SIEMENS
Ingenuity for life

对症工业网络信息安全，西门子有哪些秘方？

悄无声息之中，一款危险的蠕虫病毒潜入伊朗的核电设施，对工业控制系统发起猛烈攻击，最终导致约 1000 台核离心机发生故障。这就是震惊全球的"震网"病毒。它为工业、能源和交通等基础设施领域的众多企业敲响了警钟，促使其更加重视网络信息安全。

随着数字化浪潮的兴起，各国政府对于工业领域的信息安全也投以关注的目光。2017 年 6 月，中国施行《网络安全法》，对关键基础设施的网络安全保护作出了具体的法律规定。在"工业化与信息化融合"、"互联网+先进制造业"的产业发展趋势下，政府部门的相关法规变得更加严格和具体。在这样的产业和政策环境中，西门子凭借在工业领域深厚的积累和在网络信息安全领域 30 余年的研发经验脱颖而出。

"信任是构建数字化世界坚固的基石，安全是企业运营的一把锁，更是数字化转型升级的根基。"西门子大中华区总裁兼首席执行官赫尔曼（Lothar Herrmann）表示，"凭借卓越的创新技术，广泛的的行业知识与多年的实践经验，我们愿携手各行各业的伙伴，共同构建安全的数字化生态，为数字化旅程保驾护航。"

截至目前，西门子已成为第一家获得信息安全服务资质和核心基础设施等级保护三级认证的在华跨国企业，第一家获得全套 PLC（可编程逻辑控制器）产品安全认证的工业企业，乃至第一家在公司实体、基础设施及关键产品组合三方面均具备相关本地信息安全法律法规认证的在华国际企业。不仅如此，西门子在中国销售运营的所有产品和业务组合都符合中国《网络安全法》的规定。

"这些安全资质就像高级驾照，有了它们才可以放心地驶上数字化快车道，跑得又快又稳。我们为很多客户实施的安全项目均参照中国信息安全等级保护第三级的要求，充分保障企业安全。"西门子（中国）有限公司首席网络与信息安全官胡建钧说道。

这些光环背后是西门子多年的持续投入和辛勤耕耘。西门子全球超过 1300 名网络信息安全专家通力攻关，与顶级大学和研究机构合作创新，与志同道合的行业客户共创实践，在网络信息安全领域每年注册约 70 项新专利。

“相忘于江湖”的 IT 与 OT

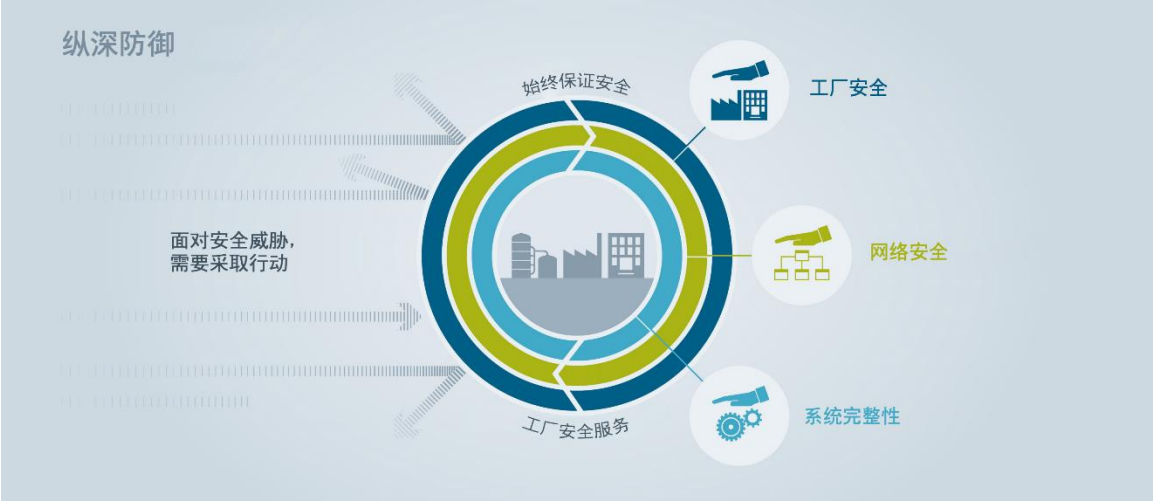
那么究竟何谓工业网络信息安全？

对企业而言，安全通常包含三个层面：物理设备安全、IT（信息技术）安全和 OT（运营技术）安全。

与 IT 系统相比，OT 系统架构更繁杂，组件和层级更多，专用通讯协议也更多样。但 OT 系统的安全保护却通常更为脆弱。以往的工控系统鲜有接入互联网，甚至有的工业设备连 U 盘或网络接口都没有，因此人们往往认为 OT 是远离侵袭的“世外桃源”。

但随着物联网、云计算和 5G 等数字化技术的发展，IT 与 OT 已不再能“相忘于江湖”。那么，如何在实现 IT 与 OT 融合的情况下，完整地保障网络信息安全呢？

西门子配出了秘方——纵深防御安全理念，即从物理安全到网络安全，再到系统完整性的全面防御。工厂物理安全着眼于对自动化系统的物理保护和信息安全管理，包括安保措施、电子门卡等；网络安全是指工业网络中的通信安全，主要目的在于按目标划分不同网络区域，在边界上进行防护，隔离未授权的访问；系统完整性则强调利用认证和用户管理、补丁管理、攻击检测等多种安全手段保障底层工业系统符合设计时的“初心”。



（西门子提出涵盖物理安全、网络安全和系统完整性的纵深防御安全理念）

例如，西门子为江苏徐州市的首条地铁——徐州地铁一号线提供了地铁信号系统，并应用了纵深防御及下一代防火墙技术，为利用无线网络实现对列车的远程监测与控制提供立体安全保障。

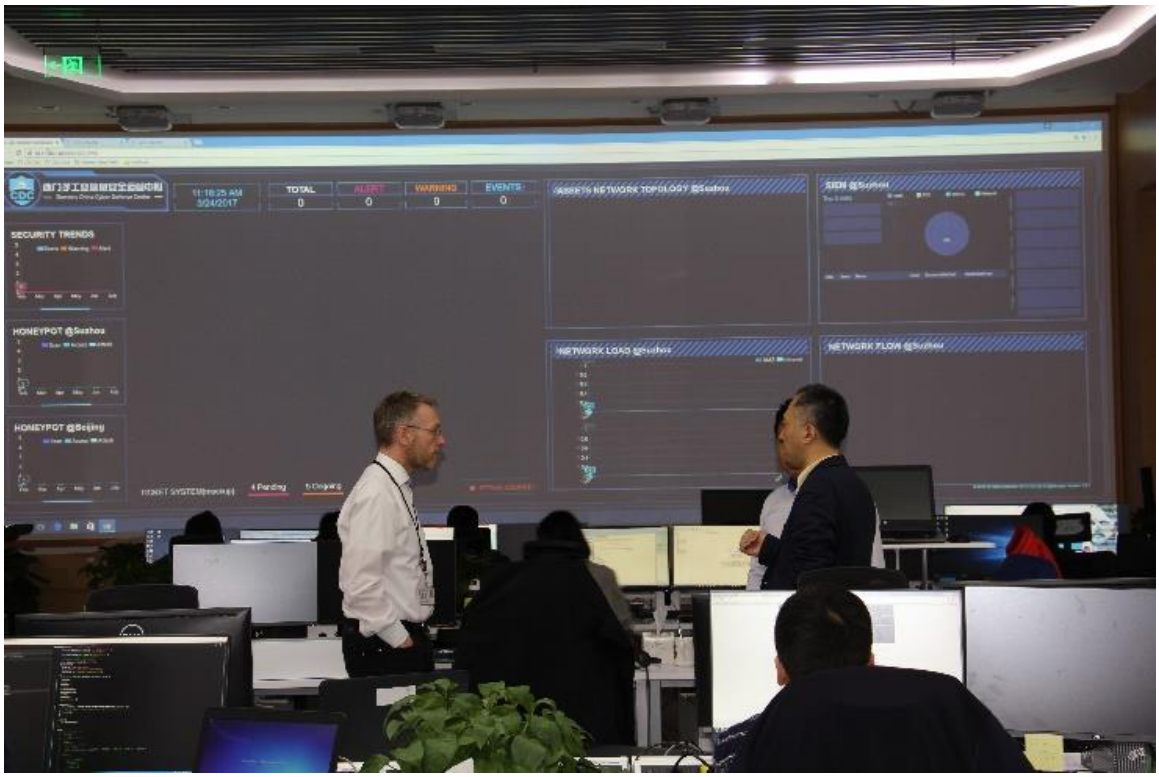
创新驱动 行稳致远

秉承纵深防御安全理念，西门子科学家们不断突破创新，以前沿科技保障着公司和客户数字化资产的安全。

2016 年，西门子工业信息安全运营中心（CDC）在苏州成立，这是西门子全球四大安全运营中心之一，承担着创新、研发以及引领行业实践的重要使命。在这里，科学家们利用威胁情报分析、人工智能、大数据分析等尖端技术，开发了一系列保障安全的系统和工具。

“聪者听于无声，明者见于未形。“保障安全，最重要的莫过于“防患于未然”。因此，CDC 自主研发并部署了安全态势感知系统。它全面收集工业现场数据，实时监测工控网络流量，自动识别异常行为，并可视化地呈现工控系统的关键指标，像如影随形的“私人医生”，全面掌握企业安全的“健康”情况。

目前，西门子位于成都、北京、苏州、无锡等地的工厂都已接入这套系统。工厂网络一旦出现异常，CDC 会立即通知工厂人员，并提供技术建议和指导。



（西门子 CDC 在投入运营后不久就获得了国际信息安全管理标准 ISO 27001 认证及中国信息系统安全等级保护三级认证）

携手客户 共创价值

在钢铁、石化、交通等众多行业，西门子工业网络信息安全解决方案均已落地生根，为客户的数字化转型保驾护航。

早在 2012 年，中国石化青岛炼化公司（青岛炼化）就与西门子合作，以产线病毒防治为切入点，部署了基于纵深防御安全理念的网络信息安全解决方案。2018 年，双方再次携手，将态势感知系统投入实践。

中国石化青岛炼化公司电器仪表中心主任陈鑫表示：“针对数字化转型中的网络安全问题，我们很早就和西门子开展思考和探索。西门子帮助我们真正实现了对工厂内网络信息安全的可感知、可控制和可管理。”

（西门子帮助青岛炼化打造符合网络信息安全标准的标杆智能工厂）

在宝武炭材料科技有限公司（宝武炭材），西门子遵循“评估——实施——持续监控”的整体提升路线，为其布局了涵盖全公司多基地的评估及加固方案。宝武炭材由此提升了工控安全态势感知、安全防护和应急处置能力，在外部威胁和工控网络之间建立起尽可能多层次的保护。

（西门子助力宝武炭材实现对安全的全面感知和防控，上图为宝武炭材集中控制中心）（宝武炭材供图）

从理念到技术创新，再到行业实践，西门子如同技艺精湛的“医生”，对症工业网络信息安全的“顽疾”，开出了良方。然而，在日新月异的网络世界，并不存在百分之百的安全。对西门子而言，对技术创新的不懈追求和服务社会的远大使命都时刻激励着这家百年企业在构筑安全数字化世界的道路上坚定前行！

（此文在 *2020* 年 *4* 月 发布于新华客户端）