工业控制系统网络安全咨询与服务白皮书

（标准版）

北京夏石科技有限责任公司

2019 年 5 月

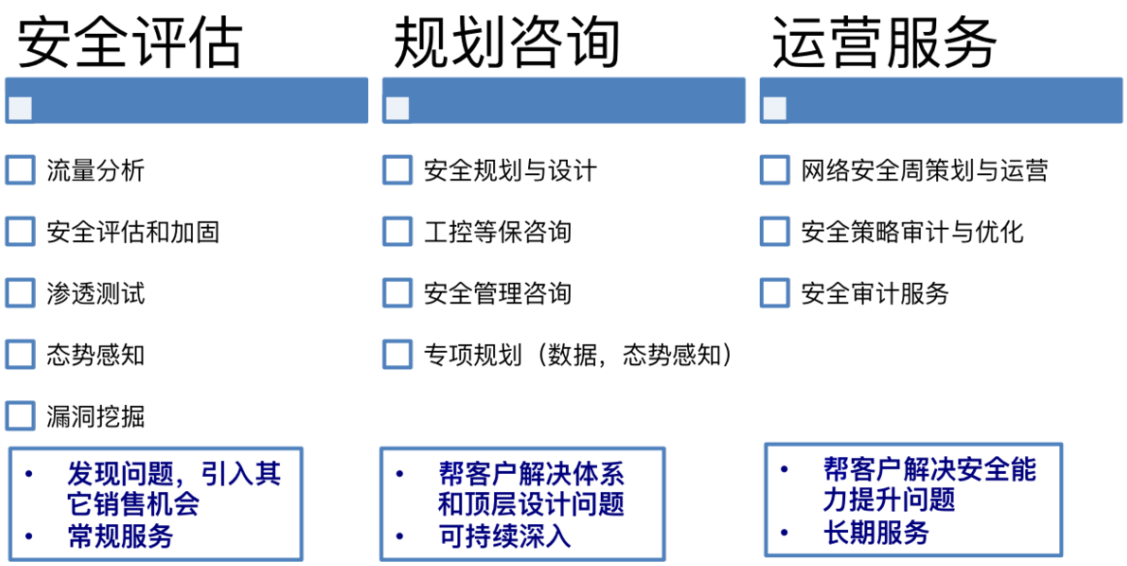
目 录

1. 背景介绍

一方面，随着用工成本的大幅提升，大量的制造行业开始撤离中国；另一方面，中国制造 2025 的逐渐落实使得更多的中国企业的生产线逐渐与数字化、网络化和智能化靠近，封闭的生产控制网络也逐渐变的开放——两化深度融合。而在此过程中，网络安全问题随之而来，“震网病毒”、“乌克兰电网事件”以及最近以“Mirai”为代表的物联网安全事件均已表明网络攻击可以影响现实世界，导致企业发生产安全生产故，而这些生产企业可能涉及能源、交通、水利、公共服务等关乎国计民生的关键信息基础设施。相应的，国家外保障关键信息基础设施的安全发布了《国家网络安全法》，而相应的监管部门也相继发布了各种工业控制系统信息安全监管要求，企业在转型升级过程中面临者巨大的安全风险以及监管压力，企业需要认真考虑如何弥补自身的薄弱项——工控安全问题——从前甚少考虑或几乎没有考虑的问题。

2. 咨询业务介绍

2.1. 服务目录

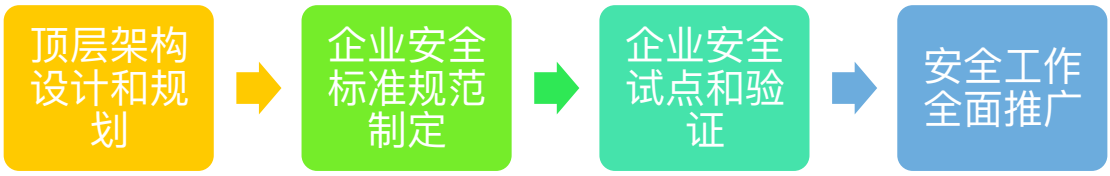


2.2. 总体路径

企业自身可以根据企业网络安全防护水平来选择合适的方式开展工控安全项目，特别是大型企业，主要有两种：

(1) 自上而下实施：

以某集团科技信息技术部门作为牵头单位，自上而下在全集团层面进行推广。



a) 开展顶层设计工作：前期进行现状摸底并进行架构设计和和 3-5 年的蓝图规划，开始相应的安全意识宣贯工作；

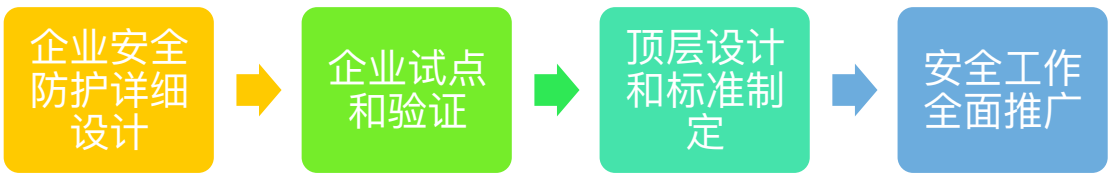
b) 制定企业安全标准和规范：制定具体的安全标准和规范用于指导安全工作的实施；

c) 试点建设工作：选择代表性企业进行试点，制定企业的安全标准和规范并不断验证；

d) 全面推广工作：在集团范围或业界开展全面推广工作。

(2) 自下而上实施；

以某集团从一线生产企业为起点，积累相应的技术经验，并逐步向全集团推广：



a) 试点方案建设：针对一线生产企业进行详细安全防护设计，并评价方案的合理性；

b) 试点建设工作：根据前期的方案设计企业开始产品选型和部署实施，并评价实施的效果；

c) 顶层设计工作：开展顶层设计工作和标准规范制定工作，用于指导全集团的推广。

d) 全面推广工作：在集团范围或业界开展全面推广工作。

无论采取哪种方式，对于集团的生产业务部门、安全部门以及科技部门而言，应遵循“统筹规划、分步实施”原则。

2.3. 服务特点

(1) 咨询方案落地性强：夏石科技积攒了大量行业实践经验，为客户带来了不同行业的先进经验和理念，并在充分了解客户安全现状的基础上，结合客户的业务特点开展各项工控安全工作，而强大安全服务团队以及雄厚的技术实力保证工控安全工作的可落地性。

(2) 灵活多变的服务方式：采用专家顾问以及服务项目的方式开展各类安全工作。

a) 咨询项目：企业在基于未来发展的考虑并在资金相对充足的情况下，通过项目的方式为企业实际状况进行把脉，并通过“望闻问切”（现场调研、访谈、技术评估、渗透测试、文档调阅等）的方式开出良方来解决客户的实际问题（未来 3-5 年的规划、试点推广工作、安全运营问题、人员培养以及实验室规划等问题），并每年持续投入将规划逐步落实。

b) 专家顾问：企业在基于自身发展的考虑并在资金相对有限的情况下，通过雇佣合适的专家顾问的方式来帮助企业设计和规划工控安全体系，专家顾问可以为企业在关键节点（如技术选型、方案设计以及可研论证等）

献言献策，并提供合适的方法和工具来支撑企业规划和建设工控安全体系。

3. 重点咨询服务介绍

咨询服务总体价值：

1. 把脉企业当前安全工作开展的重点和切入点；
2. 为企业规划工控安全体系建设目标、建设路径和所需资源；
3. 帮助客户打造企业内部安全品牌！

3.1. 工控安全防护体系规划与设计咨询

3.1.1. 目标群体

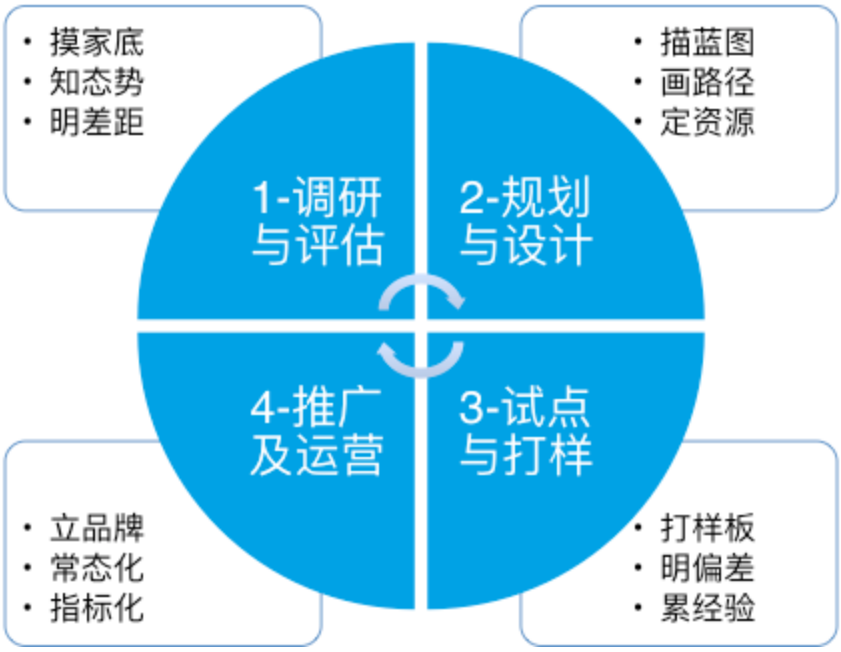
大中型工业企业，比如电力、石油石化、烟草、智能制造、城市燃气、数字矿山各类涉及国计民生的工业生产、制造业务的信息化管理部门（或者网络安全管理部门）、生产管理部门。

3.1.2. 客户价值

《网络安全法》及行业安全监管要求不断加强，以及不断增高的工业网络安全风险，你是否碰到以下困惑：

1. 工控安全工作千头万绪，安全建设项目应如何开始？
2. 信息化管理部门与生产部门在工控安全的责任边界该如何划分？
3. 工控安全的建设怎样做才不会影响到生产业务？

3.1.3. 服务过程与内容



现状调研与安全评估

1. 摸家底：全面的信息资产清点和梳理；
2. 知态势：全面评估当前网络安全态势和安全风险状况；
3. 明差距：对标国家和行业法律和标准要求，明确控制差距；

防护体系规划与设计

1. 描蓝图：明确企业未来1-3年安全规划总体目标；
2. 画路径：明确建安全能力成长、体系建设路径以及对应阶段目标；
3. 定资源：确定各建设阶段所需人力和财务预算；

试点与经验积累

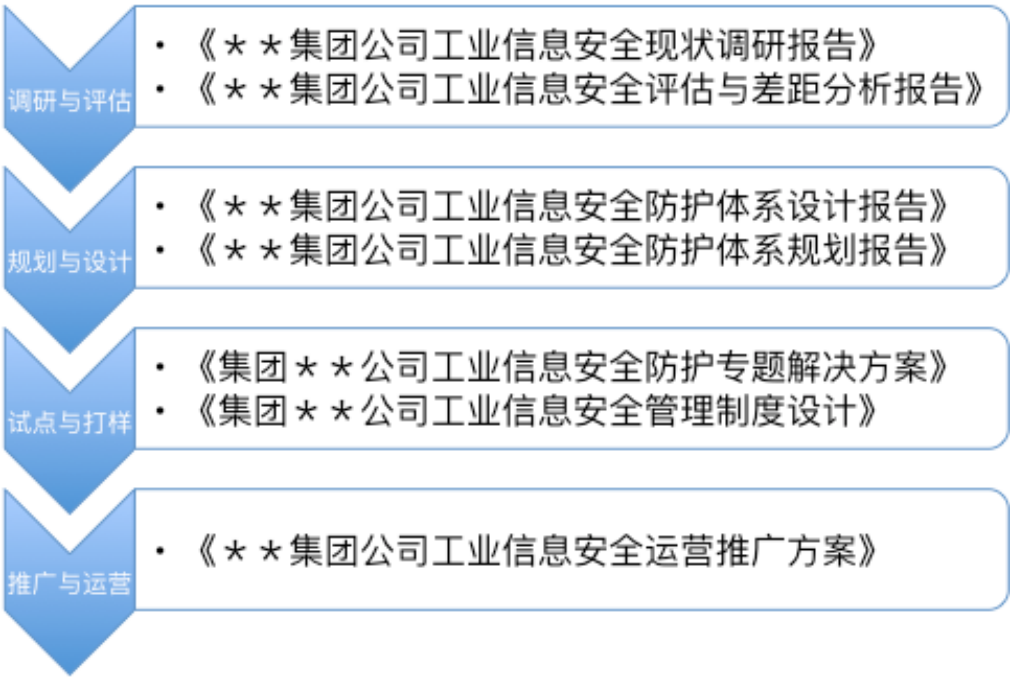
1. 打样板：小范围先试点，验证方案可落地和可执行性；
2. 明偏差：明确安全方案在生产控制环境中的特征性需求；
3. 累经验：信息化团队积累在与生产团队协调配合工控安全事务的经验；

运营推广和持续完善

1. 立品牌：通过持续运营推广，在企业内部建立和维护安全部门的品牌；
2. 常态化：持续监控－防护－应急响应－持续优化
3. 指标化：关键安全绩效指标化和数量化，客观衡量安全工作的持续改进；

3.1.4. 服务交付物

服务的最终交付以知识传递（培训、报告、方案等）为主，帮助具有不同企业文化的客户解决在不同阶段的工控安全建设问题。



3.2. 网络安全周策划与运营

3.2.1. 目标群体

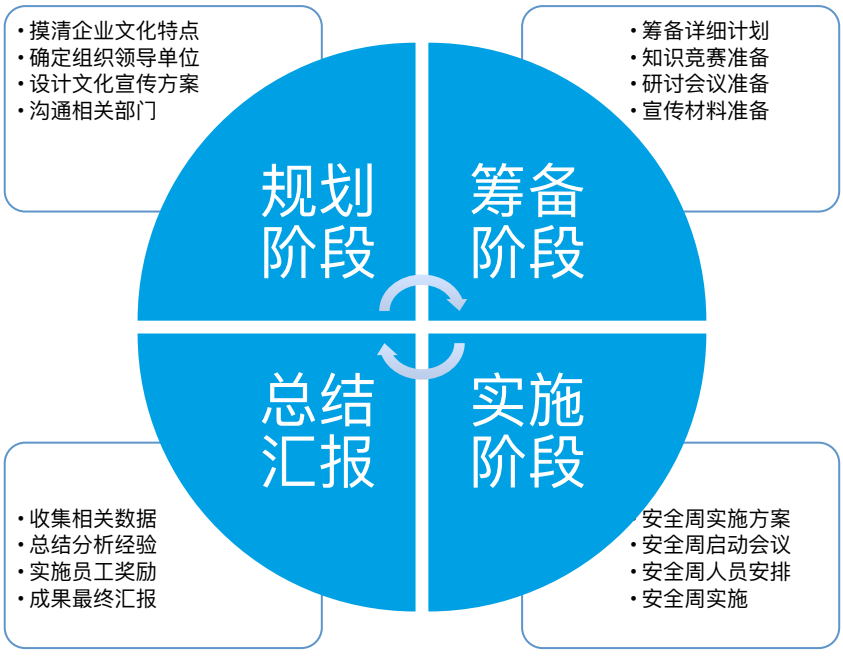
大中型工业企业，比如电力、石油石化、烟草、智能制造、城市燃气、数字矿山各类涉及国计民生的工业生产、制造业务的信息化管理部门（或者网络安全管理部门）。

3.2.2. 客户价值

网络安全不仅仅是企业安全团队的事情，同时需要各级领导的支持和员工的配合，在工作开展时，你是否有以下难题：

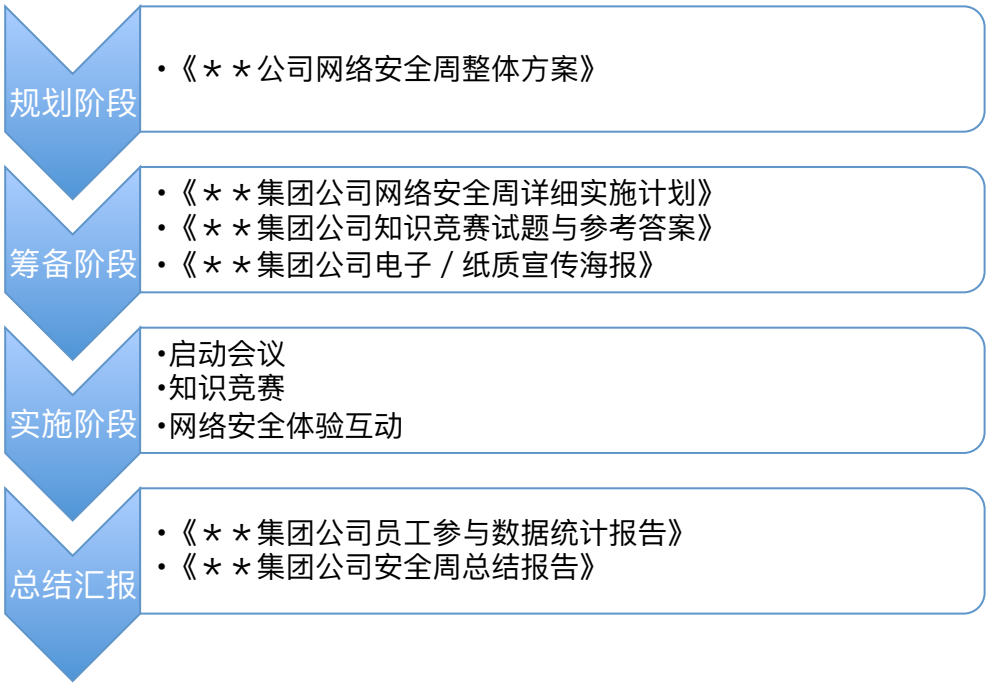
1. 安全团队时常面临团队小，预算少但压力大、责任大的不对称困境；
2. 安全团队协调内部其他部门或者分子公司工作时时常处处受限；
3. 各级领导对网络安全都是说起来重要，做起来次要，忙起来不要的尴尬；

3.2.3. 服务过程与内容



3.2.4. 服务交付物

网络安全周可以依据企业信息管理部门／安全管理部门所掌握的资源，因地制宜，网络安全周可以作为企业安全运营年度工作的例行工作来推动，逐年开展。



3.3. 工控安全风险评估服务

3.3.1. 目标群体

军工、电力、石油、煤炭、核工业、机械制造、电子、纺织、化工、冶金、智慧城市、轨道交通等领域与工业自动化控制生产相关的所有客户。

3.3.2. 客户价值

风险评估帮助企业客户解决以下问题：

1. 梳理工控系统信息存在的网络安全攻击面；
2. 厘清工控系统日常安全活动与国际标准、国家标准、行业监管要求、行业最佳实践等要求之间的差距；
3. 以发现的安全问题为抓手，请为后续的工作改善提供支撑依据；

3.3.3. 服务内容

采用管理和技术相结合的评估手段针对工控系统展开全方位的风险评估，管理风险评估包含工控系统资产风险评估和合规风险评估两种方式，技术风险评估包含流量分析评估和漏洞分析评估。

评估与检测是通过专业的服务帮助工控企业及科研机构认识、研究工业控制网络的脆弱性及安全威胁，为安全防护提供依据及指导。

3.3.4. 服务交付物

核心交付成果：

(1) 《工控系统信息安全风险评估报告》

(2) 《工控系统信息安全风险整改方案》

4. 人才培养

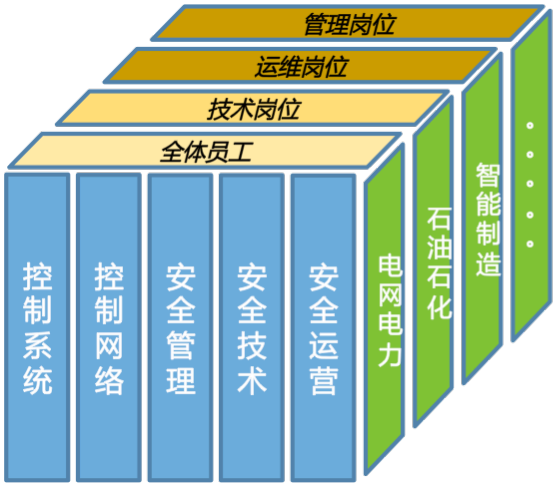
4.1. 服务价值

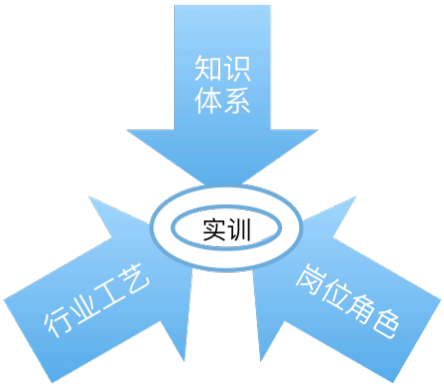
1. 为企业规划工控安全人才体系和培训矩阵；
2. 以工控安全靶场为依托，强调管理与技术，理论和实操相结合的培养方式；
3. 讲授安全思维，授人以鱼不如授人以渔！

4.2. 课程体系

课程体系具有以下特点：

1. 全面立体的工控安全课程体系；
2. 基础知识、岗位角色以及行业特点相结合三维课程矩阵；
3. 以工控安全靶场为实训托底；

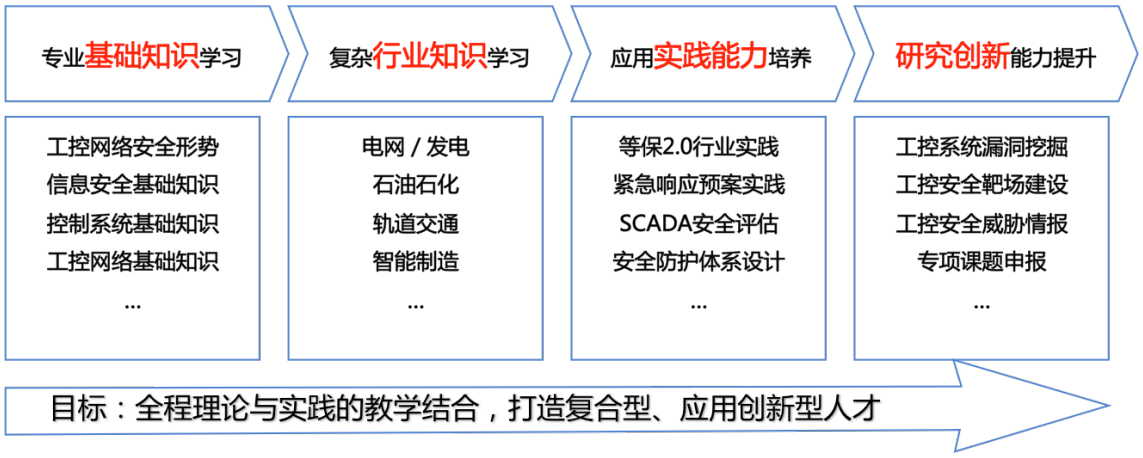




4.3. 人才发展路径

工控安全特别要求即懂工业控制系统又网络安全的复合人才，因此工控安全人才的培养和发展遵循一定的阶段规律：

1. 第一阶段：控制系统与网络安全基础知识融合的基础阶段；
2. 第二阶段：工控安全基础知识与工业行业通用和特定安全需求的融合阶段；
3. 第三阶段：专业岗位上的特殊技能在行业基础上的发展阶段；
4. 第四阶段：工控安全专深领域的突破阶段；



4.4. CISSP 认证安全思维班

4.4.1. 课程介绍

CISSP（Certified Information Systems Security Professional，国际注册信息系统安全认证专家）是目前世界上最权威、最全面的国际化信息系统安全方面的认证，由国际信息系统安全认证协会(ISC)²组织和管理，(ISC)²在全世界各地举办考试，符合考试资格的人员在通过考试后被授予 CISSP 认证证书。CISSP 可以证明证书持有者具备了符合国际标准要求的信息安全知识水平和经验能力，提升其专业可信度，

并为企业和组织提供寻找专业人员的凭证依据，目前已经得到了全世界广泛的认可。取得 CISSP 认证，表明持有者拥有完善的信息安全知识体系和丰富的行业经验，以卓越的能力服务于各大 IT 相关企业及电信、金融、大型制造业、服务业等行业，CISSP 的工作能力值得信赖。

正在从事或即将从事工业互联网安全管理的人士，你需要一张 CISSP 认证。

4.4.2. 课程的独特价值

1. 授人以鱼不如授人以渔：我们讲授安全思维模式，一通百通，让你更系统、更立体的看待企业网络安全问题；
2. 更轻松的备考：8个知识域被若干安全思维编织成知识串和知识网，克服CISSP知识点多而散的难点，同时把习题按照思维模型划分为若干类别，帮助学员更好的把握解题思路；

2.1. 工控安全入门与实践提高班

2.1.1. 培训对象

自动化从业背景人员（1-10 年工作经验）

传统网络安全或系统运维背景（1-5 年工作经验）

2.1.2. 培训目标

入门工控安全，进入工控安全相关岗位能够快速上手。

达到用人单位招聘基本需求，并推荐工作，入职工控安全行业公司，薪水提升 30-40%。

2.1.3. 培训特点

强调基本理论和实践(工控安全靶场实训)相结合。

注重安全思维方法的讲授和专门练习。

课程详情:

http://www.xiashisec.com/blog/ocd77614b74

3. 典型案例

3.1. 某能源集团工控安全体系规划项目

央企工控安全防护体系咨询第一单

(1) 概述:某能源集团作为作为国内综合能源生产企业领导者,两化融合对于集团的生产运营效率的提升起到很大的帮助,同时面临生产监控系统网络攻击面增大的风险;

(2) 实施范围:覆盖全集团煤矿、电力、煤化工等大板块共 154 家单位;

(3) 涉及部门:信息管理部(牵头)、安监部门,各业务板块主管部门等;

(4) 具体需求:集团的工控系统到底有哪些?存在什么样的问题?这些问题如何解决?由谁来解决?

(5) 隐含需求:在"两化深度融合"过程中,信息口对于生产口缺乏有效的"抓手"

3.2. 某燃气集团安全体系建设与运营项目

大型地方国企安全防护体系持续建设运营项目

⑴ 概述：自 2012 年信息安全架构并信息安全规划以来，在企业初步建立了安全治理、风控以及合规审计机制，安全运营机制逐步提升，企业网络安全文化深入基层单位，行业影响力也逐步扩大；

⑵ 涉及部门：技术信息部、信息中心、运营调度中心等

⑶ 具体需求：网络安全规划落地并持续运行；

⑷ 隐含需求：网络安全成为信息化对外的窗口和抓手

3.3. 某央企粮食集团工控安全工作管理方案

央企食品加工集团企业如何开始工控安全建设项目

⑴ 背景：集团 2009 年的信息安全规划随着信息安全技术和安全态势的不断发展，已不能满足集团现有信息化发展的需求，重新作了整体规划，并将明确集团工控安全工作方案，确定相关方职责以及后续动作。

⑵ 涉及部门：信息中心、集团下属各专业化公司

⑶ 具体需求：了解各专业化公司工控安全现状；

⑷ 隐含需求：工控安全工作抓手在哪，工作如何推进

3.4. 某燃气集团网络安全周策划与运营项目

大型地方国企安全防护体系持续建设运营项目

⑴ 早于国家网络安全周，于 2013 年开办了第一届集团网络安全周，公司内普及性宣传，参与人次：2500+；

⑵ 2014-2016 年，筹划创办内部网络安全知识竞赛，打造线上宣传平台，参与人次 9000+；

⑶ 2017 年，扩散式宣传，参与单位 30+，参与人次 35000+；

⑷ 2018 年，体验式宣传，主办行业论坛、联合竞赛、攻防演练、安全拼图、交互平台、人脸识别等，内容丰富多彩，集团安全团队影响力持续扩大；

4. 联系我们

联系电话：010-84783641

地址：北京市朝阳区望京西园 221 号博泰大厦 10 层