

工业控制系统网络与信息安全

北京力控华康 魏钦志

摘要：随着“两化”融合的推进和以太网技术在工业控制系统中的大量应用，进而引发的病毒和木马对 SCADA 系统的攻击事件频发，直接影响公共基础设施的安全，其造成的损失可能非常巨大，甚至不可估量。而在工业控制系统中，工控网络管理和维护存在着特殊性，不同设备厂家使用不同的通信协议/规约，不同的行业对系统网络层次设计要求也各不相同，直接导致商用 IT 网络的安全技术无法适应工业控制系统。本文将从工业控制的角度，分析工业控制系统安全的特殊性，并提出针对工控系统安全的综合解决方案。

关键字：工业控制系统 安全 两化融合 SCADA 工业协议

一、工业控制系统介绍

1、工业控制系统

工业控制系统 (Industrial Control Systems, ICS)，由几种不同类型的控制系统组成，包括监控数据采集系统 (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) 和远程测控单元 (RTU) 等，广泛运用于石油、石化、冶金、电力、燃气、煤矿、烟草以及市政等领域，用于控制关键生产设备的运行。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。

国外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。

2、工业控制网络的发展

现场总线技术作为传统的数据通讯方式广泛地应用在工业控制中。经过多年的争论和斗争后，现场总线国际标准 IEC - 61158 放弃了其制定单一现场总线标准的初衷，最终发布了包括 10 种类型总线的国际标准。因此，各大总线各具特点、不可互相替代的局面得到世界工控界的认可。多种现场总线协议和标准的共存，意味着在各总线之间实现相互操作、相互兼容的代价是高昂的，且困难的。

目前控制器甚至远程 I/O 支持以太网的功能越来越强,在有些控制器和远程 I/O 模块中已经集成了 Web 服务器,从而允许信息层的用户也可以和控制层的用户一样直接获取控制器和远程 I/O 模块中的当前状态值。采用以太网架构和开放的软件系统的制造企业也被称为“数字工厂”。此外,通过 Internet 可以实现对工业生产过程的实时远程监控,将实时生产数据与 ERP 系统以及实时的用户需求结合起来,使生产不只是面向订单的生产,而是直接面向机会和市场的“电子制造”,从而使企业能够适应经济全球化的要求。

3、 工业网络协议

目前,市场上具有以太网接口和 TCP/IP 协议的设备很多。以太网技术的高速发展及它的 80%的市场占有率和现场总线的明显缺陷,促使工控领域的各大厂商纷纷研发出适合自己工控产品且兼容性强的工业以太网。其中应用较为广泛的工业以太网之一是德国西门子公司研发的 SIMATIC NET 工业以太网;拥有丰富的工业应用经验的施耐德电气公司,也推出了一系列完整、以 TCP/IP 以太网为基础、对用户高度友好的服务,专门用于工业控制领域。自 1979 年以来, Modbus 就已成为工业领域串行链路协议方面的事实标准,它已经在数以百万计的自动化设备中作为通信协议得到了应用。由于它的成功应用,互联网社团给 Modbus 协议保留了 TCP 502 端口作为专用端口。通过 Modbus 消息可以在 TCP/IP 以太网和互联网上交换自动化数据,以及其它各种应用(文件交换、网页、电子邮件等等)。

其它知名的工控硬件厂商,也提供了支持以太网接口的通信协议。如 Rockwell 支持的 EtherNet/IP 协议,GE 支持的 SRTP TCP/IP、EGD、MODBUS TCP/IP 协议,浙大中控、和利时支持的 OPC 协议等。如今,在同一个网络上,无需任何接口就可以有机地融合信息技术与自动化已成为现实。

二、 工业控制系统的安全现状分析

1、 工业控制系统的安全威胁：

一旦工业控制系统信息安全出现漏洞,将对工业生产运行和国家经济安全造成重大隐患。随着计算机和网络技术的发展,特别是信息化与工业化深度融合以及物联网的快速发展,工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件,以各种方式与互联网等公共网络连接,病毒、木马等威胁正在向工业控制系统扩散,工业控制系统信息安全问题日益突出。“震网”病毒事件,充分反映出工业控制系统信息安全面临着严峻的形势。与此同时,我国工业控制系统信息安全管理工作中仍存在不少问题,主要是对工业控制系统信息安全问题重视不够,管理制度不健全,相关标准规范缺失,技术防护措施不到位,安全防护能力和应急处置能力不高等,威胁着工业生产安全和社会正常运转。

2、 工业控制网络的安全隐患：

2.1、 非授权使用：入侵

系统被入侵是系统常见的一种安全隐患。黑客侵入计算机和网络可以非法使用计算机和网络资源，甚至是完全掌控计算机和网络。

控制网络的计算机终端和网络往往可以控制或影响诸如大型化工装置、公用工程设备，甚至核电站安全系统等大型工程化设备。黑客一旦控制该系统，对系统造成一些参数的修改，就可能导致生产运行的瘫痪，就意味着可能利用被感染的控制中心系统破坏生产过程、切断整个城市的供电系统、恶意污染饮用水甚至是破坏核电站的正常运行。随着近些年来越来越多的控制网络接入到互联网当中，这种可能就越来越大。

2.2、 拒绝服务攻击

受到拒绝服务攻击是一种危害很大的安全隐患。常见的流量型攻击如 Ping Flooding、UDP Flooding 等，以及常见的连接型攻击如 SYN Flooding、ACK Flooding 等，通过消耗系统的资源，如网络带宽、连接数、CPU 处理能力等使得正常的服务功能无法进行。拒绝服务攻击难以防范的原因是它的攻击对象非常普遍，从服务器到各种网络设备如路由器、交换机、防火墙等都可以被拒绝服务攻击。

控制网络一旦遭受严重的拒绝服务攻击就会导致操作站的服务瘫痪，与控制系统的通信完全中断等。可以想象，受到拒绝服务攻击后的控制网络可能导致网络中所有操作站和监控终端无法进行实时监控，其后果是非常严重的。而传统的安全技术对拒绝服务攻击几乎不可避免，缺乏有效的手段来解决。

2.3、 病毒攻击：

Stuxnet 蠕虫病毒对西门子公司的数据采集与监控系统 SIMATIC 进行攻击，Stuxnet 蠕虫（俗称“震网”）在 2010 年 7 月开始爆发。它利用了微软操作系统中至少 4 个漏洞，其中有 3 个全新的零日漏洞；伪造驱动程序的数字签名；通过一套完整的入侵和传播流程，突破工业专用局域网的物理限制；利用 SIMATIC 系统的 2 个漏洞，对其开展破坏性攻击。它是第一个直接破坏现实世界中工业基础设施的恶意代码。据赛门铁克公司的统计，目前全球已有约 45000 个网络被该蠕虫感染，其中 60% 的受害主机位于伊朗境内。伊朗政府已经确认该国的布什尔核电站遭到 Stuxnet 蠕虫的攻击。

为此工信部于 2011 年 10 月份发布了《关于加强工业控制系统信息安全管理的通知》工信部协[2011]451 号文件，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。

Stuxnet 是一个专门针对特定工业控制系统的威胁，Stuxnet 的终极目标是帮助袭击者实现破坏可编程逻辑控制器(plc)的程序，以及控制网络的边界。伊朗已经检测到了被专家们认为是基于“震网”病毒的“Duqu”计算机病毒。专家们表示，尽管“震网”病毒意在破坏工业控制系统，并且可能已经摧毁了伊朗的一些用于铀浓缩的离心机，但是“Duqu”病毒

似乎专为收集数据而来，其目的是使未来发动网络袭击变得更加容易。赛门铁克公司称：“‘Duqu’病毒基本上是未来‘震网’式袭击的预兆。”该公司在发布的报告中指出，这个变种新病毒的目的不是破坏工业控制系统，而是获得远距离的进入能力。

2.4、 开放式 OPC 接口的安全性

OPC 全称是 Object Linking and Embedding (OLE) for Process Control，它的出现为基于 Windows 的应用程序和现场过程控制应用建立了桥梁。在过去，为了存取现场设备的数据信息，每一个应用软件开发商都需要编写专用的接口函数。现场设备的种类繁多，且产品的不断升级，在给用户和软件开发商带来了巨大的工作负担也不能满足工作的实际需要，系统集成商和开发商迫切需要一种具有高效性、可靠性、开放性、可互操作性的即插即用的设备驱动程序。在这种情况下，OPC 标准应运而生。OPC 标准以微软公司的 OLE 技术为基础，它的制定是通过提供一套标准的 OLE/COM 接口完成的，在 OPC 技术中使用的是 OLE 2 技术，OLE 标准允许多台微机之间交换文档、图形等对象。

OPC 因为其基于 DCOM 技术，在进行数据通讯时，为了响应请求，操作系统就会为开放从 1024 到 5000 动态端口使用，所以 IT 部门在使用普通商用防火墙时根本没有任何意义。对于一般防火墙更无法进行剖析，而使 OPC 客户端可以轻易对 OPC 服务器数据项进行读写，一旦黑客对客户端电脑取得控制权，控制系统就面临很大风险。黑客可以很轻松的获得系统所开放的端口，获取/伪装管理员身份，对系统进行恶意破坏，影响企业的正常生产运营。

3、 SCADA 系统软件的漏洞：

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD），在 2011 年 CNVD 收录了 100 余个对我国影响广泛的工业控制系统软件安全漏洞，较 2010 年大幅增长近 10 倍，涉及西门子、北京三维力控和北京亚控等国内外知名工业控制系统制造商的产品。相关企业虽然积极配合 CNCERT 处理了安全漏洞，但这些漏洞可能被黑客或恶意软件利用。

4、 与商用网络的对比：

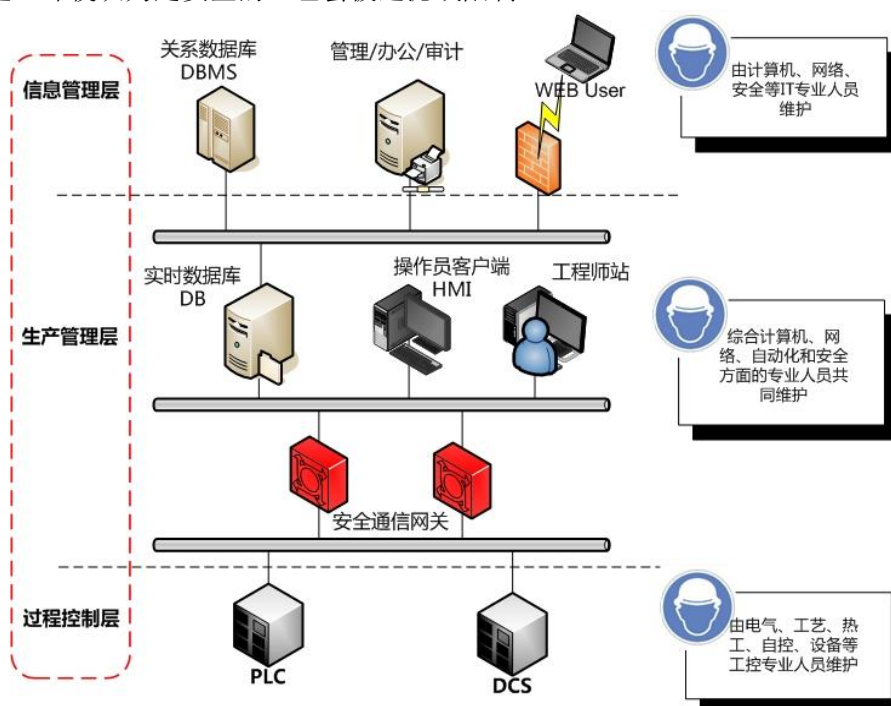
在商用网络里可以存在病毒，几乎每天都有新的补丁出现，计算机可能会死机、暂停，而这些如果发生在控制网络里，带来的危险和影响几乎是不可想象的。为了保证生产安全，在极端情况下，即便将控制网络与信息网络断开，停止与信息网络交换数据也要保证控制系统的安全。因此，过程生产的连续不间断的高可靠性，要求控制网络具备更高的安全性。

另外，从数据安全角度来看，商用网络往往对数据的私密性要求很高，要防止信息的泄露，而控制网络强调的是数据的可靠性。另外，商用网络的应用数据类型极其复杂，传输的通信标准多样化，如 HTTP、SMTP、FTP、SOAP 等；而控制网络的应用数据类型相对单一，以过程数据为主，传输的通信标准以工业通信标准为主，如 OPC、Modbus 等。

三、 工业控制系统安全测试、评估及目标

1、 保证安全管理可控性

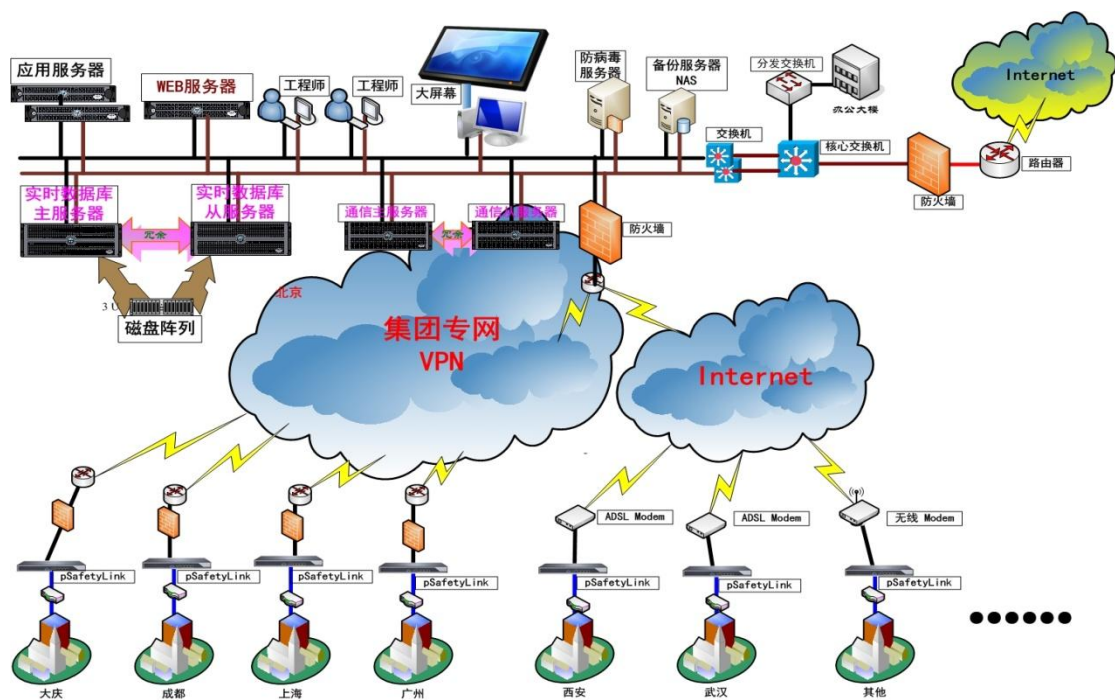
目前，许多工业控制系统的用户将已经开始关注，并试图寻求最好的安全管理办法。但是在确保控制系统的意见时，一个常见的误区是，他们把主要工作在信息技术（IT）领域的专业人士。做过控制系统工程的人都知道，这两个世界是截然不同的。最明显的区别是典型的优先权问题，IT 人士在部署安全策略时，在网络畅通的情况下，尽量保证网络安全。而工业控制网则正相反，工业控制网络要求传输“绝对、必需的”业务，与业务不相关的数据均不允许通过，即使认为是安全的，也会被过滤或限制。



2、 整体防护策略

也许应对一个工厂或是一个应用程序已经绰绰有余，但许多使用者需要管理的是几十甚至是几百个工厂的安全防护体系。

例如，昆仑燃气公司在全国各地拥有 100 多家子公司，覆盖近 100 座城市，供气能力达 50 亿方以上。为了保护其 PLC 的监控系统、数据采集(SCADA)系统和分布式控制系统(DCS)，液化气集团很早就认识到它必须建立网络防护体系以应对可能的网络威胁。虽然他们已经实施了复杂的防火墙规则和嵌入式监控系统，但信息化评估结果显示，他们需要更多的 SCADA 监测和工业网络保护。



四、 工业控制系统安全防护策略：

工业控制系统的安全防护需要从每一个细节进行考虑，从现场 I/O 设备、控制器，到操作站的计算机操作系统，工业控制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及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架构，分别采取不同的对应手段，构筑从整体到细节的立体防御体系。

1、 通用防火墙在工业控制系统中的适用范围：

网络防火墙通过设置不同的安全规则，来控制设备或系统之间的数据流，在实际应用中，主要用于分析与互联网连接的 TCP/IP 协议簇。防火墙在网络中使用的前提是必须保证网络的连通性，通过规则设置和协议分析，来限制和过滤那些对管理比较敏感、不安全的信息，防止未经授权的访问。

由于工业控制与网络商用网络的差异，常规的 IT 网络安全设置规则，用在控制网络上就会存在很多局限性。因此，正确地设计、配置和维护硬件防火墙的规则，才可以保护工业控制网络系统的安全环境。建议设置的特殊规则包括：

■ 超文本传输协议(HTTP)

一般来说，HTTP 不应该被允许从企业管理网透过进入控制网络，因为他们带来重要的安全风险。如果 HTTP 服务到控制网络是绝对必需的，那么在防火墙中需要通过 HTTP 代理配置来阻止所有执行脚本和 Java 应用程序，而且建议特定的设备使用 HTTPS 更安全。

■ 限制文件传输协议(FTP)

FTP 和其它需要的文件传输协议(TFTP)用于在设备之间传输、交换文件，包括许多 SCADA

系统、DCS、PLC、RTU 等系统中都有应用。不幸的是，FTP 协议并没有任何安全原则，登录密码不加密，有些 FTP 为了实现历史缓冲区而出现溢出的漏洞，所以配置防火墙规则应阻塞其通信。如果 FTP 通讯不能被要求禁止，通过 FTP 输出数据时，应额外增加多个特征码授权认证，并提供加密的通信隧道。

■ 简单邮件传输协议(SMTP)

SMTP 在互联网上是主要的电子邮件传输协议。电子邮件经常包含恶意软件，所以不应该被允许以任何控制网络设备接收电子邮件，SMTP 邮件主要用于从控制网络到办公网络之间输出发送报警信息。

■ 简单网络管理协议(SNMP)

SNMP(单网络管理协议)是用来为网络管理服务中心，提供与管理控制台与设备之间的监控与管理的会话规则，如路由器、网络设备、打印机和 PLC。虽然为维持一个网络，SNMP 是一个非常有用的服务，在安全方面却很软弱。SNMP2.0 和 SNMP1.0 的安全机制比较脆弱，通信不加密，所有通信字符串和数据都以明文形式发送。攻击者一旦捕获了网络通信，就可以利用各种嗅探工具直接获取通信字符串，即使用户改变了通信字符串的默认值也无济于事。第三版本具相当的安全性，但却没有被广泛使用。从控制网中使用 SNMP V1 和 V2 的命令，都应被禁止，除非它是在一个完全独立的信任管理网络。即使设备已经支持 SNMP3.0，许多厂商使用的还是标准的通信字符串，这些字符串对黑客组织来说根本不是秘密。因此，虽然 SNMP3.0 比以前的版本提供了更多的安全特性，如果配置不当，其实际效果仍旧有限。

■ 分布式组件对象模型(DCOM)

在过程控制中，OLE 和 ProfiNet(OPC)是使用 DCOM 的，它运用了微软的远程过程调用(RPC)服务。该服务有很多的漏洞，很多病毒都会利用这个弱点获取系统权限。此外，OPC 也利用 DCOM，动态地打开范围内的任意端口(1024 – 65535)，这在防火墙中过滤是非常困难的。通用防火墙无法完成对 OPC 协议的规则限制，如果必须需要该协议，则要求控制网络、网络之间必须物理分开，将控制网络和企业网络横向隔离。

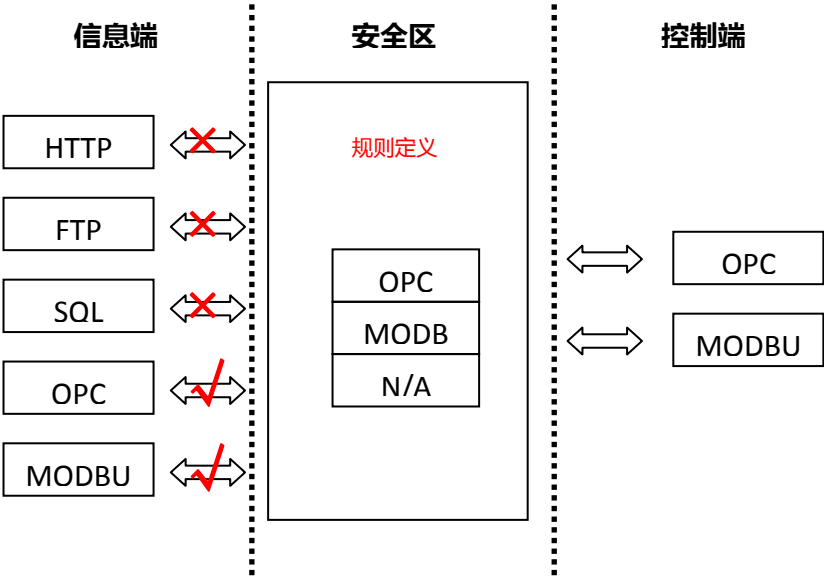
■ SCADA 和工业协议

SCADA 和工业协议，如 MODBUS/ TCP, EtherNet/ IP 和 DNP3 等被大量使用。不幸的是，这些协议在设计时，没有安全加密机制，通常也不会要求任何认证，便可以在远程对一个控制装置执行命令。这些协议应该只被允许在控制网络单向传输，不准许在办公网络穿透到控制网络。

能够完成以上功能的工业防火墙或者安全路由器，通常被部署在具有以太网接口的 I/O 设备和控制器上，从而避免因设备联网而造成的病毒攻击或广播风暴，还可以避免各子系统间的病毒攻击和干扰。

2、 基于“白名单”的安全机制

白名单主动防御技术是通过提前计划好的协议规则来限制网络数据的交换,在控制网到信息网之间进行动态行为判断。通过对约定协议的特征分析和端口限制的方法,从根源上节制未知恶意软件的运行和传播。



“白名单”安全机制是一种安全管理规范,不仅应用于防火墙软件的设置规则,也是在实际管理中要遵循的原则,例如在对设备和计算机进行实际操作时,需要使用指定的笔记本、U 盘等,管理人员只信任可识别的身份,未经授权的行为将被拒绝。

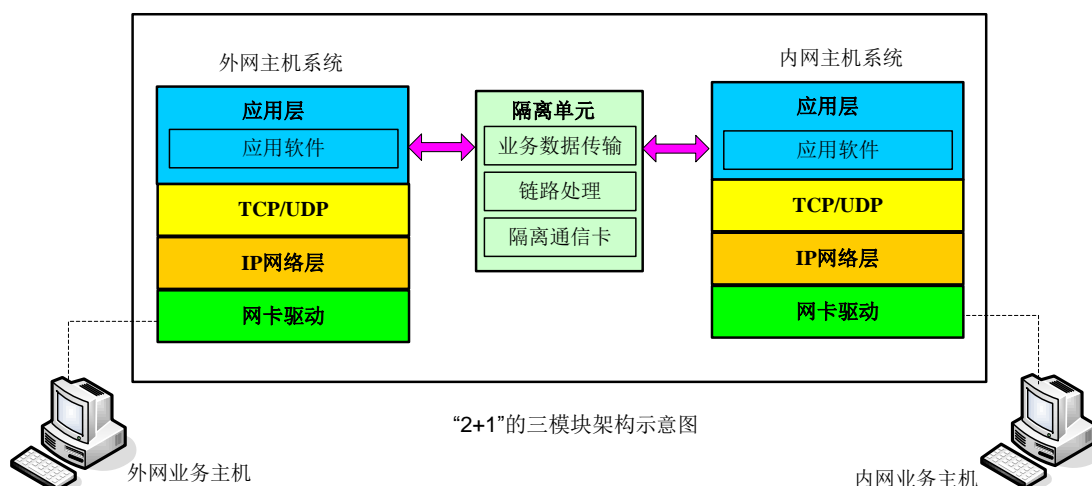
3、网络物理隔离

网络物理隔离类技术诞生较早,最初是用来解决涉密网络与非涉密网络之间的安全数据交换问题。后来,网络物理隔离由于其高安全性,开始被广泛应用于政府、军队、电力、铁道、金融、银行、证券、保险、税务、海关、民航、社保等多个行业部门,其主要功能支持:文件数据交换、HTTP 访问、WWW 服务、FTP 访问、收发电子邮件、关系数据库同步以及 TCP/UDP 定制等。

在工业控制领域,网络物理隔离也开始得到应用和推广。通常采用“2+1”的三模块架构,内置双主机系统,隔离单元通过总线技术建立安全通道以安全地实现快速数据交换。网络物理隔离提供的应用专门针对控制网络的安全防护,因此它只提供控制网络常用通信功能如 OPC、Modbus 等,而不提供通用互联网功能,因此更适合于控制网络与办公网络,以及控制网络各独立子系统之间的隔离。其主要特点如下:

- 独立的运算单元和存储单元,各自运行独立的操作系统和应用系统;
- 安全隔离区采用私有加密的数据交互技术,数据交换不依靠TCP/IP协议;
- 工业通信协议,OPC/MODBUS/60870-5-104/等;
- 与信息层上传数据时,可实现断线缓存、续传;
- 实时数据交换,延时时间小于1ms;
- 访问控制
- 身份认证

■ 安全审计与日志管理



4、 入侵预防系统

入侵预防系统(IPS: Intrusion Prevention System)是电脑网络安全设施，是对防病毒软件（Antivirus Programs）和防火墙的补充。入侵预防系统是一部能够监视网络或网络设备的网络资料传输行为的计算机网络安全设备，能够即时的中断、调整或隔离一些不正常或是具有伤害性的网络资料传输行为。

在 ISO/OSI 网络层次模型中，防火墙主要在第二到第四层起作用，它的作用在第四到第七层一般很微弱。而除病毒软体主要在第五到第七层起作用。为了弥补防火墙和除病毒软件二者在第四到第五层之间留下的空档，几年前，工业界已经有入侵侦查系统(IDS: Intrusion Detection System)投入使用。入侵侦查系统在发现异常情况及时向网路安全管理人员或防火墙系统发出警报。可惜这时灾害往往已经形成。虽然，亡羊补牢，尤未为晚，但是，防卫机制最好应该是在危害形成之前先期起作用。随后应运而生的入侵响应系统(IRS: Intrusion Response Systems) 作为对入侵侦查系统的补充能够在发现入侵时，迅速作出反应，并自动采取阻止措施。而入侵预防系统则作为二者的进一步发展，汲取了二者的长处。

入侵预防系统也像入侵侦查系统一样，专门深入网路数据内部，查找它所认识的攻击代码特征，过滤有害数据流，丢弃有害数据包，并进行记载，以便事后分析。

由于防火墙和杀毒软件对已存在危险进行控制，属于“亡羊补牢”的滞后手段，管理人员需要对其进行定期维护和更新。入侵预防系统则提供了提前预警的报告手段，以便于管理人员采取必要应对措施。

5、 建立私有云

构建满足工业控制系统的全厂级风险识别模型，除了需要细化工业控制系统的风险因素，还需要建立基于工业控制系统的安全管理域，实施分等级的基线建设，兼顾包括终端与链路、威胁与异常、安全与可用性等综合因素的功能考虑。

安全管理私有云的建立要求包括：

- 方便地对整个系统里所有安全设备模块、控制器和工作站，进行部署、监控和管理；
- 规则辅助生成，指导用户方便快捷地从权限、授权管理报告中，创建防火墙的规则；
- 自动阻止并报告任何与系统流量不匹配的规则；
- 接收、处理和记录由安全模块所上传的报警信息；
- 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；
- 可视化配置、组态；
- 安全事件搜索、跟踪和预处理能力。

五、 总结：

未来的信息安全技术必须要与工业控制系统相互融合，而不仅仅是简单的集成，在制订工业控制系统安全标准的时候，就需要考虑到可能存在的各种网络与信息安全隐患。随着以太网技术在工业控制网络的应用，以及国家对“两化”整合的继续推进，未来的工业控制系统将会融合更多的先进的信息安全技术，如可信计算、云安全等。工业控制网络将会发展成基于可信计算的可信网络平台。工业控制网络中的可信设备通过网络搜集和验证接入者的完整性信息，依据安全策略对这些信息进行评估，从而决定是否允许接入，以确保工业控制网络的安全性。同时，可信计算还可以协助工业控制网络建立合理的用户控制策略，并依据用户的行为分析数据来建立统一的用户信任管理模型。工业控制网络还将会融合云安全技术，借助于云端的数据信息，在病毒未危害到设备时就提前阻止危害发生。云端数据信息的实时更新将会是物联网时代应对病毒的有效手段。

参考文献：

- 1、 DRAFT Guide to Industrial Control Systems (ICS) Security
- 2、 关于加强工业控制系统信息安全管理的通知
- 3、 工业控制系统安全风险分析（金山网络张帅）
- 4、 工业网络安全（Security）发表时间：2012-3-8 王聪 来源：e-works
- 5、 工业以太网在实际应用中安全对策解决方案发布 来源：ducuimei
- 6、 工业控制系统网络安全防护策略
- 7、 施耐德 Connexium 工业以太网产品目录及参数
- 8、 石化 MES 控制网络安全分析与实践
- 9、 2011 年我国互联网网络安全态势综述 CNVD