ICS 工业控制系统安全风险分析

金山网络企业安全事业部 张帅

本文将从 IT 领域熟悉的信息安全管理体系的基本理论和潜在威胁的角度，借鉴国际上有关工业控制系统安全保护要求及标准，分析当前我国工业控制系统存在的风险，并提出一套基于 ICS 系统的威胁发现与识别模型。

目录

11 月 12 日，待测伊朗弹道导弹收到控制指令后突然爆炸。事故经媒体披露，迅速引发各国政府与安全机构的广泛关注，对真凶的质疑直指曾攻击布什尔核电站工业控制系统的 Stuxnet 蠕虫病毒。截至目前，事故真相与细节并未公布，但工业控制系统长期存在的风险隐患却已是影响国家关键基础设施稳定运行重要因素，甚至威胁到国家安全战略实施。为此工信部于 10 月份发布文件，要求加强国家主要工业领域基础设施控制系统与 SCADA 系统的安全保护工作。

本文将从 IT 领域熟悉的信息安全管理体系的基本理论和潜在威胁的角度，借鉴国际上有关工业控制系统安全保护要求及标准，分析当前我国工业控制系统存在的风险，并提出一套基于 ICS 系统的威胁发现与识别模型。

一、 工业控制系统介绍

工业控制系统（Industrial Control Systems, ICS），是由各种自动化控制组件以及对实时数据进行采集、监测的过程控制组件，共同构成的确保工业基础设施自动化运行、过程控制与监控的业务流程管控系统。其核心组件包括数据采集与监控系统（SCADA）、分布式控制系统（DCS）、可编程逻辑控制器（PLC）、远程终端（RTU）、智能电子设备（IED），以及确保各组件通信的接口技术。

目前工业控制系统广泛的应用于我国电力、水利、污水处理、石油天然气、化工、交通运输、制药以及大型制造行业，其中超过 80%的涉及国计民生的关键基础设施依靠工业控制系统来实现自动化作业，工业控制系统已是国家安全战略的重要组成部分。

一次典型的 ICS 控制过程通常由控制回路、HMI、远程诊断与维护工具三部分组件共同完成，控制回路用以控制逻辑运算，HMI 执行信息交互，远程诊断与维护工具确保出现异常的操作时进行诊断和恢复。

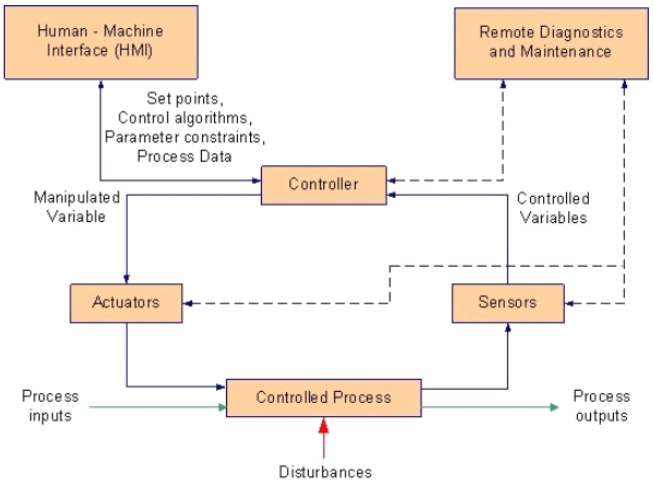

图 1：典型的 ICS 操作过程

SCADA（Supervisory Control And Data Acquisition）**数据采集与监控系统**，是工业控制系统的重要组件，通过与数据传输系统和 HMI 交互，SCADA 可以对现场的运行设备进行实时监视和控制，以实现数据采集、设备控制、测量、参数调节以及各类信号报警等各项功能。目前，SCADA 广泛应用于水利、电力、石油化工、电气化、铁路等分布式工业控制系统中。

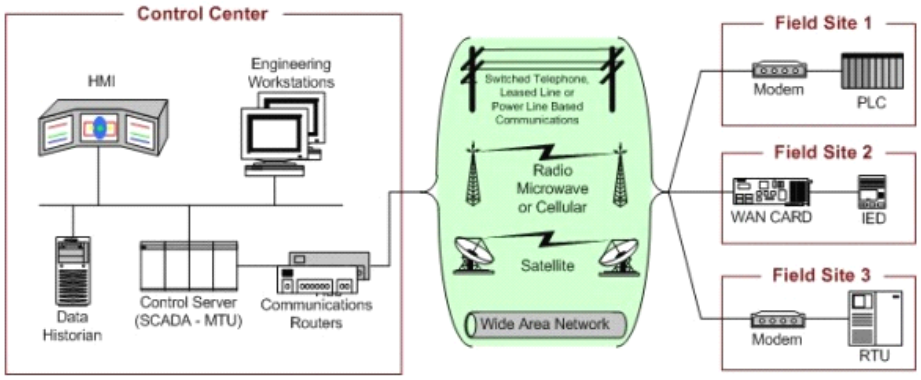

图 2：SCADA 系统总体布局

DCS（Distributed Control Systems）**分布式控制系统**，广泛应用于基于流程控制的行业，例如电力、石化等行业分布式作业，实现对各个子系统运行过程的整理管控。

PLC（Programmable Logic Controllers）**可编程逻辑控制器**，用以实现工业设备的具体操作与工艺控制。通常 SCADA 或 DCS 系统通过调用各 PLC 组件来为其分布式业务提供基本的操作控制，例如汽车制造流水线等。

二、 工业控制系统安全现状

与传统的信息系统安全需求不同，ICS 系统设计需要兼顾应用场景与控制管理等多方面因素，以优先确保系统的高可用性和业务连续性。在这种设计理念的影响下，缺乏有效的工业安全防御和数据通信保密措施是很多工业控制系统所面临的通病。

据权威工业安全事件信息库 RISI（Repository of Security Incidents）统计，截止 2011 年 10 月，全球已发生 200 余起针对工业控制系统的攻击事件。2001 年后，通用开发标准与互联网技术的广泛使用，使得针对 ICS 系统的攻击行为出现大幅度增长，ICS 系统对于信息安全管理的需求变得更加迫切。

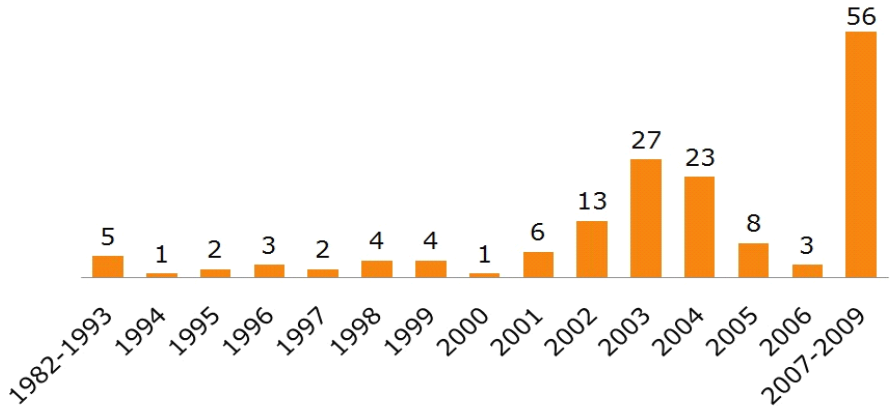

图 3：1982-2009 工业系统攻击事件

纵观我国工业控制系统的整体现状，西门子、洛克韦尔、IGSS 等国际知名厂商生产的工控设备占据主动地位，由于缺乏核心知识产权和相关行业管理实施标准，在愈发智能开放的 ICS 系统架构与参差不齐的网络运维现实前，存储于控制系统、数据采集与监控系统、现场总线以及相关联的 ERP、CRM、SCM 系统中的核心数据、控制指令、机密信息随时可能被攻击者窃取或篡改破坏。作为一项复杂而繁琐的系统工程，保障工业系统的信息安全除了需要涉及工业自动化过程中所涉及到的产品、技术、操作系统、网络架构等因素，企业自身的管理水平更直接决定了 ICS 系统的整体运维效果。遗憾的是当前我国网络运维现实，决定了国内 ICS 系统的安全运维效果并不理想，安全风险存在于管理、配置、架构的各个环节。

借鉴 IT 安全领域 ISO27001 信息安全管理体系和风险控制的成功经验，综合工业控制网络特点以及工业环境业务类型、组织职能、位置、资产、技术等客观因素，对工业控制系统构建 ICS 信息安全管理体系，是确保工业控制系统高效稳定运行的理论依据。

三、 工业控制系统安全风险分析

1、风险分析

工业控制系统是我国重要基础设施自动化生产的基础组件，安全的重要性可见一斑，然而受到核心技术限制、系统结构复杂、缺乏安全与管理标准等诸多因素影响，运行在 ICS 系统中的数据及操作指令随时可能遭受来自敌对势力、商业间谍、网络犯罪团伙的破坏。根据工信部《关于加强工业控制系统信息安全管理的通知》要求，我国工业控制系统信息安全管理的重点领域包括核设施、钢铁、有色、化工、石油石化、电力、天然气、先进制造、水利枢纽、环境保护、铁路、城市轨道交通、民航、城市供水供气供热以及其他与国计民生紧密相关的领域。这些领域中的工业控制系统一旦遭到破坏，不仅会影响产业经济的持续发展，更会对国家安全造成巨大的损害。

典型工业控制系统入侵事件：

- 2007 年，攻击者入侵加拿大的一个水利 SCADA 控制系统，通过安装恶意软件破坏了用于取水调度的控制计算机；
- 2008 年，攻击者入侵波兰某城市的地铁系统，通过电视遥控器改变轨道扳道器，导致 4 节车厢脱轨；
- 2010 年，“网络超级武器”Stuxnet 病毒通过针对性的入侵 ICS 系统，严重威胁到伊朗布什尔核电站核反应堆的安全运营；
- 2011 年，黑客通过入侵数据采集与监控系统 SCADA，使得美国伊利诺伊州城市供水系统的供水泵遭到破坏。

分析可以发现，造成工业控制系统安全风险加剧的主要原因有两方面：

首先，传统工业控制系统的出现时间要早于互联网，它需要采用专用的硬件、软件和通信协议，设计上以武力安全为主，基本没有考虑互联互通所必须考虑的通信安全问题。

其次，互联网技术的出现，导致工业控制网络中大量采用通用 TCP/IP 技术，工业控制系统与各种业务系统的协作成为可能，愈加智能的 ICS 网络中各种应用、工控设备以及办公用 PC 系统逐渐形成一张复杂的网络拓扑。

仅基于工控协议识别与控制的安全解决方案在两方面因素的合力下，已无法满足新形势下 ICS 网络运维要求，**确保应用层安全是当前 ICS 系统稳定运营的基本前提**。利用工控设备漏洞、TCP/IP 协议缺陷、工业应用漏洞，攻击者可以针对性的构建更加隐蔽的攻击通道。以 Stuxnet 蠕虫为例，其充分利用了伊朗布什尔核电站工控网络中工业 PC 与控制系统存在

的安全漏洞（LIK 文件处理漏洞、打印机漏洞、RPC 漏洞、WinCC 漏洞、S7 项目文件漏洞以及 Autorun.inf 漏洞），为攻击者入侵提供了七条隐蔽的通道。

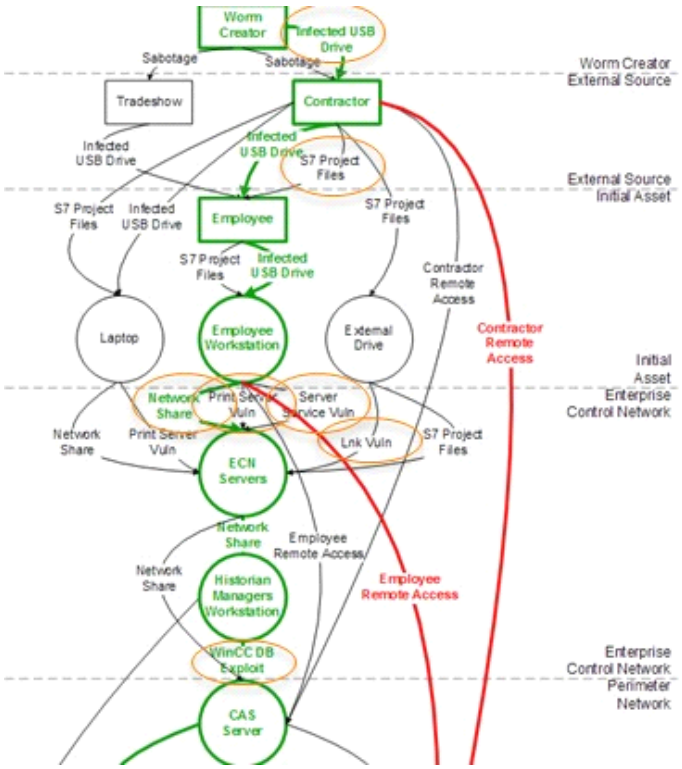

图 4：Stuxnet 蠕虫病毒传播的七条途径

2、 脆弱性分析

工业控制系统的安全性和重要性直接影响到国家战略安全实施，但为兼顾工业应用的场景和执行效率，在追求 ICS 系统高可用性和业务连续性的过程中，用户往往会被动的降低 ICS 系统的安全防御需求。识别 ICS 存在的风险与安全隐患，实施相应的安全保障策略是确保 ICS 系统稳定运行的有效手段。

- **安全策略与管理流程的脆弱性**

追求可用性而牺牲安全，这是很多工业控制系统存在普遍现象，缺乏完整有效的安全策略与管理流程是当前我国工业控制系统的最大难题，很多已经实施了安全防御措施的 ICS 网络仍然会因为管理或操作上的失误，造成 ICS 系统出现潜在的安全短板。例如，工业控制系统中的移动存储介质的使用和不严格的访问控制策略。

作为信息安全管理的重要组成部分，制定满足业务场景需求的安全策略，并依据策略制定管理流程，是确保 ICS 系统稳定运行的基础。参照 NERC CIP、ANSI/ISA-99、IEC 62443 等国际标准，目前我国安全策略与管理流程的脆弱性表现为：

- 缺乏 ICS 的安全策略；

- 缺乏 ICS 的安全培训与意识培养；
- 缺乏安全架构与设计
- 缺乏根据安全策略制定的正规、可备案的安全流程；
- 缺乏 ICS 安全审计机制；
- 缺乏针对 ICS 的业务连续性与灾难恢复计划；
- 缺乏针对 ICS 配置变更管理。

- **工控平台的脆弱性**

随着 TCP/IP 等通用协议与开发标准引入工业控制系统，开放、透明的工业控制系统同样为物联网、云计算、移动互联网等新兴技术领域开辟出广阔的想象空间。理论上绝对的物理隔离网络正因为需求和业务模式的改变而不再切实可行。

目前，多数 ICS 网络仅通过部署防火墙来保证工业网络与办公网络的相对隔离，各个工业自动化单元之间缺乏可靠的安全通信机制，例如基于 DCOM 编程规范的 OPC 接口几乎不可能使用传统的 IT 防火墙来确保其安全性。数据加密效果不佳，工业控制协议的识别能力不理想，加之缺乏行业标准规范与管理制度，工业控制系统的安全防御能力十分有限。

旨在保护电力生产与交通运输控制系统安全的国际标准 NERC CIP 明确要求，**实施安全策略确保资产安全是确保控制系统稳定运行的最基本要求**。将具有相同功能和安全要求的控制设备划分到同一区域，区域之间执行管道通信，通过控制区域间管道中的通信内容是目前工业控制领域普遍被认可的安全防御措施。

另一种容易忽略的情况是，由于不同行业的应用场景不同，其对于功能区域的划分和安全防御的要求也各不相同，而对于利用针对性通信协议与应用层协议的漏洞来传播的恶意攻击行为更是无能为力。更为严重的是工业控制系统的补丁管理效果始终无法令人满意，考虑到 ICS 补丁升级所存在的运行平台与软件版本限制，以及系统可用性与连续性的硬性要求，ICS 系统管理员绝不会轻易安装非 ICS 设备制造商指定的升级补丁。与此同时，工业系统补丁动辄半年的补丁发布周期，也让攻击者有较多的时间来利用已存在漏洞发起攻击。著名的工业自动化与控制设备提供商西门子就曾因漏洞公布不及时而饱受质疑。

据金山网络企业安全事业部统计，2010-2011 年间，已确认的针对工业控制系统攻击，从攻击代码传播到样本被检测确认，传统的安全防御机制通常需要 2 个月左右的时间，而对于例如 Stuxnet 或更隐蔽的 Duqu 病毒，其潜伏期更是长达半年之久。无论是针对工业系统的攻击事件，还是更隐蔽且持续威胁的 APT 攻击行为，基于黑名单或单一特征比对的信息安全解决方案都无法有效防御，更不要说利用 0day 漏洞的攻击行为。而 IT 领域广泛采

用的主动防御技术，因为其存在较大的误杀风险，并不适用于工业控制系统的高性能作业。目前，唯有基于白名单机制的安全监测技术是被工业控制系统用户普遍任何的解决方案。

- **网络的脆弱性**

通用以太网技术的引入让 ICS 变得智能，也让工业控制网络愈发透明、开放、互联，TCP/IP 存在的威胁同样会在工业网络中重现。此外，工业控制网络的专属控制协议更为攻击者提供了了解工业控制网络内部环境的机会。确保工业网络的安全稳定运营，必须针对 ICS 网络环境进行实时异常行为的 “发现、检测、清除、恢复、审计”一体化的保障机制。当前 ICS 网络主要的脆弱性集中体现为：

- 边界安全策略缺失；
- 系统安全防御机制缺失；
- 管理制度缺失或不完善；
- 网络配置规范缺失；
- 监控与应急响应制度缺失；
- 网络通信保障机制缺失；
- 无线网络接入认证机制缺失；
- 基础设施可用性保障机制缺失。

3、潜在威胁分析

作为国家关键基础设施自动化控制的基本组成部分，由于其承载着海量的操作数据，并可以通过篡改逻辑控制器控制指令而实现对目标控制系统的攻击，针对工业控制网络的定向攻击目前正成为敌对势力和网络犯罪集团实施渗透攫取利益的重点对象。稍有不慎就有可能对涉及国计民生的重要基础设施造成损害。可导致 ICS 系统遭受破坏的威胁主要有：

- 控制系统发生拒绝服务；
- 向控制系统注入恶意代码；
- 对可编程控制器进行非法操作；
- 对无线 AP 进行渗透；
- 工业控制系统存在漏洞；
- 错误的策略配置；
- 人员及流程控制策略缺失。

四、 工业控制系统安全管理体系

信息化与工业化深度融合的今天，无论是关乎国计民生的电力、石化、水利、铁路、民航等基础保障行业，还是逐渐成规模的物联网、移动互联网等新型行业，交互已成 ICS 系统的重要特性。互联与交互体验提升的同时，威胁也在与日俱增。

目前我国 ICS 系统的信息安全管理仍存在诸多问题，例如，大型制造行业普遍存在因设备使用时间较长，安全防护能力缺失等问题；而在诸如石化电力等重要基础设施保障行业，又因为应用和新技术的更替，海量的分布式控制组件与业务单元都让电力控制网络变得愈发复杂，在可用性面前安全防御机制难免出现疏漏。因此，在参照国际流行标准以及我国工业控制系统所存在的具体安全风险等因素，一种基于终端可用性和安全性兼顾的控制系统安全解决方案被提出，用以从威胁入侵的根源满足工业控制系统的安全需求。

基于终端的工业系统安全防御体系

工业网络中同时存在保障工业系统的工业控制网络和保障生产经营的办公网络，考虑到不同业务终端的安全性与故障容忍程度的不同，对其防御的策略和保障措施应该按照等级进行划分，实施分层次的纵深防御体系。

按照业务职能和安全需求的不同，工业网络可划分为以下几个区域：

- 满足办公终端业务需要的办公区域；
- 满足在线业务需要 DMZ 区域；
- 满足 ICS 管理与监控需要的管理区域；
- 满足自动化作业需要的控制区域。

针对不同区域间数据通信安全和整体信息化建设要求，实施工业控制网络安全建设，首先需要针对 ICS 网络管理的关键区域实施可靠的边界安全策略，实现分层级的纵深安全防御策略，抵御各种已知的攻击威胁。

图 5：工业控制系统边界防御思想

- **办公网络终端的安全防御**

办公网络相对于工业控制网络是开放，其安全防御的核心是确保各种办公业务终端的安全性和可用性，以及基于终端使用者的角色实施访问控制策略。办公网络也是最容易受到攻击者攻击并实施进一步定向攻击的桥头堡，实施有效的办公网络终端安全策略可最大限度的抵御针对 ICS 系统的破坏。办公网络通用终端安全防御能力建设包括：

- 病毒、木马等威胁系统正常运行恶意软件防御能力；
- 基于白名单的恶意行为发现与检测能力；
- 终端应用控制与审计能力；
- 基于角色的访问控制能力；
- 系统漏洞的检测与修复能力；
- 基于系统异常的恢复能力；
- 外设的管理与控制能力；
- 基于终端行为与事件的审计能力；
- 终端安全的应急响应能力。

- **工业控制网络终端的安全防御**

工业控制网络具有明显的独有特性，其安全防御的核心是确保控制系统与监控系统的可用性，以及针对 ICS 系统与管理员、ICS 系统内部自动化控制组件间的访问控制策略。同时需要确保控制系统在发生异常或安全事件时，能够在不影响系统可用性的情况下，帮助管理员快速定位安全故障点。

在确保控制系统可用性的前提下，工业控制网络终端安全防御能力建设需要做到如下几

个方面：

- 基于行业最佳实践标准的合规保证能力；
- 基于白名单策略的控制终端恶意软件防御能力；
- 基于白名单的恶意未知行为发现与检测能力；
- 基于 ICS 协议的内容监测能力；
- 基于控制系统的漏洞及威胁防御能力；
- 基于可用性的最小威胁容忍模型建设能力；
- 基于事件与行为的审计能力；
- 基于可用性的系统补丁修复能力；
- 终端安全的应急响应能。

- **工业网络终端安全管控平台建设**

充分了解控制终端与业务终端的安全能力建设规范与功能，是构建高性能安全事件审计与管理运维平台模型的前提，也是实现工业网络中对分布式控制系统、数据采集系统、监控系统的统一监控、预警和安全响应的基础平台。安全管控平台不仅是实施工业数据采集和监控内容的汇聚中心，基于 ICS 安全威胁的知识库仿真模块，更可实时对检测到的异常或未授权访问进行核查评估，并将风险通过短信、邮件等方式对管理员告警。

为确保安管平台的可用性和时效性，可基于云计算与虚拟化技术对管理平台进行建设，目前较成熟的私有云安全技术、虚拟终端管理技术、数据灾备技术，都可为 ICS 系统统一管理提供良性的技术支撑。在客户端系统资源优化方面，先进的私有云平台可将信息终端繁重的功能负载迁移到云端执行，为系统的关键应用提供宝贵的计算资源，实现工业系统调度与计算资源的最大利用。

另一方面，工业系统安全管理体系还应该具备应用行为分析与学习能力，例如对系统性能的异常检测模型、工业系统协议的内容识别模型、OPC 组件的调用规则模型、以及外设和 WIFI 的审计报警模型等。知识库和各种分析模型的建立离不开对用户工业控制系统的理解和产业攻击事件与趋势的跟踪分析研究。

只有将涉及到工业控制系统各个环境的关键运维保障风险点和最基本的运维需求规范化、流程化，才能为 ICS 系统实施可行的风险控制基线，实现以用户为核心的主动威胁防御与运维保障体系。

参照 NIST 最新发布的《工业系统安全指南》有关 ICS 系统纵深防御体系架构的建议，通过引入基于私有云技术的终端安全管理体系，实现客户端、服务端、探针对工业网络中关

键信息终端和关键应用的实时分析与审计。

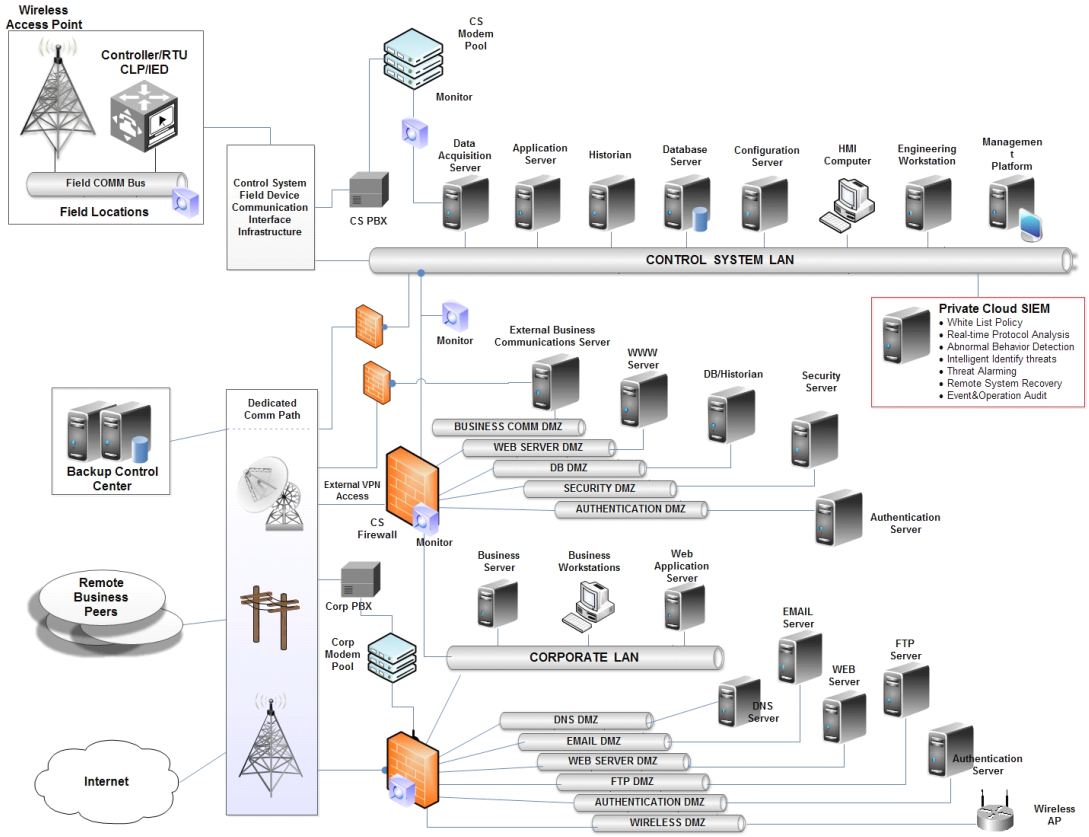

图 6：工业控制系统安全架构

一种基于私有云技术的 ICS 威胁识别模型

目前，工业控制系统风险识别模型的实现主要有两种方式：基于 ICS 网络的协议识别风险模型；基于 ICS 系统特征的仿真控制模型。其核心设计思想通常是通过识别 ICS 网络通用及专属协议内容，并根据其中包含的主从关系、访问控制、行为特征、传递途径、Exploit 方式、命令请求等信息提取非法特征，最后通过加权的方式判断威胁是否存在。

图 7：传统的风险识别

然而，更具针对性、隐蔽性的 APT 攻击行为的出现，传统 ICS 风险识别模型增加了许多不确定的因素。通过对 APT 攻击事件、工业控制系统管理需求的分析，我们可以清晰的看到，在确保 ICS 可用性的前提下，CS 组件的未公开漏洞，受信的合法控制路径，OPC 的调度组件，PLC 的过程控制，网络架构以及管理制度设计缺陷都加重了不确定的因素。

因此构建满足工业控制系统的风险识别模型，除了需要细化工业控制系统的风险因素，

还需要基于工业控制系统的安全管理域的差异，实施分等级的基线建设，兼顾终端与链路、威胁与异常、安全与可用性等综合因素的考虑同样必不可少。

模型建立：

- 全网流量收集识别能力；
- 基于白名单的终端应用控制能力；
- 实时 ICS 协议与内容识别能力；
- 异常行为的仿真能力；
- 动态基线自适应能力；
- 可视化运维能力；
- 安全事件跟踪研究能力。

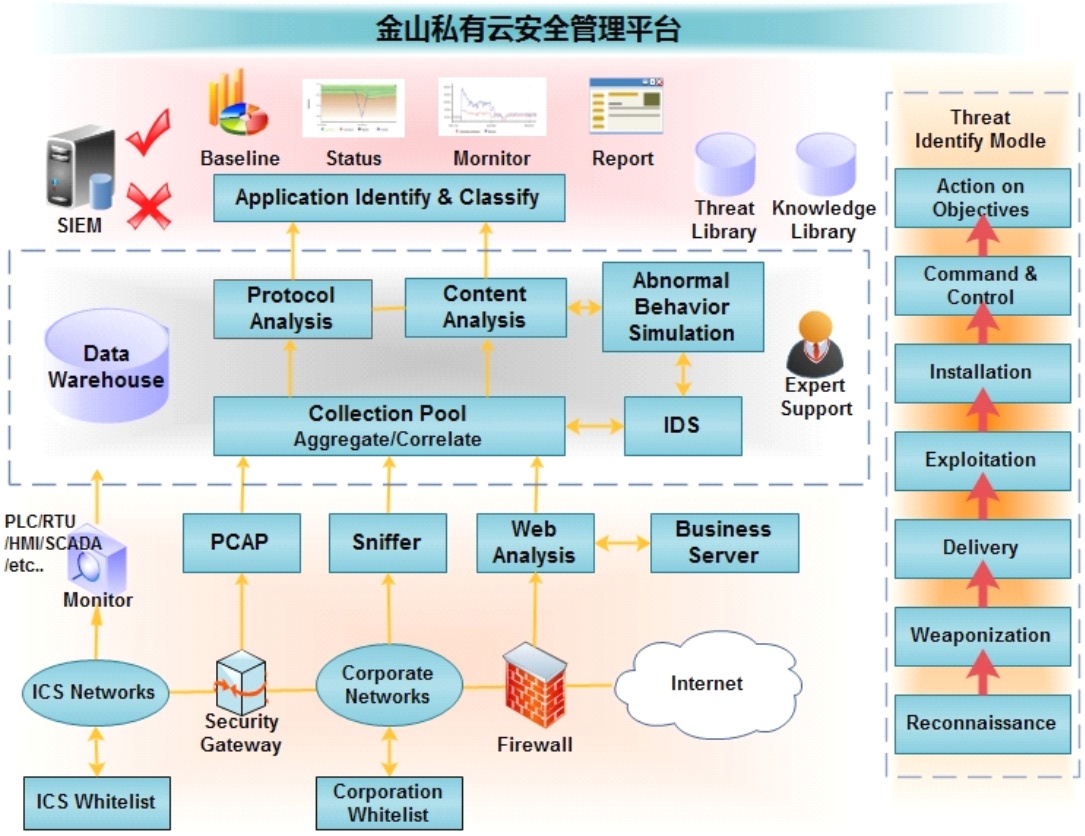

图 8：基于私有云的工业系统威胁识别模型

五、 总结

作为国家的重要基础设施，工业控制系统的的安全性对国家安全、社会利益具有重要的影响，为此工信部 10 月印发通知，要求各级政府和国有大型企业切实加强 ICS 系统的信息安全管理。而与此同时，国内重要行业 ICS 系统还普遍被《信息安全等级保护》定为第 3 或第 4 级，工业信息系统的安全管理体系建设还需兼顾等级保护技术要求。

国际方面，各国网络空间战略的进一步发展，国与国的防御战略已经从现实延伸到虚拟世界，网络空间更是各国未来发展战略中得必争之地。自从网络“超级武器”Stuxnet 蠕虫的出现，谁也无法保证本国的关键基础设施不会成为下一个攻击目标。

因此，传统的信息安全管理体系需要重新思考工业安全的重要性和防御策略，针对工业控制系统终端的特殊性以及 IT 信息安全的管理需求，构建基于终端的安全管理体系是现阶段满足不同环境信息安全管理需求的重要手段。

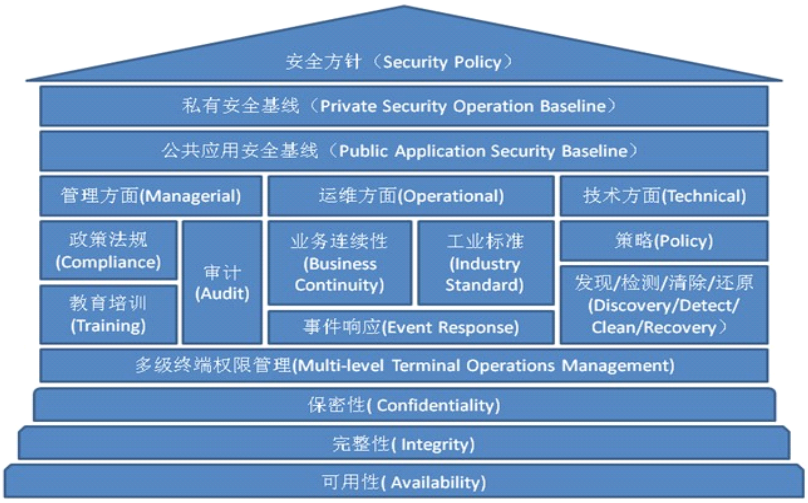

图 9：基于终端的信息安全管理体系

当然，无论是国家未来发展战略的要求，还是确保国家重要基础设施可用性的需要，从管理、流程、架构、设备、技术等多个角度，构建满足工业控制系统安全管理体系，不断改进并完善，是确保新时期工业控制系统和国家重要基础设施安全的最有效手段。

六、 附录

SCADA 网络安全建设 21 条

1. 识别所有网络链接；
2. 阻断所有不必要的网络链接；
3. 对所有网络链接进行评估并实施安全策略；
4. 删除并阻止一切不必要的服务选项；
5. 不要依赖专有协议确保 SCADA 网络安全；
6. 部署适当的安全解决方案，例如西门子 SCALANCE S，金山私有云安全系统；
7. 对工业控制系统应用实施强访问控制策略，以限制其被恶意软件利用；
8. 部署实时的旁路事件监测系统；
9. 实施基于网络连接与设备行为的审计系统，识别安全威胁；
10. 分析并评估远程接入的安全性；
11. 安排专人负责对网络安全状况进行分析并预警；
12. 明确界定管理人员的在网络运维中的角色和职责；
13. 实施额外的安全功能保护网络中的敏感功能与信息；
14. 建立严格且持续的风险管理流程；
15. 基于深度保护原则建立防御策略；
16. 全面了解行业最佳实践及网络防御要求；
17. 制定有效的配置管理流程；
18. 实施常规的自我评估机制；
19. 制定系统备份及灾难恢复计划；
20. 针对各种潜在的威胁攻击实施应急响应策略；
21. 制定员工规范和安全培训计划，将风险控制在可接受的最低范畴。

七、 参考文献

1) Keith Stouffer，Joe Falco，Karen Scarfone，Guide to Industrial Control Systems (ICS) Security，June 2011；
2) 贾东耀，汪仁煌，工业控制网络结构的发展趋势，工业仪表与自动化装置，2002 年第 5 期；
3) Eric M. Hutchins，Michael J. Clopperty，Rohan M. Amin, Ph.D.，Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains
4) Eric Byres，P.Eng.，What Does Stuxnet Mean for Industrial Control System
5) 唐文，西门子中国研究院信息安全部，工业基础设施信息安全，2011