技術詞彙

以下為本文件所用與我們及／或我們業務有關的若干詞彙的詞彙表。因此，該等詞彙及其涵義未必與該等詞彙的標準行業涵義或用法相符。

「5G」	指	第五代蜂窩網絡技術標準
「AI驅動技術」	指	用於增强系統或安全能力的技術
「「氣隙」防禦」	指	依賴於與網絡物理隔離的安全模型
「AMI」	指	先進計量基礎設施，智能電網中用於遠程抄表、用電數據收集及電網管理的集成系統
「高級持續性威脅」	指	高級持續性威脅，一種長期且隱匿的網絡攻擊
「一帶一路」	指	中國全球基礎設施發展戰略
「大數據」	指	從傳統及數字來源捕捉及分析龐大複雜數據集的策略與技術，以推動可執行洞察力及智能決策
「BMS」	指	電池管理系統，電池組內的關鍵電子系統，負責管理可充電電池單元(通常為鋰離子電池)的性能、安全性及使用壽命
「CICSVD」	指	國家工業信息安全漏洞庫(工業控制產品安全漏洞專業庫)，中國國家級專業數據庫，致力於收集、分析、發佈及管理工業控制系統產品、軟件及組件中發現的安全漏洞相關資料
「CII」	指	關鍵信息基礎設施，對國家安全及公共利益至關重要的網絡設施及信息系統
「雲計算」	指	通過互聯網採用按需付費定價模式，按需交付IT資源與應用程序
「雲邊端協同」	指	一種協作式安全架構模型，即一種集成的安全架構模型，將安全功能、智能及數據處理在雲端、邊緣及終端設備三個邏輯層之間進行分佈及協調

技術詞彙

「CMMI 5級」	指	軟件開發的最高成熟度等級認證，一種全球公認的用於改進及評估組織在軟件開發及服務交付方面過程能力的模型
「CNCERT」	指	國家計算機網絡應急技術處理協調中心，隸屬於工業和信息化部，是中國境內及影響中國國家利益的重大網絡安全事件預防、發現、預警及處置的中央協調中心
「CNNVD」	指	國家信息安全漏洞庫，由中國政府授權管理網絡安全漏洞信息的國家級官方平台
「CNVD」	指	國家信息安全漏洞共享平台，是中國負責收集、分析及披露有關信息安全漏洞的資料的國家級平台
「網絡安全等級保護制度2.0」	指	最新的強制性中國網絡安全合規框架
「數據資產化」	指	將數據轉化為有價值戰略資源的過程
「數據庫審計」	指	出於安全、合規及故障排除的目的，對選定的用戶數據庫活動進行系統監測與記錄
「DCS」	指	分佈式控制系統，一種用於過程或工廠的控制系統，其控制器元件分佈在整個系統中
「數字化轉型」	指	將數字技術融入所有業務領域
「數字孿生」	指	一個物理過程或系統的虛擬模型
「DNP3」	指	一種常用於電力和水務設施等關鍵基礎設施的通信協議，支持遠程監測與控制
「雙碳目標」	指	中國的碳達峰及碳中和國家目標
「邊緣物聯網」	指	一種將邊緣算力直接集成到物聯網基礎設施的架構樣式
「能源數智化市場」	指	能源行業數智解決方案市場

技術詞彙

「ERP」	指	企業資源規劃軟件，一套集成的業務應用模塊，旨在通過單一、統一的數據庫及通用用戶介面，管理、自動化及同步組織的核心運營及管理流程
「全生命週期安全保護」	指	涵蓋數據或系統存在所有階段的安全措施
「GPU集群」	指	用於併行計算的圖形處理單元集群
「工業控制系統」	指	一個涵蓋硬件、軟件及網絡組件集成的統稱，該等組件旨在監控、控制及自動化物理工業過程和基礎設施
「IEC 62443」	指	工業自動化和控制系統安全國際標準
「綜合監控系統」	指	綜合監控系統，通常用於軌道交通環境，集中監測多個子系統(如電力、信號、環境)的運行狀態
「工業網絡安全」	指	一套旨在保護工業控制系統、網絡及數據免受網絡威脅的技術、流程與實踐，確保工業運營的連續性、安全性與可靠性
「工業防火墻」	指	一種專為工業控制環境設計的網絡安全設備，用於監測與控制工業網絡流量，以防止未經授權的訪問及惡意攻擊
「工業互聯網」	指	工業機械與聯網傳感器和軟件的集成
「工業入侵檢測」	指	一種用於監測工業網絡異常活動或潛在威脅的系統或工具，旨在迅速檢測並應對安全事件
「工業網絡」	指	一套針對工業生產中IT及OT資產的全面安全保護系統

技術詞彙

「物聯網」	指	物聯網，指由內置傳感器、軟件及其他技術的物理對象(「**物**」)構成的無處不在的網絡，旨在通過互聯網或其他通信網絡與其他設備及系統連接、收集和交換數據
「IPv6」	指	互聯網協議第6版，是互聯網協議的最新版本，為網絡中的計算機提供識別及定位系統，並在互聯網中路由流量
「ISO 14001」	指	環境管理體系認證
「ISO 20000」	指	信息技術服務管理體系認證
「ISO 22301」	指	業務連續性管理體系認證
「ISO 27001」	指	信息安全管理體系認證
「ISO 27701」	指	隱私信息管理體系認證
「ISO 9001」	指	質量管理體系認證
「IT」	指	信息技術，對基於計算機的信息系統的綜合研究、設計、開發、實施、支持及管理
「KPI」	指	關鍵績效指標，用於評估組織或特定活動在實現其關鍵目標方面取得成功的可量化指標
「KVM」	指	基於內核的虛擬機器，一個Linux內核模塊，使操作系統能夠作為管理程序運行多個隔離的虛擬機器
「LFP」	指	磷酸鐵鋰，一種鋰離子電池正極材料，因其穩定性、安全性與長壽命而備受推崇
「日誌審計」	指	對事件日誌進行系統審查，以監測安全性、確保合規並診斷操作問題
「製造執行系統」	指	製造執行系統，用於管理與監測生產流程中的生產活動，實現實時數據收集與流程優化的系統

技術詞彙

「Modbus」	指	一種在工業自動化領域廣泛用於控制器與設備之間數據交換的通信協議
「MSSP」	指	安全託管服務提供商，提供持續安全監控及管理服務
「等保制度」	指	中國網絡安全等級保護制度
「網絡流量審計」	指	檢查及分析網絡中的數據流以確保安全、優化性能及執行合規的過程
「運維」	指	運營及維護，為於項目完成後向客戶或終端用戶就構建的資產或安裝的系統提供所編纂的一套完整的文件
「OMS」	指	訂單管理系統，為集中、自動化及管理客戶訂單整個生命週期的軟件平台或綜合應用組
「一站式國產替代」	指	一項採用全套自主研發／採購技術的戰略
「OT」	指	運營技術，一種專門的硬件及軟件類別，旨在直接監視、控制及管理現實世界中的物理設備、工業過程及基礎設施
「滲透測試」	指	對計算機系統進行授權模擬網絡攻擊，通過利用漏洞評估其安全性
「PKCS#7」	指	一項加密保護消息的標準
「PKI」	指	公開秘鑰基礎設施，一個全面的技術、政策及程序框架，能夠實現數字證書及公開金鑰加密的安全創建、管理、分發、使用、存儲及撤銷
「PLC」	指	可編程邏輯控制器，一種堅固耐用的工業數字計算機，專為製造或工藝環境中的自動化及控制而設計
「政策驅動生態系統」	指	深受政府政策影響的產業生態系統

技術詞彙

「軌道交通工業網絡安全」	指	專為軌道交通系統(如信號、供電及列車控制)量身打造的工業網絡安全措施，確保交通系統的安全與穩定運作
「RTU」	指	遠端終端單元，用於工業設備遠程監測與控制的設備，常見於SCADA系統中
「SCADA」	指	監控與數據採集系統，工業控制系統(ICS)的一個類別，由硬件及軟件組成，用於對地理上分散的資產及流程進行高級監督、控制及實時監測
「SM2/SM4/SM9」	指	中國國密算法
「智能電網」	指	採用數字通信技術的電網
「智能製造」	指	採用計算機控制及AI驅動流程的製造
「SOC/SOH」	指	荷電狀態／健康狀態(電池指標)，一種表明在特定時間點電池的剩餘可用容量的指標，以佔其當前最大容量的百分比(%)表示
「國有企業」	指	國有企業，由國家全資或控股，其經營由政府控制的商業企業
「震網事件」	指	2010年發現的一種複雜的電腦蠕蟲，是已知的第一種專門用於攻擊和破壞工業控制系統的惡意軟件，尤其是伊朗核計劃中使用的系統
「系統化競爭」	指	基於一體化、系統化解決方案能力的市場競爭
「威脅情報」	指	收集、分析及傳播有關潛在或當前網絡威脅的信息，以協助組織預防或應對安全攻擊
「列車運行控制系統」	指	列車運行控制系統，用於監測和管理列車運行狀態、調度及安全控制的系統

技術詞彙

「UPS」	指	不間斷供電系統，一種電氣設備，當主電源(總電源)發生故障時，其幾乎可以立即為連接的設備提供緊急備用電源，防止資料丟失及操作停機
「漏洞掃描」	指	主動識別組織IT系統、網絡及應用程序中的安全性漏洞、配置錯誤及缺失補丁以評估網絡安全風險的自動化過程
「WAMS」	指	廣域測量系統，用於電力系統實時監測電網狀況，以提升電網穩定性與可靠性的系統
「WAN」	指	廣域網，一種在廣闊的地理區域內延伸的電信網絡，例如跨越都市、國家或大陸
「零信任安全理念」	指	假設不存在隱性信任的安全模型