安全加社区

公益译文项目

2016

实操建议：采取纵深防御策略，提升工控系统网络安全

美国国土安全部

2009 年 10 月

文档信息			
原文名称	Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies		
原文作者	美国国土安全部	原文发布日期	2009 年 10 月
作者简介			
原文发布单位			
原文出处			
译者	小蜜蜂公益翻译组	校对者	小蜜蜂公益翻译组

“安全加”社区　　小蜜蜂公益翻译组

目录

执行摘要 …… 1

缩略语及其定义 …… 2

1.0 概述 …… 3

1.1 背景 …… 3

1.2 现行工控系统架构概览 …… 4

2.0 工控系统内的安全挑战 …… 6

2.1 安全状况与攻击方法 …… 7

3.0 隔离与保护资产：纵深防御策略 …… 13

3.1 纵深防御战略框架 …… 13

3.2 防火墙 …… 16

3.3 创建 DMZ 域 …… 18

3.4 入侵检测系统 …… 19

3.5 指导方案与规程 …… 21

4.0 建议与措施 …… 25

4.1 工控系统的五个关键的安全措施 …… 25

5.0 延伸阅读 …… 26

免责声明

本报告项目由美国政府机构发起，美国政府、政府所属机构及其员工对于任何第三方使用本文、使用本文造成的后果以及本文所披露的信息、设备、产品或流程不作任何明示或暗示的保证，不承担任何法律责任或义务，同时并不表示第三方使用如上信息不会侵犯私有权。

执行摘要

工控系统作为关键基础设施不可分割的一部分，可简化电力、石油天然气、供水、交通及化工等重要行业部门的运营。日益增长的网络安全问题及其对工控系统的影响愈发凸显了关键基础设施所面临的重大风险。解决工控系统的网络安全问题，须对安全挑战与特定防护措施有清晰认识。全局法使用特定措施逐步增强安全，助力防护工控系统中的网络安全威胁与漏洞。这种方法一般被称为“纵深防御”，适用于工控系统，为优化网络安全防护提供了灵活、可用的框架。

人们之所以关注控制系统的网络安全问题，一方面是因为某些系统沿用传统特性，另一方面是因为工控系统联网需求日益增长。在这种关注下，大量已知漏洞被发现，同时一些工控系统领域前所未见的新型威胁也浮出水面。许多老旧系统缺乏恰当的安防能力，无法抵御新型威胁，而现行网络安全方案由于会影响到系统可用性而无法使用。工控系统连接到企业、厂商或对等网络可加剧此问题。

本文深度探讨了较突出的网络风险问题，并结合工控系统对这些问题做了进一步阐述。文章还就如何针对特定问题制定缓解策略发表了看法，并为如何在工控环境制定深度安全防护计划提供了建议，目的是为网络缓解策略的制定以及策略在工控环境中的应用提供指导。

关键词

纵深防御；工控系统；SCADA；过程控制；网络安全；防火墙；IDS；入侵检测；

加密；隔离区；DMZ；安全区；指导方案与规程；补丁管理

缩略语及其定义

ARP	Address Resolution Protocol	地址解析协议
DCOM	Distributed Common Object Model	分布式公共对象模型
DHS	U.S. Department of Homeland Security	美国国土安全部
DMZ	Demilitarized Zone	隔离区（非军事化区）
DNP	Distributed Network Protocol	分布式网络协议
FTP	File Transfer Protocol	文件传输协议
HMI	Human Machine Interface	人机界面
ICCP	Inter Control Center Communications Protocol	控制中心间通信协议
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team	工控系统网络应急响应小组
IDS	Intrusion Detection Systems	入侵检测系统
IP	Internet Protocol	互联网协议
IT	Information Technology	信息技术
LAN	Local Area Network	局域网
MitM	Man-in-the-Middle	中间人攻击
NERC	North American Electrical Reliability Corporation	北美电力可靠性公司
NIST	National Institute of Standards and Technology	国家标准与技术研究院
NSA	National Security Agency	国家安全局
OLE	Object Linking and Embedding	对象链接与嵌入
OPC	OLE for Process Control	用于过程控制的 OLE
OPSEC	Operational Security	运营安全
PLC	Programmable Logic Controller	可编程逻辑控制器
RPC	Remote Procedure Call	远程过程调用
SCADA	Supervisory Control and Data Acquisition	数据采集与监视控制系统
SIEM	Security Incident Event Management	安全事件管理
SQL	Structured Query Language	结构化查询语言
TCP	Transmission Control Protocol	传输控制协议
US-CERT	U.S. Computer Emergency Readiness Team	美国计算机紧急响应小组
VoIP	Voice-over Internet Protocol	IP 承载语音
WARDIALING	轰炸拨打	利用使用调制解调器的个人电脑重复拨打电话号码，以定位其他未广播的调制解调器，最终非法访问计算或过程控制系统域
WARDRIVING	驾驶攻击	循环搜索无线接入点，以进入通信网络，最终非法访问计算或控制系统域

1.0 概述

许多公共及私有域的信息基础设施在信息技术（IT）部署与数据通信方面具有一些共同特性，这在工控系统领域尤其如此。这个领域中，越来越多的组织使用新型组网，通过加强外部、业务与控制系统网络的融合来提高生产率，降低成本。然而，这些融合策略常会导致漏洞，极大地降低组织的网络安全状况，置关键业务工控系统于网络威胁之下。

本文为使用控制系统网络、同时维护多级信息架构的组织就制定“纵深防御”策略提供了指导。

1.1 背景

关键基础设施体系为制造、交通及能源等主要行业提供支持，极度依赖信息系统的命令与控制。一方面，关键基础设施体系对于老旧工控系统仍有极大的依赖性，另一方面，它们要进行迁移，与新兴的通信技术对接。因此，常用的通信协议与开放的架构标准正逐步替代工控系统所使用的各种不同的私有技术。这种替代有正面影响，也有负面影响。

正面影响是，技术迁移使资产所有人可以获取更为高效的新型通信方法及更为可靠的数据，促使产品更快上市，具有更好的互通性。负面影响是，控制系统用户获取最新技术能力后会引入新的风险。网络相关的漏洞与风险在工控系统独立运行时并不存在。许多事例已经表明，电力等行业的工控系统间相互依赖[1]，2003 年北美大停电事故也说明了这一点。要切实了解工控系统的安全状况，需有风险模型来更有效地反映这些复杂系统。控制系统会影响到现实世界的事物，因此，适用于工控系统的风险定义需要将后果一并考虑。更确切地说，风险可被视为漏洞与威胁和后果的因变量。

新协议与通信标准为工控系统提供了更强的互通性，但同时，也会被利用入侵互联网与企业网。从老旧架构迁移至新的操作系统和平台后，工控系统会带来许多已有的网络安全漏洞，其中一些漏洞虽有防护措施，但是一般无法部署在自动化系统中。

在图 1 的传统场景中，企业架构与控制域互相独立。架构提供数据共享、数据采集、点对点数据交换及其他业务运营方法。然而，对于任一系统，其安全均基于如下事实：控制系统局域网资源的复杂架构或运营机制几乎无人知晓。这正是所谓的“模糊即安全”。一般来说，这种方式可为无外部通信连接的环境提供有效防护，使组织可集中精力抓物理安全。

1 北美电力可靠性公司 . 关于 2003 年 8 月 14 日停电事故的技术分析，http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf，2004 年 7 月 13 日 . 网站上次访问时间为 2009 年 10 月。

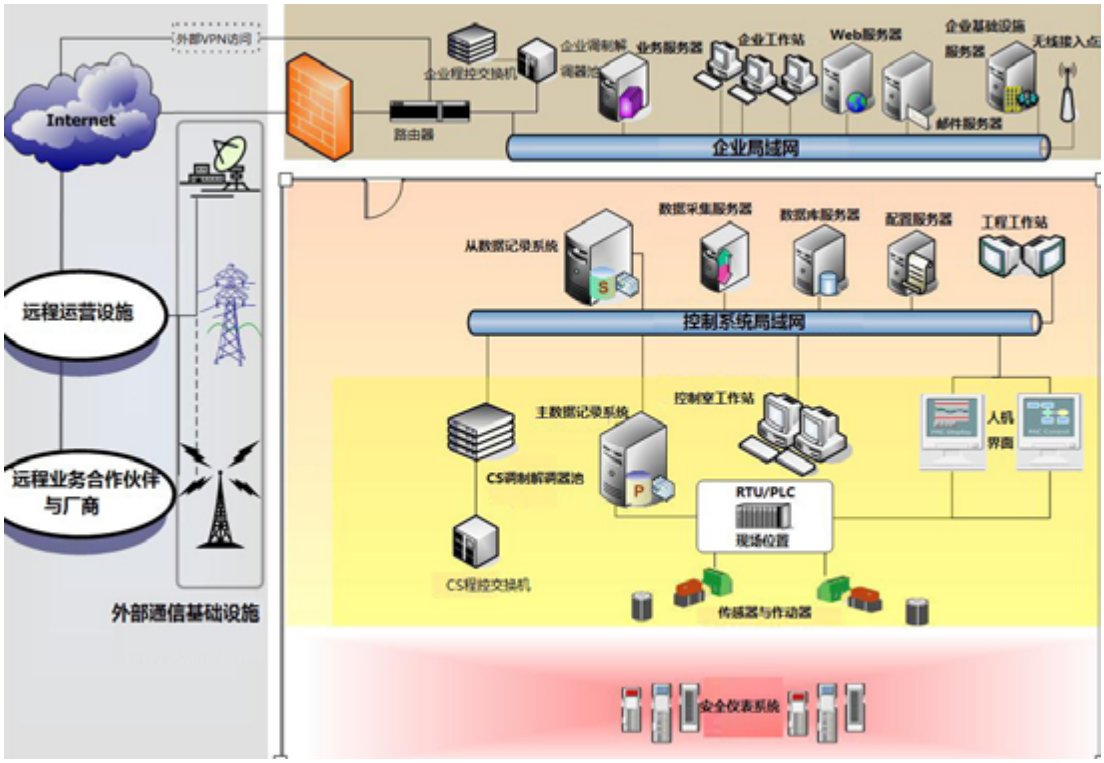

图 1 企业架构与控制域分隔的传统场景

1.2 现行工控系统架构概览

曾经隔离的工控系统逐渐走向融合，助力企业简化并管理复杂的环境。在联网及向工控系统域添加 IT 组件时，如下情况可导致安全问题：

- 对于自动化与工控系统越来越依赖；
- 与外部网络的不安全连接；
- 使用的技术包含已知漏洞，在控制域造成前所未见的网络风险；
- 缺乏与工控系统环境相关的网络安全业务案例；
- 某些控制系统技术仅有有限的安全能力，这种能力一般仅在管理员发现（或不会阻碍流程）时才会启用；
- 许多常用的控制系统通信协议缺乏基本的安全功能（如认证与授权）；
- 关于工控系统、工控系统操作及安全漏洞的开源信息大量存在。

长期以来,业界将控制系统的运营安全定义为系统安全有效运行的可靠性水平。将工控系统同外部(不可信)网络完全隔离，总体通信安全的范围被压缩至员工相关威胁（这里的员工指的是可物理访问设备或工厂车间的员工）。这样，信息基础设施内的大多数数据通信仅需要有限授权或安全监管。运行命令、指令与数据采集发生在封闭环境中，这个环境中的所有通信都受信任。一般情况下，命令或指令通过网络下发，预期在到达目标后执行授权功能，因为只有授权操作员才可以访问系统。

对于有效保障网络与 IT 网络安全，这种方法可谓另辟蹊径。将新型 IT 架构与缺乏真正网络安全防护措施的隔离网络融合具有很大挑战。显然，使用路由器与交换机可将设备进行简单互联，但是个人的非法入侵会导致对系统的不受限访问。图 2 中提供的融合架构包含了来自于外部的连接，如企业局域网、对端站点、厂商站点以及互联网。

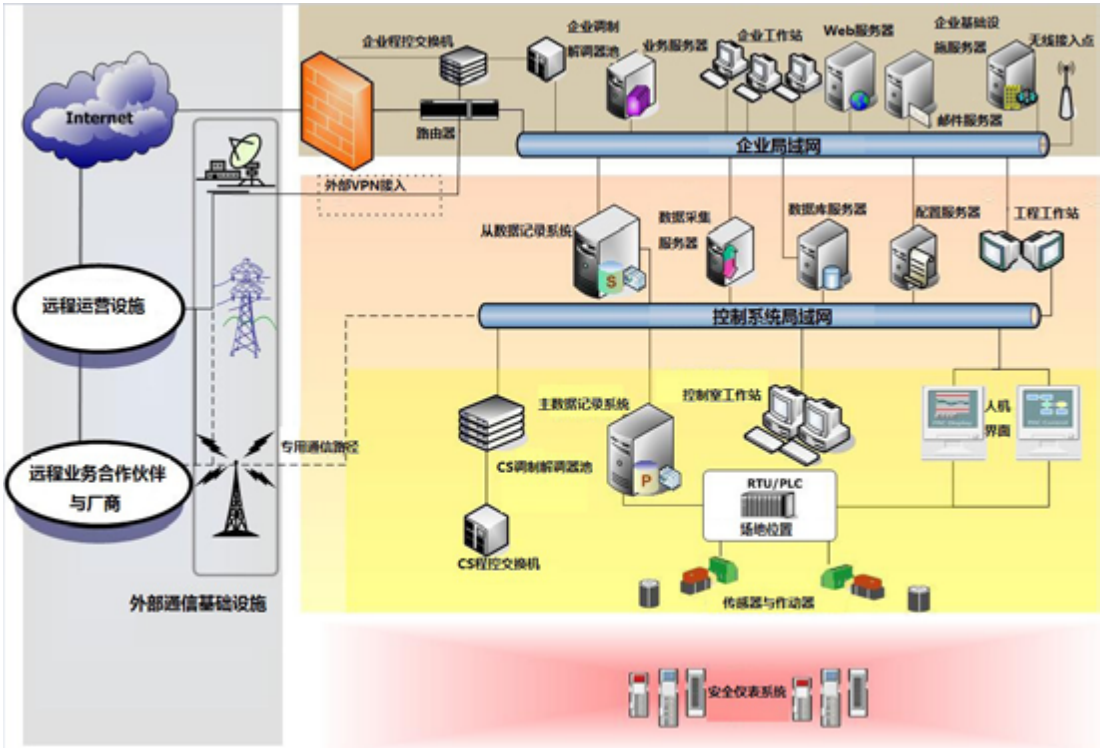

图 2 融合网络

如图 2 所示，融合架构若被入侵，攻击者可通过各种渠道访问企业局域网、控制系统局域网甚或通信局域网的关键系统。此种架构本质上要求与各种信息源交换数据，这可以被攻击者所利用。

2.0 工控系统内的安全挑战

在基于传输控制协议 / 互联网协议（TCP/IP）的现代计算环境中（如对驱动控制系统运行的业务进行管理的企业基础设施），需解决技术相关漏洞问题。传统上，这些问题由企业的 IT 安全组织负责，根据重要信息资产的安全指导方案与运营计划进行工作。当工控系统从属于联动架构时，主要关注的问题就变成如何提供同时覆盖控制系统域的安全规程。现有基于网络的通信所产生的某些安全问题须在控制系统域解决，因为各厂商使用不同协议，再加上老旧系统固有的安全问题，也许很难保护关键业务系统免于遭受时下的网络攻击。

开放的系统架构中存在的、可迁移至控制系统域的漏洞包括恶意软件（病毒、蠕虫等等）漏洞、通过操控代码提权、网络侦测与数据收集、隐蔽流量分析、通过或绕过边界防护非法入侵网络等。对于更为先进的系统，漏洞还包括恶意移动代码，如涉及 JavaScript、applet 小程序、VBScript 及 ActiveX 的恶意活动内容。成功入侵工控系统网络后，会出现新的问题，如控制系统协议反向工程、针对操作员控制台的攻击、非法访问受信任的对端网络与远程设施等。要将信息安全与信息保障完全引入控制系统域，必须了解传统 IT 架构与工控系统技术之间的关键差异。

从缓解角度看，仅在控制系统中部署 IT 安全技术也许并不可行。虽然当下工控系统的常用基础协议与 IT 及业务网络的基础协议相同，然而，由于控制系统的本质功能要求（再结合运行及可用性要求），有些安全技术虽然很可靠，可能却无法使用。有些行业（如能源、交通与化工）的需求有很强的时效性，而安全策略的延迟与“吞吐量”问题却会导致时延过长、系统性能降低或恶化。

传统 IT 环境与控制系统环境之间在安全方面存在一些重要差异。图 3 展示了组织安全功能中常见的较突出的网络安全元素，并提示了这些元素在两种环境中使用时可能以何种方式被利用，并给出了处理这些元素的方法 [2]。

安全相关项目	信息科技（IT）	控制系统（ICS）
防病毒与移动代码	极常见，易于部署并更新	考虑到对ICS造成的影响，会很难；老旧系统无法修复
补丁管理	易于定义；全企业范围远程、自动	安装补丁很麻烦；局限于特定OEM；可能影响性能
技术支持期限（外包）	2~3年；多厂商；升级普遍	10~20年；相同厂商
网络安全测试与审计（方法）	使用新方法	测试成适应系统；新方法对ICS不适用；脆弱设备会崩溃
变更管理	定期定时；系统闲时进行	战略性调度；考虑到对系统的影响，过程并不简单
资产分类	常规做法，每年进行一次；根据结果确定网络安全支出	仅在要求时进行；关键资产保护与预算费用挂钩
事件响应与取证	易于开发、部署；某些法规要求；内置于技术中	不常见（除必要的系统恢复活动）；无取证（除事件重现）
物理与环境安全	差（办公系统）到优秀（关键运营系统）不等	优秀（运营中心；门卫、大门、枪支）
安全系统开发	开发流程中的必要部分	一般非系统开发中的必要部分
安全合规	有限法规监管	特定法规指导（某些行业）

图 3 IT 与工控系统安全关注点对比

2 美国国家标准技术研究所 .NIST SP 800-82（3-1）有一小节介绍了工控系统和 IT 系统的差异 . 工控系统与 IT 系统比较，http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf，2008 年 9 月 . 网站上次访问时间为 2009 年 10 月。

2.1 安全状况与攻击方法

一般情况下，当今信息网络按如下方式划分安全目标优先级[3]：

机密性	重要
完整性	重要
可用性	不太重要

不过，工控系统需要具有高可用性，满足运营需求，因而多数管控单位按如下方式划分安全目标优先级：

可用性	非常重要
完整性	比较重要
机密性	不重要

控制网络由独立域演变为与企业 IT 环境共存的互联网络，因而引入了安全威胁与漏洞。需要解决的工控系统域关键网络安全问题有很多，但是优先级不同，最迫在眉睫的问题包括：

- 网络边界中的后门与漏洞（有意或无意造成）
- 几乎或根本没有安全特性的设备（调制解调器、老旧控制设备等）
- 常用协议中的漏洞
- 针对现场设备的攻击
- 针对数据库的攻击
- 通信劫持与中间人 (MitM) 攻击
- 软件及固件没有定期安装或根本没有安装补丁
- 不安全的编码技术
- 内外部人士网络安全操作规程不当
- 缺乏针对控制系统的缓解技术

了解漏洞及利用漏洞的攻击向量非常重要，有助于制定有效的安全缓解策略。

2.1.1 网络边界安全漏洞[4]

常见的组网环境中，控制系统域会存在各种漏洞，为攻击者提供“后门”进行非法访问。一般情况下，后门是指架构边界中的小缺陷或被遗忘、遗漏或干脆忽略的嵌入能力。威胁一般不要求物理访问某个域以获取访问权限，通常利用的是已发现的读取功能。当今网络（尤其是控制系统域的网络）常内嵌某些能力，却没有进行足够的安全分析，攻击者一旦发现就会长驱直入。这些后门存在于网络的不同位置，但无疑网络边界是最受关注的位置。

说到网络边界组件，现在的 IT 架构使用各种技术提供强大的远程访问功能。这些技术一般包括防火墙、面向公众的服务以及无线访问。每种技术作为更大、更复杂的信息基础设施的子系统，促进网络内部 / 之间的通信。然而，每个组件或多或少都会有安全漏洞，而攻击者会试图发现并利用这些漏洞。攻击者尤其对互联网络感兴趣，因为互联资源间的相互信任关系，他们只需单点突破，便能在网络中自由出入。

由于无线通信设备的大量使用，网络边界大大扩展，尤其是对于边远地区的站点来说。这带来了可被利用的新漏洞，因为许多组织都存在不安全的无线访问。因为无线通信的易用性以及对于无线网络安全隐患认识不足，无线访问网络无处不在。更有甚者，在工厂车间环境中，无线技术比传统的有线通信设施更易部署，因为后者要求穿墙打孔以及布线。因为认同无线通信的便利性，许多厂商已经具有一整套的无线解决方案。

3 一般说来，机密性、完整性与可用性的重要程度取决于业务功能，许多情况下，不同行业对其有不同定义。不过，支持核心关键基础设施、涉及到生活质量与人身安全（指控制系统用户）的系统一般要求数据长期可用并完整无缺。满足这些要求比防止数据被非法查看更为重要，除非此类行为造成的数据泄露会影响到其他关键属性。

4 乔恩 · 纳什: 网络边界的后门与漏洞，http://www.us-cert.gov/control systems/pdf/backdoor0503.pdf，2005 年 8 月。网站上次访问时间为 2009 年 10 月。

无线通信的常见安全问题包括默认安装带来的副作用。攻击者一旦发现了无线通信点，便可以基于无线网络的固有功能，利用服务集标识符（SSID）广播、有限的访问控制措施、加密缺失及有限的网络分段发动攻击。考虑到控制系统网络的历史特点，尤其是明文流量及固有信任关系带来的安全影响，非法访问（通过无线接入点）控制域会为攻击者洞开后门，助其绕过安全边界。

最近的某些研究发现了 802.15.4 协议中存在一些重要的服务型漏洞，这些漏洞可能导致流量拥挤、拒绝服务。有些针对协议实现的修补（如为了扩展地址空间）会因为需要满足互通要求而降低安全防护。

虽然恰当的补丁管理程序可降低安全系统维护的复杂性，在同时关注设备的地理位置和可达性时，控制系统单元就会面临严重问题。尤其需要注意的是，不同的控制系统部件可通过远程通信访问。一般情况下，若系统基于商业操作系统，攻击可通过拒绝服务、提权利用程序或木马、逻辑炸弹之类的秘密工具发动。

现在的计算技术允许进行远程控制系统操作，这样，安全边界就外延至远程访问接入点。这对安全管理员提出了新需求，他们既需要管理这些新连接，同时还要防止重要的命令与控制功能被破坏。许多情况下，入侵对控制系统有管理权限的计算资源具有和入侵操作员控制台一样的效果。需关注的问题包括对数据进行拦截、修改及回注到网络、攻击者在控制域内提权以便在整个控制信号通信回路执行工程级指令。

控制系统所有人基于从控制系统收集的信息进行业务决策（如计算负载、预估需求）。在提供客户支持服务时，许多行业的组织通过公共服务器提供数据给客户、供应商及附属机构。这类服务器中的数据通常来源于业务域（从控制或现场操作域收集）或公共域。

这种互联能力虽然高效，但同时也为攻击者提供了攻击向量，使其可访问被保护的业务网络甚或工控系统网络。攻击者一般从公共服务器收集重要信息，包括与操作、客户及文件传输相关的数据。此外，攻击者在入侵服务器后，可提升自己的权限，针对后端业务网络甚或控制网络发动攻击。这种攻击的典型例子出现在高级计量架构（AMI）领域，这个领域积累了从客户处获得的大量能源使用数据，并对这些数据进行处理、展示，将其作为计费依据。因为 AMI 涉及到的是双向操作，这种合并的命令与控制会导致漏洞，若被利用，则会影响公共设施运行。

有些组织用防火墙将公共服务器同内部网络隔离，此种情况下，很难防护这类攻击。欲通过外部服务如 Web 或 FTP 服务器提供可靠的信息，Web 服务器需与内部数据库或数据记录系统通过防火墙建立连接进行通信。若缺乏有效的安全防护措施，防火墙与 Web 服务器之间的信任关系则会允许外部数据进入内部。如果这些数据没有经过授权，并且来自于针对可信 Web 服务器的攻击，攻击者就可以通过这个渠道访问业务（工控系统）局域网中的内部服务。

总的来说，要在业务功能与安全之间达成微妙的平衡，这种平衡须恰当评估，经常审议。通过部署新技术提高生产率、访问更多资源，要求特别关注如何防止业务或控制系统网络中植入后门。

2.1.2 利用常用协议发动的攻击（如 OPC/DCOM 攻击）[5]

新型操作系统对工控系统有重大影响。在过去几年间，越来越多的组织开始在自己的环境中使用底层服务，如对象链接与嵌入（OLE）、分布式组件对象模型（DCOM）与远程过程调用（RPC）。用于过程控制的 OLE（OPC）是基于这些服务的实时数据通信标准。虽然许多设备正弃用基于微软的 OPC 模型，但因为 OPC 可保证与各种工控系统设备的有效连接，因而仍在普遍使用。此外，OPC 被广泛部署在控制系统环境中的关键业务组件（如人机界面（HMI）工作站、数据记录系统以及许多对 OPC 有持续依赖的企业资源计划系统）中。最近一项研究表明，许多工控系统及其流程在 OPC 服务不可用时可能会永久丢失历史数据与产生时间记录[6]。

控制系统环境中常用的 OPC 标准与应用编程接口包括 OPC 数据访问 3.0、OPC 报警、OPC 数据交换及 OPC 数据 -XML。Windows XP 与 Windows Server 各版本支持并使用所有的 OPC 标准与应用编程。OPC 服务与标准中已发现各种安全隐患和漏洞，包括简单的系统枚举与密码漏洞以及更为复杂的远程注册表篡改及缓冲溢出漏洞。这些漏洞将许多工控系统置于严重的风险之下，这些风险包括安装未知恶意软件、拒

5 美国计算机紧急响应小组 . 控制系统中 OPC、OLE、DCOM 和 RPC 的安全隐患，http://csrp.inl.gov/Documents/OPC%20Abstract.pdf，网站上次访问时间为 2009 年 9 月。

6 数字联结（Digital Bond）、英属哥伦比亚理工学院，Byres 研究所 .OPC 是什么及如何部署，http://csrp.inl.gov/documents/OPC%20Security%20WP1.pdf，2007 年 7 月 27. 网站上次访问时间为 2009 年 10 月。

绝服务攻击、提升主机操作权限及 / 或因超载漏洞造成的工控系统意外停机。

虽然许多此类漏洞已有解决方案或规避措施，但这些缓解措施对于工控系统架构并不一定有效。例如，Windows XP SP2 默认可修改主机配置，这会造成连接至远程服务器的 DCOM 应用不可用。为保证兼容性，针对 DCOM 与依赖 OPC 的应用，需进行大型内部测试，然而实际上这种测试并未进行。许多组织受这些默认设置影响，却并没有升级或更改应用，也没有将操作系统升级至 SP2。此外，微软针对分布式编程更新了自己的操作建议，开始弃用 DCOM，向基于 .NET 架构的面向服务架构演进。未来，由于缺乏对 DCOM 与 OPC 标准的支持，再加上工控系统的超长生命周期，大量部署 OPC 与 DCOM 的组织将无法得到厂商支持。许多常用的操作系统长期受安全漏洞影响，未来在与缺乏厂商支持的系统结合使用时，会凸显各种安全问题。

2.1.3 通过现场设备攻击控制系统

工控系统架构一般都提供远程访问终端端点与遥测设备的能力。某些情况下，现场设备本身允许通过各种方式（电话或专用设备）访问。为收集运营与维护数据，现在有些设备内嵌了文件服务器与 Web 服务器，以保证可靠通信。在与具有这种访问能力的现场设备通信时，除了专门的通信渠道，工程师与管理员还有其他备用方法。

例如，许多控制系统架构设计之初就是利用公共电话网络或专用调制解调器访问线路建立远程连接。在没有安全防护的情况下，攻击者可轻松进行远程连接而不被发觉（在几乎没有监控或日志的情况下）。通过轰炸拨打和暴力破解，具有用户名与密码的安全调制解调器仍会遭到攻击。很多情况下，系统缺乏基于登录失败次数的自动账户锁定设置[7]。多数关键系统仍使用拨号进行远程控制，这已人所共知，再加上 IP 承载语音（VoIP）的使用，这种一度被认为过时的侦测手段正卷土重来[8]。

此外，现场设备属于内部信任域，因此攻击者一旦访问这些设备，便可入侵控制系统架构。通过访问现场设备，攻击者可进入到传感器网络，并黑进控制系统网络。攻击者在意识到现场设备是控制域的延伸后，可将这些设备添加到可攻击目标清单中，在攻击的侦测与扫描阶段对其进行进一步研究。虽然这类攻击在串联情况下一般无法成功，远程设备若将新型组网协议与传统控制协议结合，其安全问题仍值得关注。

攻击者在入侵设备后，可控制设备，进行非法活动，并开始执行一系列操作，包括扫描内部控制网络、修改发往控制主机的数据、改变设备本身的行为等。若攻击者决定利用资源间的信任关系扫描控制网络，整个控制系统域实际使用的通信协议可被用来实现该目标。这对攻击者尤为有利，因为没人监控连接是否有恶意或可疑流量[9]。

2.1.4 数据库与 SQL 数据注入攻击[10]

数据库应用已成为工控系统及其相关记录软件的核心应用组件。传统的安全模型通过隔离核心控制系统组件以及专门防护针对计算机或软件组件的安全威胁来保护系统。工控系统内的数据库安全沿用了这些模型，使用彼此独立、同时又相互依赖的系统。而两个系统间的高度依赖关系扩大了威胁面。

工控系统使用的数据库一般与业务网络中的 Web 应用数据库或安装了 Web 应用的计算机连接。基本上，每个数据驱动的应用都转化为某种形式的数据库，多数应用使用的是结构化查询语言（SQL），其中许多具有 Web 接口，易于遭受典型的 Web 攻击，如跨站脚本攻击（XSS）或 SQL 注入攻击。

数据库中的信息对于任何攻击者来说都是高价值目标。若控制系统数据库连接到业务或金融数据库或连接到通过应用访问数据的计算机，攻击者可利用两个网络间的通信信道，绕过用于保护控制系统环境的安全机制。

---

7 美国国土安全部 . 控制系统调制解调器安全防护的推荐做法，http://csrp.inl.gov/Documents/SecuringModems.pdf，2008 年 1 月，网站上次访问时间为 2009 年 10 月。

8 已发布相关工具，用来编写利用 VoIP 系统的软件，通过轰炸拨打，一小时可拨打 1000 个号码。

9 某些入侵检测系统（IDS）可更新工控系统特征，防护控制域。通常，这些系统基于特征，在检测到恶意流量时触发防护。在不基于特征的情况下，IDS 可针对非特定流量或意外、异常流量触发防护。有关 IDS 的讨论，见下文。

10 美国计算机紧急响应小组 . 攻击方法分析：SQL 注入攻击，http://www.us- cert.gov/control_systems/csdocuments.html，2005 年 9 月，网站上次访问时间为 2009 年 10 月。

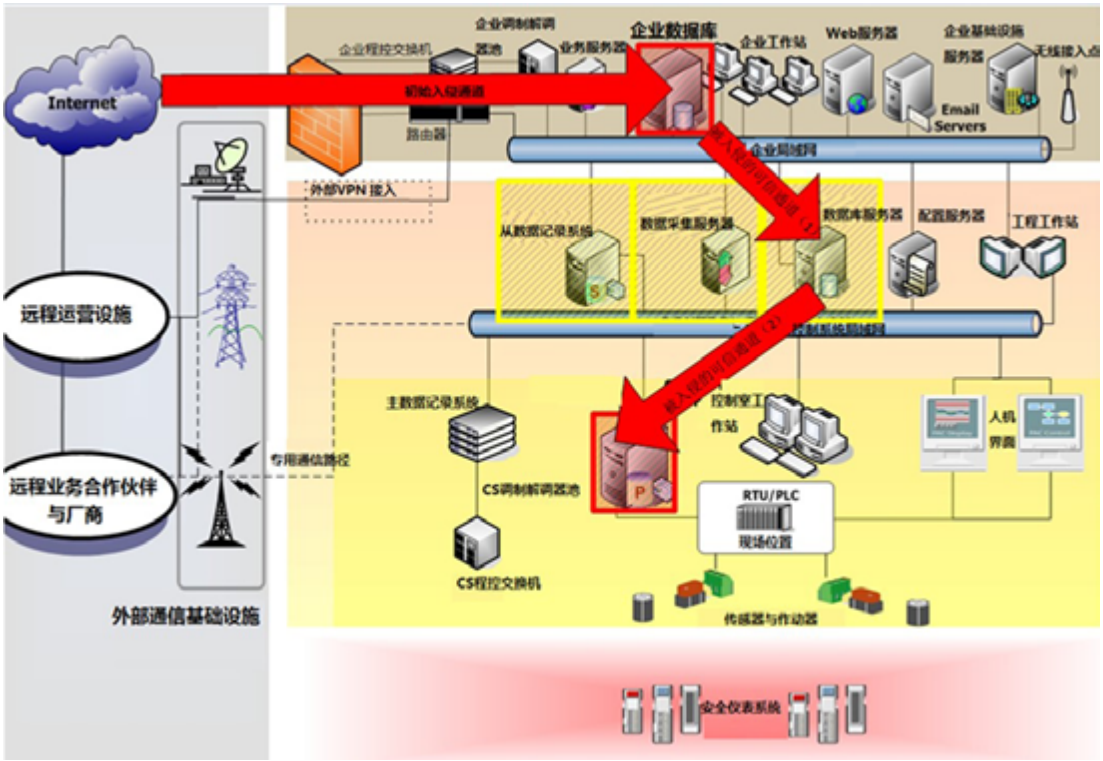

图 4 通过数据库进行攻击

图 4 举例说明了数据库之间的开放连接。此例中，攻击者可利用服务器间的通信路径获得控制网络的访问权。向数据库注入重要数据会有深远影响，控制系统环境中尤为如此，因为其数据准确性与完整性对业务和运营决策至关重要。数据库内容被损坏造成的级联效应会影响到数据采集服务器、数据记录系统、甚至操作员 HMI 控制台。相较普通 IT 数据库而言，工控系统受 SQL 注入的影响更大，因为它们更依赖于数据可用性与完整性。此外，通过入侵数据库等关键可信资产，攻击者会获得其他资源进行侦测与代码执行。

考虑到工控系统对于命令与控制数据的存储、准确性及可达性的依赖，以及这类网络中 SQL 数据库的普遍使用，标准的控制系统组件 SQL 注入技术对控制系统安全造成了极大威胁。

2.1.5 中间人攻击 [11]

控制系统环境一直是通过隔离网络（air gapping）来防护（或企图防护）非法访问。在这些网络中，服务器、资源与设备间的数据流一般防护措施较少。假定信任造成了三种安全问题：（1）攻击者可重路由网络中正在传输的数据；（2）可抓取、分析明文流量；（3）可反向工程控制协议，操控控制通信。将所有这些结合起来，攻击者可对网络中流动的数据获得极高的控制权，最终将真实与“欺骗”流量导入网络资源中，达到自己的目的。这就是中间人（MiTM）攻击。

管理网络（不管是控制系统还是业务局域网）中的地址对于高效运营意义重大。地址解析协议（ARP）将网络地址映射为物理机器地址，用这种方式进行路由。在每个网络设备中使用 ARP 表，计算机与其他设备在请求通信时便知道如何路由自己的流量。ARP 表操控（或污染）是攻击者的主要目标，因为污染 ARP 表会迫使所有的网络流量（包括控制流量）经过攻击者已入侵的计算机。这样，网络中的所有资源在不知情的情况下与攻击者进行“对话”。此外，攻击者可以看到、抓取、重放数据，并将数据注入到网络，并让人以为这些数据经过授权，来源于可信信息源。

假设攻击者通过上述攻击入侵到控制系统网络，便可利用网络侦测来判断网络中的资源是否可用。因为攻击发生在控制域，所以可捕捉（嗅探）到明文流量，进行离线分析及审核。攻击者审核、重新构造报文与负载内容后，根据攻击目标修改指令集，将新（可能为恶意）报文回注到网络。就数据负载中的指令名称而言，控制流量（不管其性质如何）并不复杂。报文数据用于控制现场设备行为，为 HMI 工作站操作员提供输入。

11 美国国土安全部 . 工控系统通用漏洞，Idaho 国家实验室，INNL/EXT-05-00993，http://www.us-cert.gov/control_systems/pdf/csvul1105.pdf，网站上次访问时间为 2009 年 10 月。

通过 ARP 污染及流量收集，攻击者可对网络中的通信进行控制，并维持此等控制。若攻击者欲采集、分析各种控制系统协议，需要看到、抓取并操控数据。反向工程关键控制数据、恶意操控数据的时长并不固定，取决于攻击者的攻击技能以及数据的复杂程度。然而，数据离线后，攻击者可根据自己的实际情况把握工作节奏。

在任何环境中，中间人攻击都极其危险。不过，在工控系统网络中，这种攻击更为致命。中间人攻击利用的是工控系统中的常见漏洞，如弱认证协议或不完备的固件完整性检查。利用控制系统中的常见漏洞会扩大攻击面，进而提高攻击的成功率。另外，通过控制关键信息资源发动中间人攻击，非法访问用户可通过如下方式攻击系统：

- 终止运行
- 抓取、修改、回放控制数据
- 注入不准确数据，伪造关键数据库、时钟与数据记录系统中的信息
- 在恶意攻击现场设备时将正常运行数据回放给操作者 HMI（同时阻止 HMI 发出告警）

2.1.6 不正确或不存在的操作系统和应用补丁

正如前文所述，典型的工控系统的技术生命可长达 10 至 20 年。正因如此，很多工控系统上运行的固件和操作系统都存在各种已知漏洞。通常对隔离工控系统普遍过于依赖且不支持适当的补丁管理操作规程，加剧了这一安全问题。典型的 IT 运营安全计划都包含一个安全程序，它不仅能监控厂商或第三方发布的漏洞，还能建立一个审核和安装安全补丁的统一流程。绝大多数控制网络都使用从 IT 部门获取的相同的操作系统。同类型的操作系统漏洞使控制系统易受攻击。一些先进的控制系统环境可能有补丁管理规程。但是，这一规程通常是手动过程，可能需要很长时间为系统打补丁。这是由站点之间的距离问题或没有接受过适当培训的资源造成的。

大部分控制系统操作在修补系统方面是非常谨慎的，因为部署安全补丁可能涉及大量测试，同时还可能影响系统的可用性（和安全）。如果缺乏适当的测试资源，如额外的实验室、临时区或测试设施，安全测试流程将难以执行。此外，一些补丁将打断当前流程或软件实现，导致一些控制系统操作跳过补丁流程，因而面临风险。

此外，补丁问题是及时更新固件的问题。固件更新可能包括安全级别补丁安装。如果不在主机设备内存中安装这些补丁，设备将面临本可通过补丁解决的安全问题。虽然固件更新的频率不如软件或操作系统补丁高，但是固件更新仍会耗费大量时间。

一些新型固件设备可远程自动更新。然而，在很多情况下，传统工控系统的硬件需要进行物理连接，或更糟情况下，需要完全被新固件取代。

2.1.7 不安全的编码技术

由于复杂度和“目的”要求，许多控制系统的实现中存在固有的不安全代码。一些工控系统中有陈旧的编程代码，要么是定制化的，要么是厂商不再支持的。这些编程代码不安全，原因有多种。例如，很多控制环境都是由在编程方面几乎没有进行过任何安全培训的人员搭建起来的。自定义应用程序没有经过适当的安全测试周期，很多在代码中都缺乏任何类型的文档记录或适当注释。常见的编程安全漏洞，如缓冲区溢出或不一致的输入验证，将导致代码不被厂商支持或自定义应用程序容易受到攻击（如拒绝服务攻击）。

通用控制系统编程的另一个安全问题是应用程序中缺乏验证或加密。未使用混淆代码，采用明文，使攻击简单易行。这类例子有很多。代码加密可能无法用于传统应用程序，自定义编写的代码如果加密，可能会被认为太慢。虽然很多应用程序（如果被攻击）可能不会被视为风险，但是同一应用程序被攻击后，可以作为一个攻击向量去攻击另一个更重要的系统。攻击一个几乎没有认证机制的系统更容易成功并很难响应，因为被攻击的系统可能不得不离线维修。

自定义应用程序和遗留代码并不是进行不安全编程攻击的唯一向量。很多基础软件厂商过去常常暴露和公布漏洞代码。有时，软件厂商可能在其软件开发周期内不支持稳健的安全审计程序。近年来，很多大型厂

商已经发布其软件补丁，但漏洞披露和软件补丁发布之间的时间间隔通常比典型的 IT 厂商的时间更长。

2.1.8 不恰当的网络安全规程

随着网络集成化和操作大型控制系统日益复杂，越来越多的人能够访问控制网络。随着外部访问的增长，远程业务合作伙伴和对端网站的连接也有所增加。另一个攻击路径是在工控系统环境中广泛使用调制解调器。从安全角度看，调制解调器管理不善，因为它们总是处于启用状态，并且没有设置任何类型的认证。即使对于远程访问控制系统有合理的规程，很多控制系统设备的日志记录能力较差，而且没有适时开启，以进行审计。

这样，针对这些控制系统安全标准应运而生。电力行业已强制执行 NERC-CIP 002-009 标准，很多电力组织已开始遵守该标准。小型电力企业可能觉得遵守这一标准太复杂和费用太高，因而可能会推迟执行。其他标准，比如 NIST SP 800-53（包括修订版）支持安全工控系统，但是很多非电力行业的组织可能会回避这些标准，同时等待政府机构出台行业相关的标准。

2.1.9 缺乏控制系统相关安全技术

典型 IT 环境的管理员有多种厂商可选，帮助其实现安全和缓解风险。IT 安全公司可选择具有多种安全产品的不同大型厂商，或者针对不同安全状态，从多个厂商处获取帮助。对于控制系统环境而言，安全技术的选择是针对环境的独特需求而定的。一些常见的 IT 厂商服务可针对工控系统进行修改或定制，但流程可能非常复杂和昂贵，并且所依赖的 IT 厂商可能没有专业知识，不能及时提供帮助。并且，使用没有强大的安全功能集的老旧系统会扩大攻击面。

3.0 隔离与保护资产：纵深防御策略

随着工控系统日益复杂，并连接到业务和外部网络，安全问题及其相关风险的数量也随之增长。针对控制系统多个资源的各种攻击向量使攻击成为可能。这些攻击可在很长一段时间内异步执行，并针对控制系统环境中的多个弱点和漏洞 [12]。仅靠一项安全措施无法缓解所有的安全问题。为了有效保护工控系统免受网络攻击，需要采取多项措施，使用多种安全缓解技术分散风险。

实现多层次防御对抗多个安全问题的战略通常被称为“纵深防御”。图 5 中将缓冲区溢出作为一个已知漏洞，以此说明使用多层防御来防护漏洞。该策略是基于在整个运营、网络和主机功能中使用适当的安全措施，集合所有的安全活动为整个架构提供完整保护。

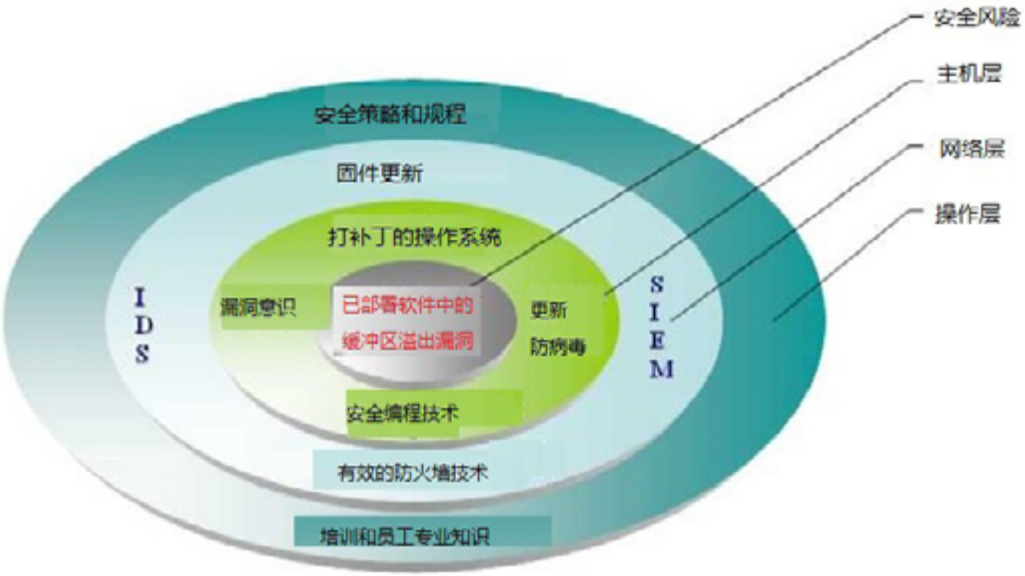

图 5 针对漏洞（例如缓冲区溢出漏洞）的层级防御

3.1 纵深防御战略框架

从纵深防御角度来看，网络安全不仅是部署特定技术来应对一定的风险。组织安全计划的有效性取决于其是否坚持并愿意将安全视为所有网络活动恒定的约束因素。实施有效的防御纵深战略需要采用全局法，并利用所有组织资源，以提供有效的层级防御。根据国家安全局（NSA）[13] 的研究成果，图 6 中显示了纵深防御战略框架的关键要素。

12 美国国土安全部 . 美国国土安全部在工控系统评估中发现的通用网络安全漏洞，http://www.us-cert.gov/control_systems/pdf/DHS_Common_Vulnerabilities_R1_08- 14750 Final 7-1-09.pdf，2009 年 7 月 . 网站上次访问时间为 2009 年 10 月。

13 美国国家安全局 . 纵深防御，http://www.nsa.gov/ia/_files/support/defenseindepth.pdf，网站上次访问时间为 2009 年 10 月。

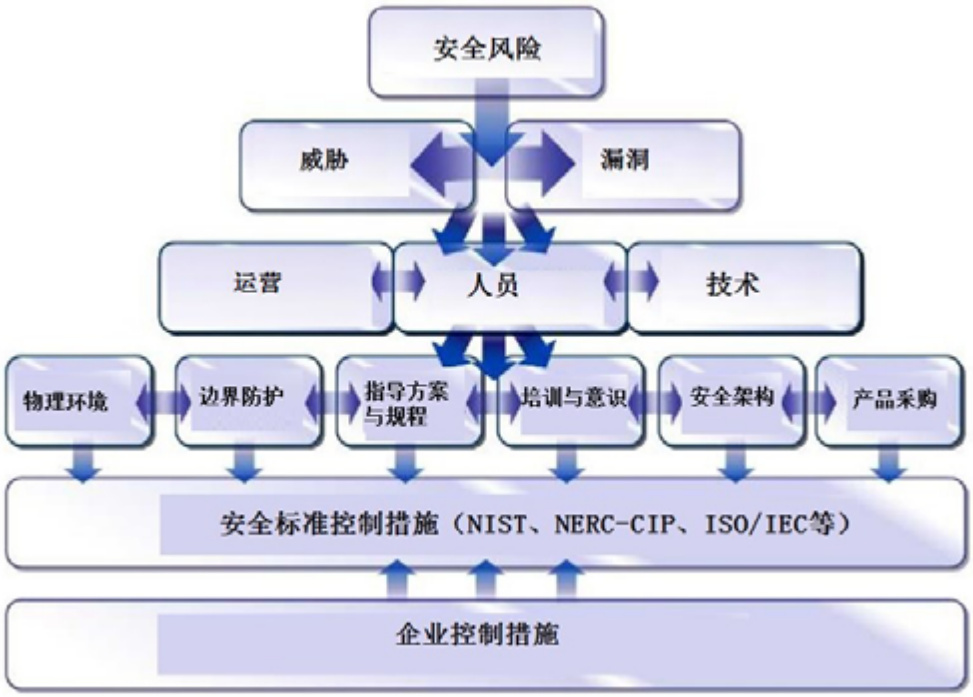

图 6 网络纵深防御的战略框架

该框架的基本宗旨是：

- 了解组织面临的安全风险
- 对风险进行定性、定量分析
- 利用主要资源来缓解安全风险
- 定义每项资源的核心能力，识别重叠区域
- 遵守针对每项控制措施已有或新制定的安全标准
- 制定、定制符合组织特点的具体控制措施

实施纵深防御战略的组织需要首先了解其当前的风险。了解了组织面临的组织面临的威胁和漏洞，就了解了对工控系统风险。为了了解风险，组织应进行严格的、覆盖组织各个方面的风险评估。风险评估是定义、理解和规划特定威胁和漏洞的补救措施的重要基础。合理的风险评估需定期持续更新，并获得组织各领域和层次的支持，包括公司高管。

为了创建起保护工控系统的文化，需要组建一个跨部门的团队。团队应包括至少一个行政级别的经理（给予领导和指导）、公司级安全与运营管理人员，并且控制系统工程师和管理人员应全面参与。该团队需要针对工控系统网络安全的主要方面进行培训，并充分意识到组织在其工控系统基础设施方面所面临的安全挑战和风险。

该团队负责制定指导方案和规程，以提高工控系统的安全能力和防护。欲对工控系统安全提供合理指导，首先应考虑所有的运营需求，确保新的安全指导方案不会对工控系统的可用性产生负面影响。一旦明确了操作要求，就可以建立完整的运营安全计划（OPSEC）[14]。OPSEC 计划应包括对角色和职责的明确划分，以及对物理安全、访问控制和强大的边界防御的日常管理操作的描述。

为了支持工作人员和 OPSEC 计划，满足组织工控系统具体需求的技术必不可少。合理的纵深防御技术

14 爱达荷国家实验室 . 利用运营安全（OPSEC）作为控制系统环境的网络安全文化的支撑，版本 1.0，http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf，2007 年 2 月。网站上次访问时间为 2007 年 10 月。

部署始于强大的技术评估计划、采购流程（采购前特别需要安全能力）[15] 和能够加强整个系统生命周期安全性的实施计划。工控系统中的技术为更大型安全架构的一部分，该安全架构划分出了互联互通和架构安全能力的关键领域。

3.1.1 架构域

为了创建层级防御，对如何融合所有技术及所有互联互通位置的清晰了解是至关重要的。将通用控制系统架构划分为多个域可以帮助组织建立明确边界，从而有效地应用多层防御。了解如何实现网络分段对创建架构域非常重要。在系统环境中或周边进行网络分段的方法可利用最佳实践，包括（但不一定限于）：

- 防火墙（单一防火墙、多宿防火墙、双宿防火墙、级联防火墙）
- 带有访问控制列表（ACL）的路由器
- 配置的交换机
- 静态路由和路由表
- 专用通信媒体

为扩展控制层 Purdue 模型 [16]，将信息架构中的域按基本功能划分为 5 类：

- 外部域连接到互联网、对等位置、备份或远程异地设施。这不是一个非军事区（DMZ），而是通常被认为不可信的连接点。对于工控系统，外部域的优先级最低，风险最多。
- 企业域是公司通信连接区域。邮件服务器、DNS 服务器和 IT 业务系统基础设施组件是本区的主要资源。由于系统数量和与外部域的连接，该区域存在各种风险。然而，由于安全状态和系统冗余的成熟，企业域的优先级应低于其他域，但远高于外部域。
- 制造 / 数据域是连接区域，其中绝大多数的监控和控制都发生在此。这是控制网络连续性和管理的关键领域。运营支持和工程管理设备，以及数据采集服务器和数据记录系统都位于此域内。制造域对终端设备和企业域业务需求的操作很重要，该域的优先级为高。风险大小取决于是否直连到外部域和企业域相关。

15 美国国土安全部 . 控制系统网络安全采购用语指南，http://www.us-cert.gov/control_systems/pdf/SCADA_Procurement_DHS_Final_to_Issue_08-19-08.pdf，2008 年 8 月，网站上次访问时间为 2009 年 10 月。

16 T. J. Williams. 普渡控制层级模型，SBN 1-55617-265-6，1992。

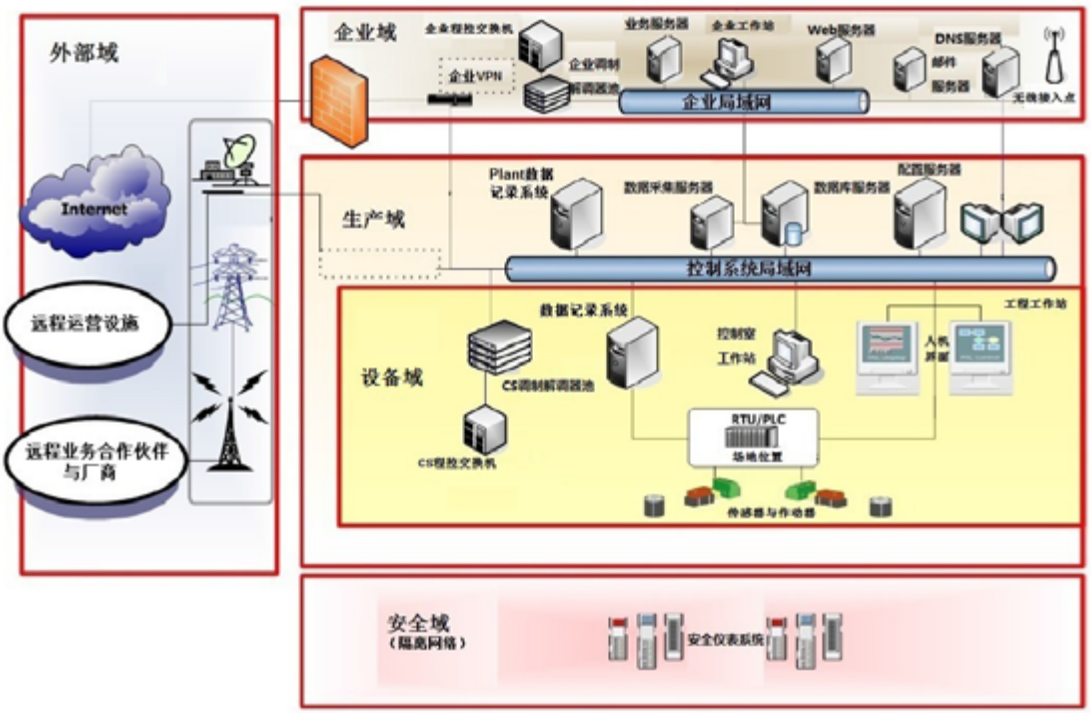

图 7 通用架构域

每个域需要关注的安全问题不同。“剥洋葱式的”分析表明，试图影响关键基础设施系统的攻击者很有可能对核心控制域[17]感兴趣。如果这个关键域被攻击，对核心服务与控制系统的运营能力进行完全控制对攻击者来说价值巨大。在很多部门内，对控制系统的恶意攻击将带来现实的物理结果。

本文以及由美国国土安全部（DHS）通过美国计算机紧急响应小组（US-CERT）提供的支持文档中讨论了很多攻击类型和结果。在这些情况下，入侵都是从控制域以外开始的，然后逐渐渗透到架构内部。

因此，能够确保每一个核心区域安全的防御战略可以创建一个纵深防御战略，为管理员提供更多访问信息和资源控制的机会，并引入不会影响业务功能的级联措施。

3.2 防火墙

防火墙增强了防御性，能够支持传统路由器，从而为不同网段或区域间的通信添加更严格、更复杂的规则。工控系统的关键是如何实施防火墙，以及防火墙的核心功能如何在一定程度上影响环境的整体业务功能。

防火墙的类型多种多样，但需要研究确定哪类防火墙才是适合控制架构的。此外，由于不同的防火墙可运行在 OSI 模型的不同层中，应考虑控制系统应用和连接将跨越的边界（若有）。了解防火墙的工作方式有助于了解网络不同层之间如何相互作用。网络架构（包括利用模型建立的控制系统架构）都是围绕 7 层模型设计的。OSI 模型允许一个网络中存在不同的协议，并支持物理连接。防火墙往往部署在网络入口和出口（域），它能在不同层上运行，并使用不同的标准限制流量。这对成功部署防火墙，尤其是制定隔离网络解决方案来说是非常重要的。防火墙最低可以工作在第 3 层，对应 OSI 模型中的网络层[18]。该层负责处理路由，并且可允许设备（如防火墙）来确定是否允许连接，但不能评估数据包内容有效性。

因此，对数据包提供更多分析和“检查”的防火墙运行在更高层，直至传输层。这些防火墙可以提供更细粒度的数据调查，并可以允许或拒绝有效载荷。在应用层工作的防火墙通常可以提供大量用户活动和数据结构的信息。然而，还是注意：尽管运行在协议栈中更高层的防火墙看起来在很多方面都更优越，但情况并非总是如此。

前文讨论了安全域的概念，它能够帮助了解组织如何确定与特定域相关的风险和后果。这样的分析可用

17 当然，这取决于攻击者的整体目标。通常，完全控制核心服务和控制系统的运营能力的值很高。

18 TCP/IP 模型早于 OSI 模型，相比之下，TCP/IP 模型的前 4 层与 OSI 模型类似，互操作性对两者都是通用功能。

来选择防火墙的类型和属性，更好地保护资产。通常，防火墙主要有以下四种类型：

- 包过滤防火墙（工作在网络层）
- 电路级网关防火墙（工作在会话层）
- 代理网关防火墙（工作在应用层）
- 状态监测防火墙（工作在网络层、会话层和应用层）

3.2.1 包过滤防火墙

包过滤防火墙对进入分隔网络的数据包进行分析，并根据预先设置的规则决定允许或拒绝数据包通过。包过滤规则是根据与数据请求类型相关的端口号、协议和其他预定义数据而制定的。虽然规则分配很灵活，这类防火墙非常适合应用在需要快速连接和可以基于设备地址制定规则的环境中。诸如工控系统之类的环境需要通过独特的应用程序和协议进行有效安全防护。

3.2.2 代理网关防火墙

代理网关防火墙的重要性在于它可以隐藏所保护的网络中，并作为主要网关代理由受保护的资源发起的连接。代理网关防火墙常被称为应用级网关。除了它能够列出应用地址外，其他与电路级网关类似。它们在 OSI 模型的应用层中过滤数据包，不允许任何无代理的连接。这些防火墙有利于分析应用程序的内部数据（POST 和 GET 数据等），以及收集有关用户活动（登录、管理等）数据。防火墙就是网关，要求用户将连接转向防火墙。由于需要分析数据，防火墙对网络性能也有一定的影响。在工控系统环境中，这类防火墙可用于分离业务和控制局域网，并保护 DMZ 域和其他需要特定应用程序防护的资产。

3.2.3 主机防火墙

主机防火墙是一种软件解决方案，能够保护防火墙安装设备的端口和服务。一些第三方软件包是基于主机的防火墙，但服务器、工作站、笔记本电脑和其他设备的很多新版操作系统上都集成了主机防火墙。主机防火墙能够创建规则集，以跟踪、允许或拒绝出入设备的流量。新版操作系统都预装了主机防火墙。这些防火墙可以定制，以协助保护其他系统端口和服务。这些防火墙集成到操作系统上，并通过定制功能来保护主机。基于主机的防火墙是移动设备和笔记本电脑的一个非常重要的功能，因为它们可能会出入工控系统域。同时，根据人机界面和工程工作站上操作系统的新旧程度，工控系统也许可以利用基于主机的防火墙来进行额外防护。

3.2.3.1 状态检测防火墙

状态检测防火墙具备其他所有类型防火墙的特点。它们在网络层过滤数据包，判断会话的合法性，并在应用层评估数据包内容。它们通常使用算法来处理数据，而不是运行代理。这些防火墙对到达接口的数据包执行大量的数据包检查。它们查看数据包的“状态”，根据之前的观察进行分析，因此通过的数据包更为可信。这些防火墙能够持续跟踪有效会话，合理确定控制域中需保护的关键资产。由于工控系统中的很多漏洞都是由于在服务器和设备之间共享信任，所以能够跟踪有效和无效会话，并做出反应，对防护这些漏洞是很有利的。

3.2.3.2 PLC/ 现场级防火墙

PLC 现场级防火墙是基于硬件的防火墙，可直接管理控制系统网络上的设备级流量。这些防火墙试图给现场设备（例如 PLCs、远程终端单元和分布式控制系统）添加安全功能。对工控系统安全域而言，现场设备级防火墙相对较新，但对保护那些没有内在安全能力的设备影响显著。它们还可以提供入侵检测，并作为日志源协助统一威胁管理。

防御措施种类繁多，防火墙部署到工控系统环境对合理的安全计划而言是至关重要的。此外，在纵深防御安全态势下，在整个组织内部署分层防火墙的策略是必不可少的。在所有外部连接点（包括从工控系统网络到企业网络）上配置防火墙可加强所有所有网络边界层的安全。此外，卓越的防火墙部署技术就是从不同的厂商那里添加第二组防火墙。这两台厂商防火墙将匹配规则集和配置，但部署在架构的同一区域内。这有

助于防护只影响其中一个厂商防火墙的固件安全漏洞，同时增加了另一个防御层，使防御网络边界有时间在易受攻击的防火墙上修复固件，从而延缓并阻止利用漏洞的攻击。

当然，这会增加一些管理和成本费用，但是相较于增强的防护能力，这些努力都是值得的。明确这些情况后，便可以在多域架构中部署分层防火墙，如图 8 所示。在图 8 及相关的网络架构图中，安全带被认为是“隔离网络”，并不与架构 [19] 相连接。

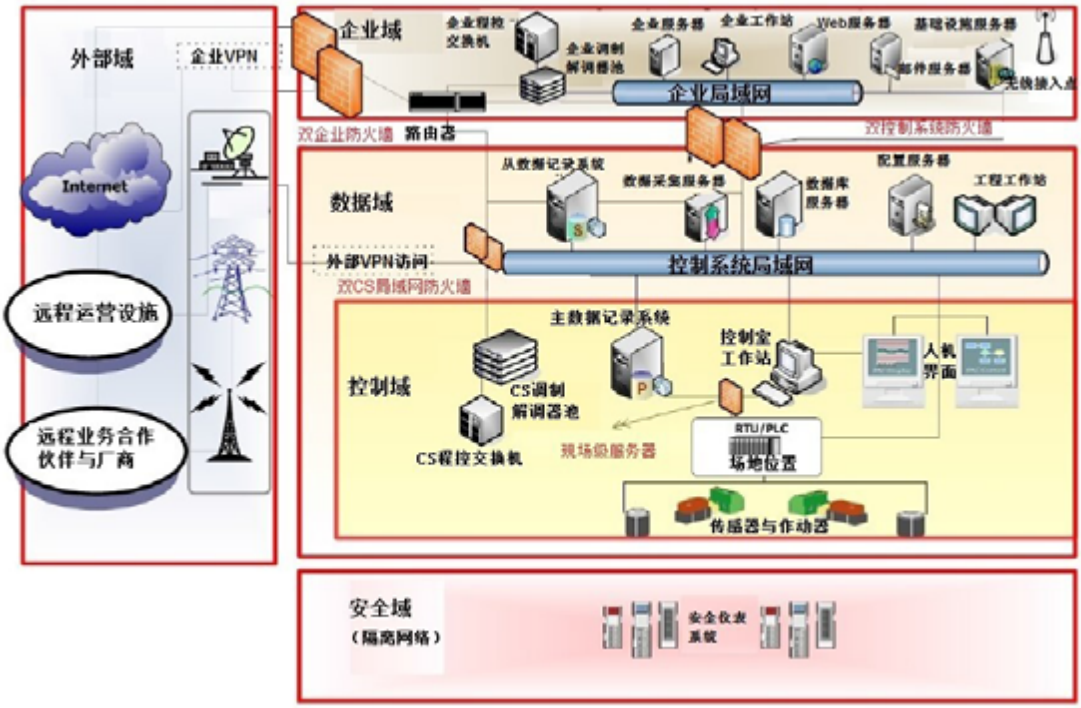

图 8 保护架构域的防火墙

正确配置防火墙对工控系统安全很重要。通信应仅限于必要的系统功能。更重要的是，进入某些特定领域的通信路径需要详细的安全风险评估，并且必须明确这些“管道”数据交换的权限。在制定网络设备的缺省规则集时，通信默认为“拒绝”，直到制定了具体的规则集。应监控工控系统流量，制定规则仅允许必要的访问。防火墙规则集中的所有异常情况都应尽可能细化，包括主机、协议和端口信息。

部署控制系统网络时一般并不限制控制域的出流量。防火墙规则应该考虑通过防火墙的双向流量。大部分管理员都能够有效阻止进入控制网络的流量，但并不过滤网络的出流量。还应该制定出流量规则，这样的规则最初应覆盖所有出流量。然后适当调整这些规则，以过滤掉所有不必要的流量。一旦确定了必要的出流量，可以创建更安全的配置，以阻止所有非必要的流量。

传统意义上，防火墙在防护网络中的角色非常简单直接。例如，针对工控系统的攻击者需要从工控系统网络中获取信息，并发送文件和命令到工控系统网络。为了远程控制在工控系统计算机上运行的程序利用代码，必须从控制网络中建立返回连接。对于工控系统领域中的攻击资源，代码必须很小，仅包含足够的代码使攻击者能够到达目标计算机。一般来说，设备上没有足够的空间来添加逻辑，使攻击者获可以得先进的功能。因此，攻击者需要额外指令以完成攻击过程中的发现环节。如果正确执行出流量过滤，攻击者将不会收到该返回连接，也不能发现和控制被利用的机器 [20]。

3.3 创建 DMZ 域

传统上，网络分段通过使用多个路由器实现的。防火墙应创建 DMZ 以保护控制网络。可以为单独的功能和访问权限创建多个 DMZ 域，例如连接、数据记录系统、数据采集与监视控制（SCADA）系统中的通信

19 历史上，安全系统已完全从控制系统中隔离出来，与安全系统之间的通信都是通过带外通信实现的。然而，一些正在考虑中的未来架构使用控制域把这些系统都网联在一起。

20 英国国家基础设施安全协调中心（NISCC）.NISCC 有关 SCADA 和过程控制网络的防火墙部署的优秀做法指南，http://www.cpni.gov.uk/docs/re-20050223-00157.pdf，2005 年 2 月。网站上次访问时间为 2009 年 10 月。

协议（ICCP）服务器、安全服务器、复制服务器和开发服务器。图 9 中是一个部署了多个 DMZ 的强大架构。

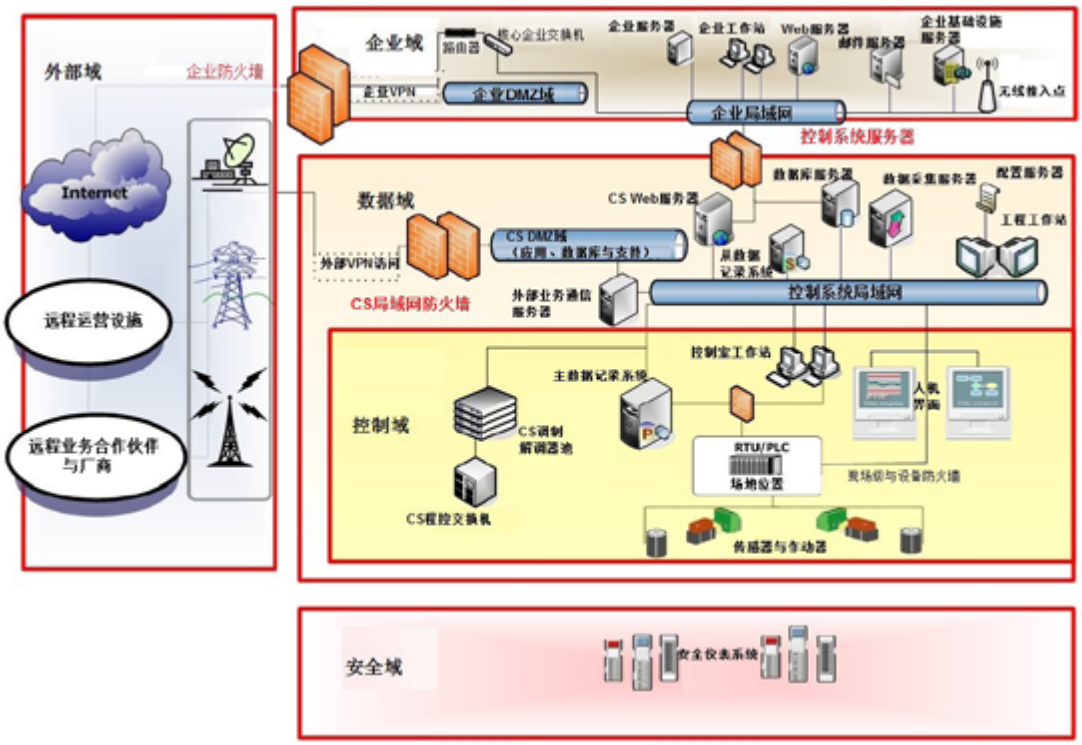

图 9 部署了 DMZ 的架构

对工控系统局域网的所有连接应通过防火墙路由，不允许任何连接绕过防火墙。网络管理员需要准确绘制工控系统局域网的网络图，以及与其他受保护的子网、DMZ 域、企业网络和外界的连接。

多个 DMZ 域在保护由不同业务活动组成的大型网络架构方面非常有效，这一点已得到证明。一个完美的例子就是针对工控系统和业务的连接网络，如图 9 所示。在此例中，安全数据流出入不同的环境对操作来说非常重要。使用多个 DMZ 域可以保护信息资源不受拟局域网跳跃和信任利用攻击，也是一个提高安全状态和加强纵深防御的好办法。

3.4 入侵检测系统

攻击者在考虑通过最合乎逻辑的路由入侵控制网络时，很容易构思出一条攻击路径，更深入地窥探网络架构。攻击者从外部环境出发，越过边界设备，试图最终接入目标网络以及网络中的主机。有些现场设备的远程访问需求会将漏洞引入工控系统架构中，这为攻击者的非法接入提供了可乘之机。一旦入侵目标网络成功，攻击者开始对其进行侦察，收集情报，之后试图入侵更多组件。每次攻击入侵，攻击者均会在目标网络上留下异常和未授权活动痕迹。通过对这些活动进行监控（和防御），提供另一层面的防御。

目前，可采用几种通用方法监控网络，识别异常或未授权的活动。其中，最有效的当属入侵检测系统（Intrusion Detection Systems，简称 IDS）。尽管目前已存在商用入侵检测系统，但入侵检测并非单一产品或技术， 而是一套网络监控工具和过程，为管理员全面展示网络的使用情况。利用多种工具可协助构建纵深防御架构，更加有效地识别攻击者的活动，并以预防性（如对非法流量采取行动）的方式使用这些工具。图 10 展示了入侵检测系统的纵深防御策略。

IDS 本质上非常被动。IDS 部署在网络中，用于监控与评估流量或网络活动，对流量没有任何影响。之前，IDS 主要部署在架构的出口 / 入口或重要网络资产的网络连接处。关于“安全区”概念，可通过配置合法流量和数据类型相关的意义明确的规则集来创建监控能力，识别突如其来的流量或非法流量。IDS 作为一款被动型设备运行，对于要求高可用性的系统来说是必不可少的。IDS 可将收集的流量与自定义和预定义规则（基于特征）以及基于启发式行为进行对比。确切地说，IDS 将所收集的流量与规则集和一系列已知攻击“特征”进行对比。IDC 将检查大量的流量属性，如端口号和数据载荷，判断是否有恶意活动（或非法活动）发生。

一旦检测出攻击特征或发现当前网络流量与所指定的正常 / 允许流量存在差异，IDS 将执行一系列指令，包括向系统管理员发出告警通知。这对于安全区管理来说非常重要，因为每个安全区可通过利用独特的检测特征进行监控。并且，这也有助于加速事件响应和资源管理，因为目前大多数 IDS 方案可提供广泛的日志功能。

大多数 IDS 基于特征，这非常适用于当前业务环境，因为目前有大量的特征可用于很多使用现行协议和操作平台的网络和主机架构。鉴于当前的业务域普遍存在安全漏洞，针对于利用普遍性技术的网络和主机来说，IDS 经稍加调整即可使用。与控制系统的补丁部署和其他安全技术相关的问题一样，IDS 的配置与部署并非易事。例如，尽管目前 IDS 的很多特征文件都能提供强大的功能，可检测出各种攻击，但用于监控控制网络中的恶意流量的特征尚不充足。在工控系统采用的独特通信协议（Modbus、ICCP、E/IP 或 DNP3）方面，传统上认为，特定载荷和端口号也是当前 IDS 特征的一部分。总之，当前工控系统中部署的 IDS 可能无法检测出系统中的攻击类型。

研究社区和厂商社区围绕解决此问题展开了研究与分析，取得了巨大进展。专注于控制系统网络安全的组织，携手厂商和集成商，创建了很多有用的特征，专门用于监控针对于控制系统中的技术或协议的特定攻击。尽管此次研究的最初输出仅针对为数不多的厂商的几个协议，但开发新特征的速度十分惊人。目前，用于控制系统的新的 IDS 特征也具备卓越的可用性。并且，这些特征的创建方法提供了一个架构，可使资产负责人和操作员为其控制系统网络[21] 创建独特的特征。此外，组织还可依据其网络的确定性，创建入侵告警。如果网络中的流量与正常的或期望的流量行为有差异，就会触发这些告警。

实际上可以设置阈值。这样，当流量或行为超过阈值时，会触发事件生成。之前，利用入侵检测系统“学习”网络行为被认为非常耗时且不可行，但现在这项技术已非常成熟。实践证明，启发式检测在工控领域的应用大获成功。很多安全厂商（甚至是某些控制系统厂商）已开发了学习引擎，构建特定的流量行为模型。控制数据的确定性极大地提升了特征的粒度，这是因为应对攻击者的违规或恶意行为，需要比预期的行为级别更高的措施。

部署 IDS 方案时，实体可能想删除某些默认特征和响应能力。因为他们认为常规类型的攻击流量不会出现在控制系统网络中，与工业操作无关，而且大量的预定义规则会影响 IDS 性能。然而，这仍需要进行分析，确保 IDS 的某些有用的能力帮助防御那些看不见的威胁。很多安全厂商，包括专注于工控系统安全的厂商，已为部署在控制架构中的 IDS 创建了特征。在工控系统网络中部署 IDS 时，必须使用通用的规则集和该领域独特的特征，包括通用特征。此外，与工控系统厂商合作开发安全特征也是非常可取的。

该行业存在的一个普遍问题是部署的网络监控工具虽投入了使用，但未进行合理的更新、监控或验证。为此，应对相关负责人进行培训，让其负责监控系统数据日志并将各类工具配置更新至当前最新版本。

21 例如，登录 http://www.digitalbond.com/wiki/index.php/SCADA IDS Signatures. 网站上次访问时间为 2009 年 10 月。

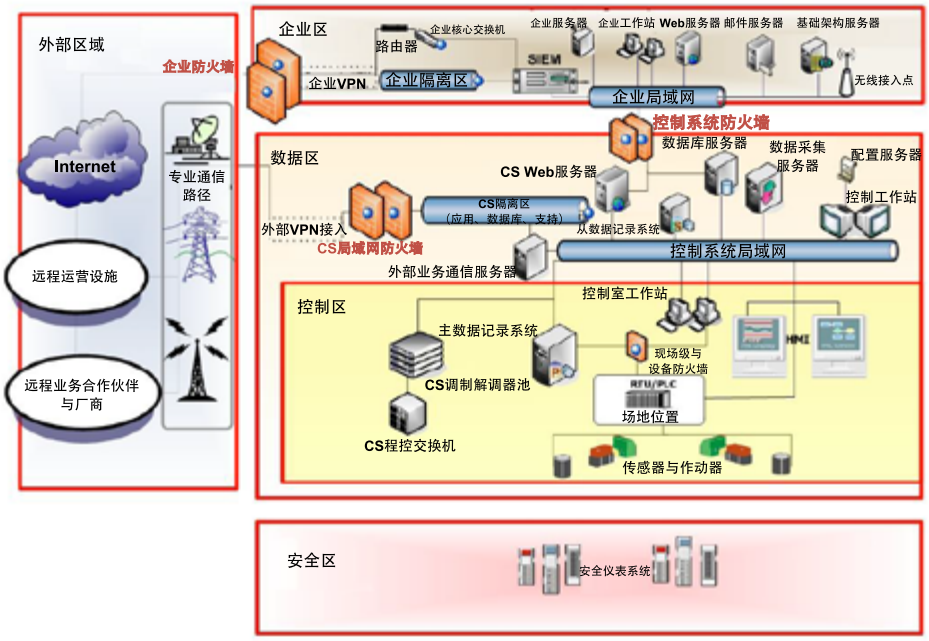

图 10 入侵检测系统和 SIEM 构成的全面纵深防御策略

IDS 在主机层面上的部署与其在网络上的部署类似。主机上部署的 IDS 对规则集进行监控，而非监控网络活动。这些规则功能强大且一应俱全，包括针对于平台或主机运行的操作系统的预定义特征生成的告警。主机层面部署的 IDS 提供另一层级的纵深防御，可增强边界和网络层部署的防御策略。

鉴于 IDS 的被动性，安全缓解和攻击实现受日志文件分析的频率（和有效性）的影响。制定健全的指导方案引导负责人及时对 IDS 日志进行分析非常重要。如果攻击者在用户查看日志文件前获得了系统访问权限且实施了攻击，那么 IDS 及其防御能力则形同虚设。除了组织须投入日志收集和分析之外，如果当前 IDS 方案不完善，可能会导致误报 [22] 相关的问题。

3.5 指导方案与规程

对于工控系统环境的指导方案与规程，准备齐全的文档且进行良好宣传，对于纵深防御策略的成功实施至关重要。应进行年度评审，确认指导方案与规程创建与维护的迭代特性。

3.5.1 日志与事件管理

随着越来越多的资产采用了防护技术，但对单个安全设备的有效监控与支持的能力却随之下降。当前的安全产品生成了大量日志。如果对其单独监控，将增加支持成本。为此，需采用安全信息与事件管理（SIEM）技术对日志和事件进行集中管理。中央控制台将给安全人员全面展示安全工具，如 IDS 日志、防火墙日志以及其他设备生成的日志。某些情况下，可从工控系统部件（如现场设备）处收集日志文件。图 10 展示了入侵检测系统和 SIEM 构成的纵深防御策略。

SIEM 产品可帮助简化安全事件管理，并过滤 IDS 日志中的误报（此过程非常耗时）。审计文件与日志文件汇聚后可关联到严重安全事件相关的常见事件。此外，SIEM 部署后可实现广泛的可视化能力。有效的数据可视化可缩短分析时间，提升响应能力，且简化新员工培训。安全数据分享与上报可帮助组织专注于其网络安全状况，因此为 SIEM 增色不少。组织如能实时共享安全数据，当前安全问题的展示也将更全面。这将会极大地促进组织各级之间的安全交流。通过准确有效的沟通，组织可把控更大的安全趋势，优化事后上报机制，并在日常运营过程中做好充分的安全准备。

22 对正常情况报错

3.5.2 安全指导方案

有效的安全指导方案和规程是确保工控系统安全的第一步。企业系统的很多 IT 安全指导方案可直接用于工控系统网络，满足其特定的安全需求。一个典型的实例就是，IT 安全指导方案促成了以下计划：北美电力可靠性委员会（NERC）电力系统[23]的网络安全需求、水利部[24]安全控制系统路线图以及化工行业[25]安全控制系统路线图。

有效的安全指导方案应切实可行且具可执行性，且可以让组织遵守其规定。此外，指导方案不应严重影响生产效率，成本过高或缺乏支持。为此，管理层和系统管理员最好尽量参与指导方案的制定。

其中，一个精彩实例是，管理层和系统管理员协作开发控制系统“金盘”。对于那些仅具备确保其在环境中安全有效地运行的必要的端口、服务、登录凭证以及软件的操作系统，金盘是基线配置。与管理层和管理员密切协作，识别合理的基线配置，可极大地提升安全管理，减少受攻击面。鉴于 OPC（用于过程控制的 OLE）主机的受攻击面[26]较大，采用这种方式可进行有效缓解。

此外，金盘可去除系统的所有来宾账户和无用的用户账户，确保用户仅具备正常运行系统所需的最小权限。这就确保了系统仅由具备更高权限的账户进行修改或调整。这一举措极大地减少了工控系统的非法使用情况，为在系统上安装不必要的恶意代码增加了难度。

另一个将特定指导方案应用于工控系统的实例是识别并维护调制解调器安全规程。一个优秀的调制解调器指导方案和规程列出了所有调制解调器的连接、明确了连接目的，并强制随付一份通过调制解调器拨打的电话号码的集中清单。应采用强验证方法，通过复杂密码保证调制解调器的安全，且这些密码须在管理层批准的经过验证的时间段内应进行例行更新。

规程应规定仅在必要时手动开启调制解调器，否则保持关闭状态。如果调制解调器提供自动应答功能，应将其移除或禁用。

如果此功能确实非常必要，应以书面形式向管理层提供合理解释，让其认识到此功能的必要性。如果每个调制解调器均开启了自动应答功能，规程应规定自动断开与预编入调制解调器内存须立即回拨的号码的连接。此技术是一项极佳的防御措施，因为这样保证了调制解调器仅通过一条专用线路进行通信。有关调制解调器安全详解，请参考美国国土安全部的《控制系统调制解调器安全防护的推荐做法》第六章。

安全指导方案也适用于无线通信。在无线接入点的规划、部署和配置过程中，无线安全指导方案可有效阻断非法接入，如 Wardriving（驾驶攻击）。无线安全指导方案应全面检查无线接入点，如 802.11、802.15（即 Zigbee 和 WirelessHART）、无线电和微波。无线防御措施应为层级结构，支持纵深防御理念，并采用有线网络的安全保障技术。无线安全指导方案应考虑并涵盖以下方面：（1）无线网络划分以及与有线网络分离；（2）强认证和授权技术；（3）基于地址和协议[27]过滤流量。一般说来，最佳无线安全指导方案是仅实施最强加密技术如 802.11 采用 WPA2-AES，不过不要完全依赖这些技术。

网络与工控系统管理员需具备技术知识，但在安全指导方案实施过程中也需管理层的授权和支持。管理层须支持配备与培养合适的人力资源，实施并管理工控系统安全。

3.5.3 补丁管理规划与规程

周全的补丁管理计划和规程对于工控系统环境来说非常必要，因为这有助于创建针对已发布漏洞的防御

23 北美电力可靠性公司（NERC）. 可靠性标准，日期 . 网站上次访问时间为 2009 年 10 月。

24 http://www.awwa.org/files/.../PDF/WaterSecurityRoadmap031908.pdf

25 美国国土安全部 . 化工行业安全控制系统路线图，http://www.us- cert.gov/control_systems/pdf/ChemSec_Roadmap.pdf，2009 年 9 月。网站上次访问时间为 2009 年 10 月。

26 数字联结（Digital Bond）、英属哥伦比亚理工学院，Byres 研究所 .OPC 主机安全加固指南 . 如欲了解基线配置详情，请登录 http://csrp.inl.gov/Documents/OPC%20Security%20WP3.pdf，2007 年 11 月。网站上次访问时间为 2009 年 10 月。

27 控制系统的无线安全：爱达荷国家实验室 . 通过 802.1H 保护无线局域网，草稿，http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf，2007 年 2 月。美国国土安全部 . 过程控制系统环境中 ZigBee 无线网络安全保护指南，http://csrp.inl.gov/Documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%2 0Control%20System%20Environments.pdf，2007 年 4 月。这两个网站的上次访问时间为 2009 年 10 月。

层。制定补丁管理计划前，应先了解每个系统的漏洞。通过分析和识别漏洞，工控系统管理员可确定需更新的设备。

要合理部署系统补丁，工控系统管理员应确保为环境中的每台设备定制合适的备份和恢复计划。配置管理、文档编写以及当前生产代码的更新的存档文件对于确保在补丁影响到系统运行时将系统恢复正常非常必要。补丁应在测试台或与当前运营环境非常相似的虚拟环境中进行测试。很多厂商都提供补丁管理计划，工控系统管理员可对其进行验证，确保补丁不会影响运营环境的其他方面。

管理员应与补丁管理计划的厂商密切合作，将自己的测试结果与批准的厂商补丁级别进行对比。这就确保了双重验证过程，提升了脆弱系统的补丁部署效率和可靠性。美国国土安全部已针对工控系统发布了补丁管理的推荐做法。如欲了解补丁流程和补丁计划 [28] 创建的详情，可参考这些推荐做法。

3.5.4 安全培训

很多情况下，工控系统网络的管理负责人并未接受过充分的安全培训。这种情况通常是因为缺乏资金或对安全培训重视不足。培训是总体安全意识计划的核心部分，涉及支撑关键信息和信息资源防护的数个关键特性。

控制系统相关的安全培训和周密的安全意识计划对于确保工控系统以及相关自动化流程的安全来说至关重要。如同为企业域名制定的安全意识计划一样，支持控制系统域名的此类计划也有一些核心组成部分，帮助提升持续且可衡量的安全态势。通用安全意识计划中，如 NIST SP800-50，《构建信息技术安全意识与培训计划 [29]》，组织可开发适用的安全意识与培训课程，涉及以下几方面：

- 目的与范围
- 资料开发
- 实施策略
- 监控与反馈
- 成功的衡量

网络安全管理员须持续接受培训，从而及时了解网络安全领域的快速变化和发展，包括最新网络架构设计、防火墙和 IDS 配置。针对于计算机网络的新攻防技术也不断涌现。因此，系统管理员和每个用户都有必要接受全面的计算机安全培训。

正规培训可能需高额费用，不过我们可从书籍、论文和网站中收集网络和工控系统安全相关的有用信息。首先看个具体的实例，美国国土资源部的控制系统安全项目（CSSP）是工控系统培训课程的优秀资源。该项目协同美国计算机紧急响应小组（US-CERT），管理并运营美国工业控制系统网络应急响应小组（ICS-CERT），专注于控制系统环境的新兴网络威胁 [30] 防御。

安全培训计划应提供面向全部人员角色和职责的年度培训。例如：

- 高级培训与安全意识培养
- 运营层培训与安全意识培养
- 关键网络资产负责人相关的技术层培训与安全意识培养

---

28 美国国土安全部 . 控制系统补丁管理推荐做法，http://csrp.inl.gov/Documents/PatchManagementRecommendedPractice_Final.pdf，2008 年 12 月。网站上次访问时间为 2009 年 10 月。

29 美国技术与标准研究院 . 构建信息技术安全意识与培训计划，http://www.csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf，2003 年 10 月。网站上次访问时间为 2009 年 10 月。

30 CSSP 和 ICS-CERT 鼓励人们上报可疑的网络活动、安全事件以及影响关键基础设施控制系统的漏洞。在线上报表格获取链接：https://forms.us-cert.gov/report/。可通过以下方式提交上报表格：
ICS-CERT 监察部门电话：1-877-776-7585
ICS 相关的网络活动：邮箱：ics-cert@dhs.gov
一般性网络活动：邮箱：soc@us-cert.gov；电话：1-888-282-0870

3.5.5 安全事件响应与取证

要全面支持纵深防御策略，需要强大的事件响应能力。一旦控制系统发生安全相关事件，应首先识别事件、然后作出响应、最后进行缓解和系统恢复。

事件响应规程应指导员工在网络中的计算机被入侵时采取响应措施。安全事件发生前，所有员工须参与培训并有权查阅此规程。例如，安全事件响应规程可回答以下问题：

- 事件发生后或正在发生时有哪些迹象？
- 应立即采取哪些措施（如断开计算机与网络的连接）？
- 应通知哪些人？通知顺序是什么？ 是否应联系执法部门？
- 应如何保存取证证据（如计算机应保持开机状态，将证据保存在内存中吗）？
- 如何恢复受影响的计算机？

如果缺乏合理规划，很难通过收集取证证据，获取确凿的证据，弄清特定事件的时间、地点、原因以及涉及的人员。应在安全事件发生前制定取证计划，以便尽可能的收集有用证据。周密的工控系统取证计划应归并到全面事件响应计划中，并说明工控系统环境中每个基线控制系统提供取证证据的能力。取证计划应是一个持续的过程，应将工控系统环境的所有部件按取证能力划分为不同类别。有关工控系统的更多信息，请参阅美国国土资源部的控制系统安全项目 [31] 的《控制系统取证计划制定的推荐做法》。

美国国家标准与技术研究院（NIST）编写了《计算机安全事件处理指南》，SP 800-61，为安全人员编写事件响应规程 [32] 提供了指导。此外，美国计算机紧急响应小组也提供了工控系统安全事件相关的广泛信息和上报能力。如欲上报安全事件，请登录 http://www.us-cert.gov/control_systems/。

31 美国国土安全部 . 推荐做法：创建控制系统的网络取证计划，http://csrp.inl.gov/Documents/Forensics_RP.pdf，2008 年 8 月。网站上次访问时间为 2009 年 10 月。

32 美国技术与标准研究院 . 计算机安全事件处理指南，NIST SP 800-61，http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf，2004 年 1 月。网站上次访问时间为 2009 年 10 月。

4.0 建议与措施

要有效保护信息基础设施，应首先具备主动安全模型。这一迭代模型由数个关键的安全策略构成，如图 11 所示。

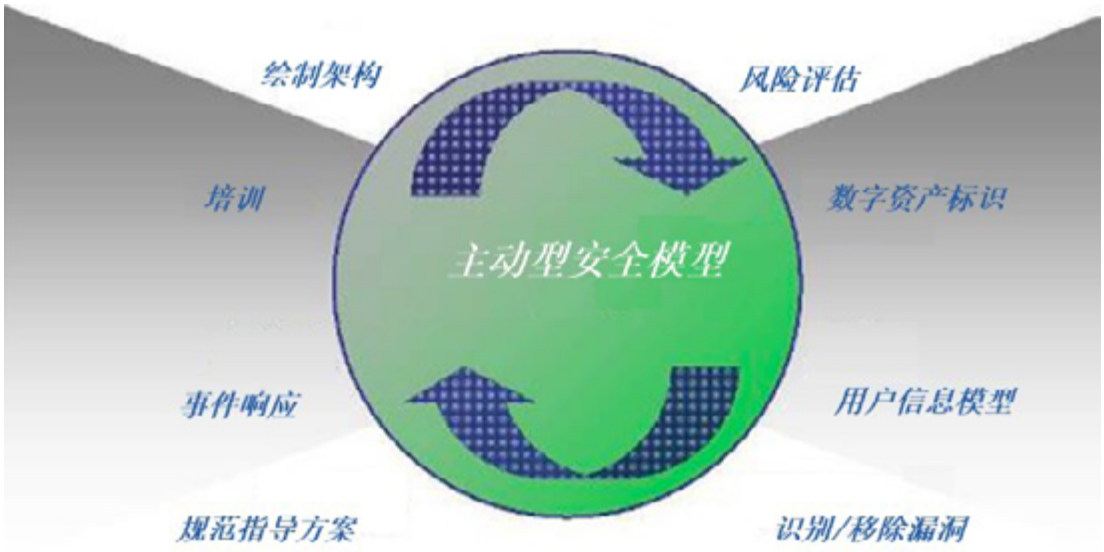

图 11 主动型安全模型

传统上，纵深防御策略的制定从绘制工控系统架构着手。绘制一个准确的架构并充分描述，会提升组织的安全意识，使其部署有效的安全措施且更容易了解安全事件。管理员在了解此架构后明确了防护目标。鉴于评估参数和流程的开发很容易与工控系统环境 [33] 中现有的（和已知）信息资产对齐，对架构的深入了解还将虑及有效风险评估。

具备安全评估能力后，组织即可在控制域内分配资产标识，明确命令与控制环境的整体概况。然后，组织可部署纵深防御策略。缓解策略的最后阶段是部署支持递归性持续安全培训的技术。

4.1 工控系统的五个关键的安全措施

以下是五个关键的安全措施，可推动工控系统环境中的网络安全活动。

- **安全指导方案。**应针对控制系统及其各部件制定安全指导方案，定期评审，以便纳入当前威胁环境、系统功能以及所需的安全级别。
- **阻止对资源和服务的访问。**一般情况下，在网络中部署提供访问控制列表的边界设备如防火墙或代理服务器，提供该技术。而主机方面，该技术可通过部署基于主机的防火墙和杀毒软件实现。
- **检测恶意活动。**恶意活动检测可在网络或主机层面实现，通常需有经验的管理员对日志文件定期监控。IDS 是识别网络问题的常用手段，也可部署在单个主机上。尽量在主机上开启审计和事件日志功能。
- **缓解可能出现的攻击。**在很多情况下，无需处理漏洞，因为漏洞修复可能会使系统不可用或效率降低。通过缓解措施，管理员可控制对漏洞的访问，确保漏洞不被利用。通常，这一情况在制定临时技术方案，创建过滤器或运行具备特定配置的服务和应用时非常必要。
- **解决核心问题。**要解决核心安全问题，需经常更新、升级、安装软件漏洞补丁或移除有漏洞的应用。软件漏洞可能会存在于网络、操作系统或应用这三层中的任一层。厂商或开发人员应提供缓解措施（如果有的话）供管理员部署。

33 美国计算机紧急响应小组（US-CERT）. 如欲了解控制系统和 IT 架构自评，推荐参阅“网络安全评估工具（CSET）”，http://www.us-cert.gov/controlsystems/satool.html. 网站上次访问时间为 2009 年 10 月。

5.0 延伸阅读

- 网络风险与漏洞

  “控制系统网络安全漏洞缓解”http://csrp.inl.gov/Documents/MitigationsForVulnerabilitiesCSNetsISA.pdf，网站上次访问时间为 2009 年 9 月。

  美国国土安全部在工控系统评估中发现的通用网络安全漏洞 http://www.us-cert.gov/control_systems/pdf/DHS_Common_Vulnerabilities_R1_08-14750_Final_7- 1-09.pdf, 网站上次访问时间为 2009 年 9 月。

  “控制系统通用漏洞”http://csrp.inl.gov/Documents/05-00993%20r0%20Common%20Vulnerability.pdf，网站上次访问时间为 2009 年 9 月。

- 安全与 SQL 攻击

  “攻击方法分析：SQL 注入攻击”，摘要

  http://csrp.inl.gov/Documents/SQL%20Abstract.pdf，网站上次访问时间为 2009 年 9 月。

- 安全与 OPC/DCOM（过程控制 OLE/ 分布式组件对象模型）

  “OPC 是什么及如何部署”

  http://csrp.inl.gov/Documents/OPC%20Security%20WP1.pdf，网站上次访问时间为 2009 年 9 月。

  《OPC 主机安全加固指南》http://csrp.inl.gov/Documents/OPC%20Security%20WP3.pdf，网站上次访问时间为 2009 年 9 月。

  “控制系统中 OPC、OLE、DCOM 和 RPC 的安全隐患”，摘要 http://csrp.inl.gov/Documents/OPC%20Abstract.pdf，网站上次访问时间为 2009 年 9 月。

- 运营安全

  利用运营安全（OPSEC）作为控制系统环境的网络安全文化的支撑

  http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf，网站上次访问时间为 2009 年 9 月。

  创建控制系统的网络取证计划

  http://csrp.inl.gov/Documents/Forensics RP.pdf，网站上次访问时间为 2009 年 9 月。

  控制系统的补丁管理

  http://csrp.inl.gov/Documents/PatchManagementRecommendedPractice_Final.pdf，网站上次访问时间为 2009 年 9 月。

- 调制解调器

  “控制系统的调制解调器的安全保护”

  http://csrp.inl.gov/Documents/SecuringModems.pdf，网站上次访问时间为 2009 年 9 月。

- 防火墙

  《NICC 有关 SCADA 和过程控制网络的防火墙部署的优秀实践指南》，http://www.cpni.gov.uk/docs/re-20050223-00157.pdf，网站上次访问时间为 2009 年 9 月。

  网络边界的后门与漏洞： 控制系统安全提升案例分析

  http://www.us-cert.gov/controlsystems/pdf/backdoorsholes0805.pdf

- 无线

  “过程控制系统环境中 ZigBee 无线网络安全保护指南”http://csrp.inl.gov/Documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%2 0Control%20System%20Environments.pdf，网站上次访问时间为 2009 年 9 月。

  “利用 802.11 保护 VLAN 安全”

  http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf，网站上次访问时间为 2009 年 9 月。

- 网络安全标准

  “石油和天然气行业的网络安全标准的比较”

  http://www.us-cert.gov/control_systems/pdf/oil_gas1104.pdf，网站上次访问时间为 2009 年 9 月。

“电力部门网络安全标准与指南的比较”http://www.us-cert.gov/controlsystems/pdf/electrical comp1004.pdf，网站上次访问时间为 2009 年 9 月。

- 美国国家安全局纵深防御

  美国国家安全局的纵深防御策略

  http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

- 入侵者检测

  入侵者检测清单

  http://www.us-cert.gov/readingroom/intruderdetcheck.html

- 人员安全指南

  “人员安全指南，”

  http://www.us-cert.gov/control_systems/pdf/personnel_guide0904.pdf

实操建议：采取纵深防御策略，提升工控系统网络安全

安全加社区

公益译文项目

2016

网络安全公益译文项目旨在分享国外先进网络安全理念，将网络安全战略性文档翻译为中文，促进国内安全组织在相关方面的思考和交流。该项目由安全加社区发起，安全加社区是国内的网络安全社区，社区欢迎网络安全人士的加入，并致力于交付网络安全问题的解决能力。