到2029年將達到人民幣1,182億元，2024年至2029年的複合年增長率為22.9%，顯示出強勁的增長勢頭。該趨勢不僅反映了政策引導和市場需求的雙重驅動，也凸顯了能源企業迫切追求降低成本、提高運營效率、實現綠色低碳轉型和智能運營的決心。

中國能源數智化綜合解決方案市場規模(2020年至2029年(預計))

複合年增長率	2020年至2024年	2024年至2029年(預計)
能源數智化綜合解決方案	17.4%	22.9%

單位：人民幣十億元



資料來源：弗若斯特沙利文、專家評論

能源數智化綜合解決方案市場的驅動因素

- ***能源轉型與可持續發展的需求***

在全球氣候治理框架下，能源系統向清潔化與低碳化轉型已成為共識。傳統能源產業高排放及低效率的模式無法滿足可持續發展目標。然而，能源數智化可對能源生產、傳輸及消費全鏈條進行數字化重構，打破多環節間的協調障礙，為能源轉型提供核心技術支持。其有助於實現碳排放總量控制與能效提升的雙重目標，而這正是驅動市場需求釋放的核心底層邏輯。

- ***能源安全保障的實際需求***

傳統能源系統存在供求響應滯後、資源配置僵化與抗風險能力不足等短板。面對能源資源分佈不均、極端天氣頻發與能源供求格局波動等挑戰，能源系統的韌性和安全性亟待提升。能源數智化可依託新興信息技術，實現能源資產的實時監測、精準預測和智能調度，強化能源系統的風險預警和應急響應能力，保障能源供應的穩定性和可靠性。與此同時，國家層面已明確將提升能源系統安全、可靠、靈活和高效運行能力作為核心目標，進一步鞏固了能源數智化在保障能源安全中的核心地位。

- ***專項政策戰略指引***

國家已出台專項政策以推動人工智能與能源產業深度融合，明確2027年及2030年的分階段發展目標，並從頂層設計角度定義能源數智化發展路徑。《推進「人工智能+」能源高質量發展的實施意見》提出，要深入拓展人工智能在能源領域深度融合應用場景，提升能源領域創新型AI應用的技術能力，加強AI在電力、煤炭、油氣等各行業的深度部署，從而為新型能源體系的發展提供有力支撐。同時，透過中央財政資金、國家科技專項及多層次資本市場提供多維度金融支持。該等政策不僅迫使傳統能源企業加速數智化轉型，更為技術研發與場景執行消除制度性及資金障礙，成為市場規模化發展的核心政策驅動力。

- ***技術創新推動***

AI、大數據、物聯網和數字孿生等技術的成熟與協同發展，為能源數智化奠定了堅實的技術基礎。一方面，專業大模型、多智能體協作與可解釋算法等人工智能技術的突破，可打破傳統能源產業的數據孤島，實現多源異構數據的融合與深度挖掘。另一方面，算力與電力協同機制的構建，以及存儲、算力、網絡一體化等技術的攻克，解決了能源數智化中算力碎片化、能耗高等瓶頸問題。與此同時，隱私計算、動態加密等技術保障了數據安全，賦予能源系統自主感知與認知決策能力，推動能源生產與管理從經驗驅動向數據驅動、智能驅動轉型。這些技術的可行性和成熟度為市場拓展奠定了基礎。

- ***降本增效及培育新質生產力的需求***

傳統能源產業面臨著運營成本高、管理效率低的困境。在能源生產端，設備運維和資源勘探方面均有優化空間；在消費端，能源使用管理和負荷調節方面也存在改進餘地。能源數智化可透過智能流程再造和資源配置，降低能源全生命週期的運維成本和提高能源利用效率。

能源數智化綜合解決方案市場趨勢

- ***深度技術集成及一體化、專業化場景應用***

未來能源數智化將以多種技術的深度融合為特徵。人工智能將不再作為獨立應用存在，而是會與能源領域的專業知識深度融合，形成專業化應用矩陣。技術應用將從孤立的單一使用場景擴展至集成化的綜合場景，涵蓋智能電網規劃與調度、可再生能源產出精準預測、少人或全無人煤炭開採作業、智能油氣勘探等傳統能源領域，同時延伸至虛擬電廠、綠氫生產、零碳工業園區及可控核聚變等新興領域。

- ***算力與電力協同的綠色、一體化發展***

該行業將構建綠色、高效的算力能耗模式，聚焦多源異構算力統一調度、一體化算存網融合等關鍵技術，實現資源集約化利用；努力提高計算中心綠電佔比，探索高效能源利用技術以解決AI計算高能耗問題，形成算力與電力相互支撐、優化的格局。

- ***協作型產業生態系統及平台型創新體系***

能源數智化將推動多利益相關方協作的產業生態系統的形成。政策鼓勵建設能源AI研發平台及跨學科創新聯盟，深化產學研用合作。將建立完善的金融支持與人才培育生態系統，以培育跨學科人才，形成「技術研發 – 場景應用 – 標準制定 – 人才供給」的閉環創新體系，並拓展數據增值服務等新商業模式。

- ***全面安全防護體系及標準體系***

隨著數智化程度的提升，網絡安全與數據安全風險不斷升級。行業將構建覆蓋技術、管理和系統的全面安全防護體系，加強技術措施並提升安全標準和應急機制。政策要求加快制定技術標準(能源數據治理、算力整合及場景設計)，建立AI應用評估體系和測試平台，並鼓勵制定國際標準以推動標準化發展。

- ***高端價值鏈與前沿技術應用***

能源數智化將推動能源產業價值鏈向高端環節延伸。企業的核心競爭力將轉向數據價值挖掘和智能服務。能源領域人工智能技術正在實現跨領域、跨行業、跨業務場景賦能，充分激活能源產業數據價值潛力，加速能源數智化轉型。通過智能感知、智能診斷、智能控制和智能檢測等數智化技術，提升能源企業安全生產管理能力及外部環境適應能力，並為智能生產管理平台及生產經營決策提供技術支持。

- ***高可靠的綠色新能源架構***

隨著能源數智化加速推進，智能後備電源系統朝著智能化、模塊化和綠色化方向演進，不僅能夠通過預測性維護、遠程監控和能效優化從而延長其使用壽命並確保極端情況下的安全，同時通過針對特殊場景的高標準工業電源與儲能產品的定製化開發，顯著提升供電可靠性與運維效率。特別是在數據中心、通信基站、高端製造及關鍵基礎設施等領域，為工業自動化設備、邊緣計算節點乃至整個數字化系統的穩定運行提供堅實的能源保障。

資料來源

本公司已委託獨立市場研究公司弗若斯特沙利文對工業網絡安全市場進行分析並編製報告。本文件所披露的有關弗若斯特沙利文的資料均摘自弗若斯特沙利文報告。我們已同意向弗若斯特沙利文支付人民幣350,000元，作為編製弗若斯特沙利文報告的費用。弗若斯特沙利文報告由弗若斯特沙利文獨立編製，不受我們或其他利益相關方的任何影響。

弗若斯特沙利文報告基於從各種來源獲得的一手和二手研究資料。一手研究包括對工業網絡安全市場中主要行業參與者以及其他與我們業務相關的專家進行訪談。二手研究包括對公司報告、獨立研究報告及弗若斯特沙利文專有研究數據庫和政府數據庫中的數據進行審查。

在匯編及編製本報告時，弗若斯特沙利文作出以下假設：

- 在預測期內，中國及全球其他主要市場的社會、經濟和政治環境將保持穩定，確保行業的持續穩定發展；

- 政府有關工業網絡安全市場的政策不會發生重大變動。

弗若斯特沙利文認為，編製本報告時所用的基本假設(包括對未來預測的假設)均真實、準確且無誤導性。弗若斯特沙利文已對數據進行獨立分析；然而，其審查結論的準確性在很大程度上取決於所收集信息的準確性。