INDUSTRIAL CONTROL NETWORK SECURITY

工控网络安全

“双评合规“解决方案

"SECURITY PROTECTION AND COMMERCIAL CIPHER ASSESSMENT COMPLIANCE" SOLUTION

Contents

01 工控网络安全现状及威胁

CURRENT SITUATION AND THREATS OF INDUSTRIAL CONTROL NETWORK SECURITY

- 工控网络概述
- 工控网络主要威胁

工控网络安全现状及威胁

工业控制系统（ICS--Industrial Control System）

工业控制系统（ICS）是数据采集与监视控制系统（SCADA）、分布式控制系统（DCS）、过程控制系统（PCS）、可编程逻辑控制器（PLC）和其他控制系统的总称。工控安全则是保障其安全的网络安全（IT）+自动化（OT）的跨界融合能力。

数据采集与监视控制系统（SCADA）

数据采集与监视控制系统（SCADA，Supervisory Control and Data Acquisition）是一种用于监控和远程控制工业系统和设备的软件系统。它通过收集和显示实时数据，允许操作员远程控制设备和设施。SCADA系统在许多行业和领域中得到广泛应用，包括电力、石油和天然气、水处理、交通控制和远程监控等。

分布式控制系统（DCS）

分布式控制系统（Distributed Control System，DCS）也称集散控制系统，是对生产过程进行集中管理和分散控制的计算机控制系统。DCS通常由多个控制器、通信网络、输入输出设备组成。DCS还可以根据需要将控制功能进一步分散到多个控制器中，实现更加精细的控制。DCS在工业领域得到广泛应用，例如石油化工、电力、钢铁等行业。

过程控制系统（PCS）

过程控制系统（Process Control System，PCS）是用于监控和控制工业过程的核心系统之一。PCS通常包括传感器、控制器、执行器和其他设备，PCS的主要功能是监测工业过程的运行状态和参数，进行控制和调节，确保过程在规定的范围内稳定、高效地运行。广泛应用于石油、化工、电力、钢铁等工业领域。

可编程逻辑控制器（PLC）

可编程逻辑控制器（Programmable Logic Controller，PLC）是一种数字运算操作的电子系统，专为在工业环境应用而设计的。它采用一类可编程的存储器，用于其内部存储程序，执行逻辑运算、顺序控制、定时、计数与算术操作等面向用户的指令，并通过数字或模拟式输入/输出控制各种类型的机械或生产过程。

工控网络安全现状及威胁

工业控制协议（Industrial control protocol）

工业控制协议是用于工业控制系统通信的协议。这些协议用于在各种工业设备之间传输数据和控制信息，以确保设备的正常运行。常见的工业控制协议包括现场总线协议(如Profibus、Ethernet/IP等)、设备通信协议(如Modbus、OPC UA等)。

Profibus协议

是一个用在自动化技术的现场总线标准，在1987年由德国西门子公司等十四家公司及五个研究机构所推动 PROFIBUS 是程序总线网络（PROcess FIeld BUS）的简称；其最大传输信息长度为255B，最大数据长度为244B，典型长度为120B。网络拓扑为线型、树型或总线型，两端带有有源的总线终端电阻。传输速率取决于网络拓扑和总线长度，从9.6Kb/s到12Mb/s不等。

Ethernet/IP协议

是由罗克韦尔自动化公司开发的工业以太网通讯协定，可应用在程序控制及其他自动化的应用中，是通用工业协定（CIP）中的一部分。名称中的IP是"Industrial Protocol"（工业协议）的简称，和网际协议没有关系。Ethernet/IP可以实现长距离传输，最大传输距离可达100公里以上。在短距离传输方面，Ethernet/IP也可以达到高速数据传输，支持10和100M bit/s产品

Modbus协议

是一种串行通信协议，是Modicon公司（现在的施耐德电气 Schneider Electric）于1979年为使用可编程逻辑控制器（PLC）通信而发表。可以使用多种电气接口，如RS-232、RS-485等（串口），还可以在各种介质上传输，如双绞线、光纤、无线等。使用RS-232串口时，Modbus协议的理论传输距离为12米；使用RS-422串口时，理论传输距离为1200米。而在光纤介质上，Modbus协议的传输距离可以达到数公里。

OPC UA协议

OPC全称是OLE（Object Linking and Embedding） for Process Control。为了便于自动化行业不同厂家的设备和应用程序能相互交换数据，定义了一个统一的接口函数，就是OPC协议规范。OPC是基于WINDOWS COM/DOM的技术，可以使用统一的方式去访问不同设备厂商的产品数据。UA全称是unified architecture（统一架构），只使用一个地址空间就能访问之前所有的对象，而且不受WINDOWS平台限制，灵活性和安全性比之前的OPC都提升了。

工控网络安全现状及威胁

工业控制系统常见安全威胁（Common security threats of Industrial control system）

- 黑客攻击：通过网络入侵获取控制权或破坏系统功能
- 软件漏洞：未修复的软件缺陷可能被利用进行攻击
- 人为因素：员工疏忽、恶意行为等可能导致安全事故
- 物理威胁：设备损坏或盗窃可能导致数据泄露或系统失控

美国首次因管道工控安全进入紧急状态!

俄罗斯石油公司德国子公司遭黑客攻击

台积电工控安全事件

3天损失

11.5亿元

2018年8月3日晚间，全球最大的代工芯片制造商台湾积体电路制造（台积电）发现遭受勒索病毒入侵，引发**产线停摆**

富士康被黑客勒索2.3亿

全球制造业巨头富士康证实，其墨西哥一家工厂在5月底遭遇了勒索攻击。黑客组织加密了这家工厂的约1200台服务器，窃取了100 GB的未加密文件，并删除了20TB至30TB的备份内容，并索取1804.0955比特币赎金，约人民币2.3亿元

工控网络安全现状及威胁

工业互联网安全风险综述

随着工业互联网的不断发展，其设备漏洞的数量和种类逐渐增多，给企业和国家带来了极高的网络安全风险。为了有效应对这些挑战，需要加强对工业互联网平台、网络和设备的安全防护，及时发现并修复设备漏洞，从而降低网络安全风险。

01 平台层面

- 海量设备状态感知、安全配置更新和主动管理不足
- 高级持续性威胁（APT）攻击风险高
- 工业应用系统安全设计缺乏

02 网络层面

- 标识解析系统存在外部非法入侵风险
- 5G与工业互联网融合带来的新安全风险
- 传统安全环境被打破，病毒、勒索软件等威胁增加

03 设备层面

- 工业控制设备安全防护薄弱，易被非法访问和控制
- 工业主机存在各种软硬件和接口漏洞
- 缺乏统一的安全标准和规范

工控网络安全现状及威胁

2023年典型工控安全事件

Typical industrial control security incidents in 2023

GhostSec 黑客组织对白俄罗斯的工业远程终端单元进行攻击 。攻击者加密了设备 TELEOFIS RTU968 V2上的文件，并且将加密文件后缀修改为.fuckPutin。该设备可以被视为远程终端单元(RTU)。此次攻击活动使得受害设备上的文件均被加密

GE Digital 的服务器被发现存在 5 个可利用的漏洞。威胁行为者可以利用安全漏洞访问历史记录、使设备崩溃或远程执行代码。这些漏洞的存在与 ICS 和操作技术(OT)环境有关，从而为攻击者从IT网络跳转到OT系统创造了一个有吸引力的支点。

2023年2月3日，半导体设备制造商MKSIn-struments遭受勒索软件的攻击。该事件影响了某些业务系统，包括与生产相关的系统，，作为遏制措施的一部分，公司已决定暂时停止某些设施的运营。

2023 年 3 月 17 日，加密 ATM 制造商 General Bytes 发生了一起安全事件，导致至少 150 万美元被盗，迫使其关闭大部分位于美国的自动取款机，General Bytes 将其描述为"最高"级别的违规行为。

2023年5月7日，据美国网络安全媒体 BLEEPINGCOMPUTER 报道，电力和自动化技术巨头 ABB 遭受了 BlackBasta 勒索软件团伙发起的网络攻击。勒索软件攻击影响了公司的 Windows-Active-Directory，影响了数百台设备的正常工作

2023年6月25日，加拿大最大的合成原油生产商之一的SuncorEnergy遭受了网络攻击，其子公司Petro-Canada遍布加拿大的加油站已经无法支持客户使用信用卡或奖励积分付款，甚至其官网的账户登录也已经瘫痪

02 双评合规概述

SECURITY PROTECTION AND COMMERCIAL CIPHER ASSESSMENT COMPLIANCE

- 国内相关法律
- 双评合规定义
- 等保测评合规
- 商用密码应用安全评估合规

“双评合规”概述

2017年6月1日起实施《中华人民共和国网络安全法》

保障网络安全，维护网络空间主权和国家安全

《网络安全法》为网络空间的安全稳定提供坚实的法律保障，维护国家安全、社会公共利益和公民个人权益。

网络安全等级保护制度

- 第二十一条　　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行网络安全保护义务，
- 制定内部安全管理制度和操作规程
- 采取防范计算机病毒和网络攻击的技术措施
- 监测、记录网络运行状态、网络安全事件
- 采取数据分类、备份和加密措施

关键信息基础设施保护

- 《网络安全法》还特别强调了对关键信息基础设施的保护，要求其运营者需采取更加严格的安全保护措施，并明确指出关键信息基础设施的设计、建设、运营应当同步规划、同步建设、同步使用安全技术和管理措施。

- 根据《网络安全法》，网络运营者应履行的安全保护义务包括但不限于：保障网络免受干扰、破坏或未经授权的访问；采取必要措施防止网络数据泄露、丢失、篡改、毁损；制定并实施内部安全管理制度和操作规程；采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；定期开展网络安全风险评估和应急演练等。

“双评合规”概述

2020年1月1日起实施《中华人民共和国密码法》

维护国家密码安全　　提升密码工作法治化水平

是首部关于密码领域的综合性、基础性法律，旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。

密码分类管理

核心密码、普通密码

属于国家秘密

用于保护国家秘密信息

商用密码

不属于国家秘密

公民、法人和其他组织可以依法使用商用密码保护网络与信息安全

密码法规定

- 国家加强核心密码、普通密码的科学规划、管理和使用，加强制度建设，完善管理措施，增强密码安全保障能力。
- 国家鼓励商用密码技术的研究开发学术交流、成果转化和推广应用，健全统一、开放、竞争、有序的商用密码市场体系，鼓励和促进商用密码产业发展。
- 国家加强密码人才培养和队伍建设对在密码工作中作出突出贡献的组织和个人，按照国家有关规定给予表彰和奖励。

对密评的要求

- 运营者责任：关键信息基础设施的运营者必须使用密码进行保护，这是其法定责任和义务。运营者需要自行或者委托密码检测机构来开展密码应用的安全性评估。
- 密码应用安全：要求运营者使用密码对关键信息基础设施进行保护，确保其安全性。这包括使用符合标准的密码算法、密钥管理系统等。
- 评估要求：网络在通过评估后，才能上线运行。评估过程中，需要对密码应用的安全性进行严格的检测和评估，确保其符合国家相关标准和规定。
- 定期评估：投入运行后，每年至少需要组织一次评估，以检查密码应用的安全性是否持续有效，是否能够抵御新的安全威胁和攻击。
- 密码检测机构：运营者可以委托专业的密码检测机构进行密码应用安全性评估。这些机构需要具备相应的资质和能力，能够按照国家标准和规范进行检测和评估。
- 法律责任：如果运营者未按照要求进行密码应用安全性评估，或者评估结果不符合国家标准和规定，将承担相应的法律责任。

“双评合规”概述

双评合规

指的是等保测评（信息安全等级保护测评）和商用密码应用安全评估这两项关键评估工作。它们共同构成了信息安全防护的双重保险，为国家和企业的数据安全提供了坚实的保障。“双评合规”则是指通过一次入场，同时开展等保测评和商用密码应用安全评估，并成功通过两项测评的过程。

法律要求

- 2017年《中华人民共和国网络安全法》开始正式施行，网络安全等级测评工作也在全国范围内按照相关法律法规和技术标准要求全面落实实施。
- 2020年1月《中华人民共和国密码法》开始正式施行，商用密码应用安全性评估也在有序推广和逐步推进。
- 网络安全等级测评和密码应用安全性评估已经成为我国网络运营者必须依法开展的两项合规测评活动。

双评合规价值

- 提升测评机构的工作效率，减少单个运营者接受多次测评的时间成本；
- 减少因重复测评产生的经济负担，使得网络运营者能够更集中地投入到实质性的安全建设中；

法律衔接

- 《密码法》第二十七条明确提出，商用密码应用安全性评估应当与关键信息基础设施的安全检测评估及网络安全等级测评紧密衔接，避免出现不必要的重复测评现象。

同步双评

- 同期，双项安全综合测评。整合测评机构资源，实现在同一时间段内对网络运营者的网络安全等级和商用密码应用安全性进行综合测评。

“双评合规”概述

等保测评合规

概述

① 等级保护对象是指网络安全等级保护工作中的对象，主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网、工业控制系统和采用移动互联技术的系统等。

安全保护能力等级

① 第一级：防护个人及小规模威胁，受损后恢复部分功能。

② 第二级：防御小型组织攻击，发现安全漏洞并及时处置，能在一定时间恢复部分功能。

③ 第三级：对抗有组织团体和严重灾害，在统一策略下快速检测并处理安全事件，受损后快速恢复大部分功能。

④ 第四级：国家级别敌对组织攻击防护，实时监测、迅速响应，遭受损害后能迅速全面恢复所有功能。

安全技术要求

① 安全物理环境
② 安全通信网络
③ 安全区域边界
④ 安全计算环境
⑤ 安全管理中心

安全管理要求

① 安全管理制度
② 安全管理机构
③ 安全管理人员
④ 安全建设管理
⑤ 安全运维管理

安全扩展要求

① 云计算
② 移动互联网
③ 物联网
④ 工业控制系统

整体能力要求

构建纵深的防御体系，采取互补的安全措施，保证一致的安全强度
建立统一的支撑平台，进行集中的安全管理

测评结论

优　良　中　差

“双评合规”概述

商用密码应用安全评估合规

通则

信息系统各密码应用等级的测评指标以“应”“宜”“可”方式进行描述

- 应 对于“应”的条款，密评人员应按照第 6 章和第 7 章中相应的测评指标要求进行测评和结果判定。
- 宜 对于“宜”的条款，密评人员应确认信息系统是否具有已通过评估的密码应用方案。
- 可 对于“可”的条款,由信息系统责任方自行决定是否纳入测评和结果判定范围

通用测评要求

① 密码算法
② 密码技术
③ 密码产品
④ 密码服务
⑤ 密钥管理

技术测评要求

① 物理和环境安全
② 网络和通信安全
③ 设备和计算安全
④ 应用和数据安全

管理测评要求

① 管理制度
② 人员管理
③ 建设运行
④ 应急处置

整体测评要求

① 概述
- 整体测评应从单元间、层面间等方面进行测评和综合安全分析。整体测评包括单元间测评和层面间测评。

② 单元间测评
- 单元测评后，分析不符合项和部分符合项对其他单元的影响。判断这些问题是否降低了系统整体安全性。

③ 层面间测评
- 在单元测评完成后，应进行层面间测评，重点分析信息系统是否存在不同层面单元间的相互弥补作用。

风险分析和评价

评估报告应对单元测评结果进行风险分析，评价密码应用的安全问题，并判定高风险。明显不符和存在风险的情形应根据业务场景判定高风险。

测评结论

符合　基本符合　不符合

03 双评合规在工控网络安全实施的意义

THE SIGNIFICANCE OF DUAL EVALUATION COMPLIANCE IN THE IMPLEMENTATION OF INDUSTRIAL CONTROL NETWORK SECURITY

- 双评合规对工控安全的意义
- 双评一致性与差异性分析
- 双评实施的意义