



实时数据库系统数据安全采集方案

尚振阳¹, 杨瑞先²

(1. 中国石油天然气股份有限公司吉林石化分公司, 吉林 吉林 132022;

2. 吉化集团信息网络技术有限公司, 吉林 吉林 132022)

摘要: 基于中国石油炼油与化工运行系统(MES)在下属企业的应用现状以及实时数据库模块的数据采集方案, 详细分析了“两网融合”导致的生产装置自控系统(DCS、PLC)面临病毒、攻击和非法入侵等安全风险。最后, 参考国内现有的一些工控隔离产品, 提出一套完整、可行、安全的解决方案, 对炼化企业 MES 系统实时数据库模块的实施具有很高的参考价值。

关键词: MES; 实时数据库; OPC 与计算机病毒; DCS/PLC 系统安全

中图分类号: TN918

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016276

Real time database system data security collection scheme

SHANG Zhenyang¹, YANG Ruixian²

1. Petro China Jilin Petrochemical Compang, Jilin 132022, China

2. JihuaGroup Information Network Technology Co., Ltd., Jilin 132022, China

Abstract: With application status of the China Petroleum Refining and Chemicals run system MES (manufacturing execution system) in subordinate enterprises as well as the data acquisition interface program in real-time database module, the security risks such as virus, attacks and illegal invasions in production unit automatic control system (DCS, PLC) because of the “two-network integration” were analyzed. Finally, referring to some of the existing domestic industrial insulation products, a complete, viable and secure solution, which has a high reference value for the implementation of petrochemical enterprises MES system real-time database module was proposed.

Key words: MES, real-time database, OPC and computer virus, DCS/PLC system security

1 引言

当前, 信息化已成为现代企业提高管理效率、降低管理成本的有效手段, 并迅速地形成一种趋势。作为中国石油信息化总体建设的重要组成部分, MES (manufacturing execution system) 具体业务流程包括生产计划、生产调度、生产计量、生产操作、质量检验、生产统计、工艺技术管理、生产绩效管理、设备管理、生产受控等。

MES 的成功应用极大地促进了企业生产过程和业务流程的优化, 加强了对整个生产执行过程的监督和控制, 提高了生产的稳定性, 降低了生产成本, 减少了质量浪费, 满足了企业的业务发展战略需求。但是, 管理网与生产网的“两网融合”, 间接地开放原本封闭的生产网, 导致 DCS/PLC 系统直接面临病毒、攻击和非法入侵等安全风险, 威胁企业生产的安全隐患日益突出。MES 采集生产装置实时数据的同时, 必须保证 DCS/PLC 系统安全, 避免造成 DCS/PLC 系统



性能下降甚至瘫痪,这也是 MES 实施的先决条件。

2 MES 的实时数据采集

根据中国石油各地区公司生产装置(单元)广泛应用 DCS/PLC 系统的现状以及国外的成功实施案例,采用标准的 OPC(OLE for process control)接口技术,实现 MES 系统实时数据库模块的数据采集。

2.1 OPC 技术

OPC 是微软(Microsoft)公司的对象链接和嵌入 OLE/COM 技术在过程控制方面的应用,为工业控制领域提供了标准的数据访问机制,旨在作为基于 Windows 的应用软件和过程控制硬件的连接桥梁。随着 OPC 基金会的成立,OPC 技术逐渐地成为工控行业的一个国际标准。

OPC 技术扩展了硬件设备的概念,只要符合 OPC 服务器的规范,OPC 客户都可以与之进行数据交换,硬件厂商只需要编写一套驱动程序就可以满足不同用户的需要,软件开发商也无需了解硬件设备的厂商及其硬件实质,只要遵循 OPC 规范,即可随时通过 OPC 接口来获取设备数据,实现应用软件和硬件设备的“即插即用”。

2.2 实施策略

为了保证实时数据库数据采集标准的统一,便于企业对系统的管理、维护、升级,中国石油 MES 项目组在实施实时数据库模块时,采用了标准的 OPC 接口技术实现统一数据采集,利用 DCS/PLC 系统的标准 OPC 服务器,通过 Honeywell(蜜罐)实时数据库 PHD 提供的标准 RDI for

OPC 进行配置和定义,实现 PHD 实时数据采集。

2.3 系统架构

中国石油 MES 的实时数据库模块采用的是 Honeywell 公司的 Uniformance 套件中的 PHD 模块,具体的系统架构如图 1 所示。

2.4 主要接口

尽管中国石油 26 家地区公司 DCS/PLC 的品牌多、型号杂,但由于采取标准的 OPC 接口技术实现的数据采集,接口类别并非十分繁杂。

3 数据采集架构的风险分析

由于炼化企业生产过程的重要性和特殊性,严格要求每一个生产环节都不允许产生纰漏,特别是控制系统必须安全、稳定运行。实时数据库采集 DCS/PLC 系统采集数据,数据采集缓存服务器(Buffer 机)直接与现场装置的 DCS/PLC 系统相连,从而导致 DCS/PLC 系统与外网的连通。这给企业原本封闭的控制系统带来了病毒、非法攻击和入侵等一系列的安全隐患。基于 OPC 服务器的 DCS/PLC 数据采集如图 2 所示。

3.1 OPC 与计算机病毒

OPC 规范的主要目的是统一、标准地描述用户数据来源,OPC 服务器表现为具有一些特定功能的 COM 对象集合,而这些特定功能就是 OPC 规范的技术细节,OPC 技术细节的制定完全是为了满足设备间的互操作性。OPC 服务器对象如图 3 所示。

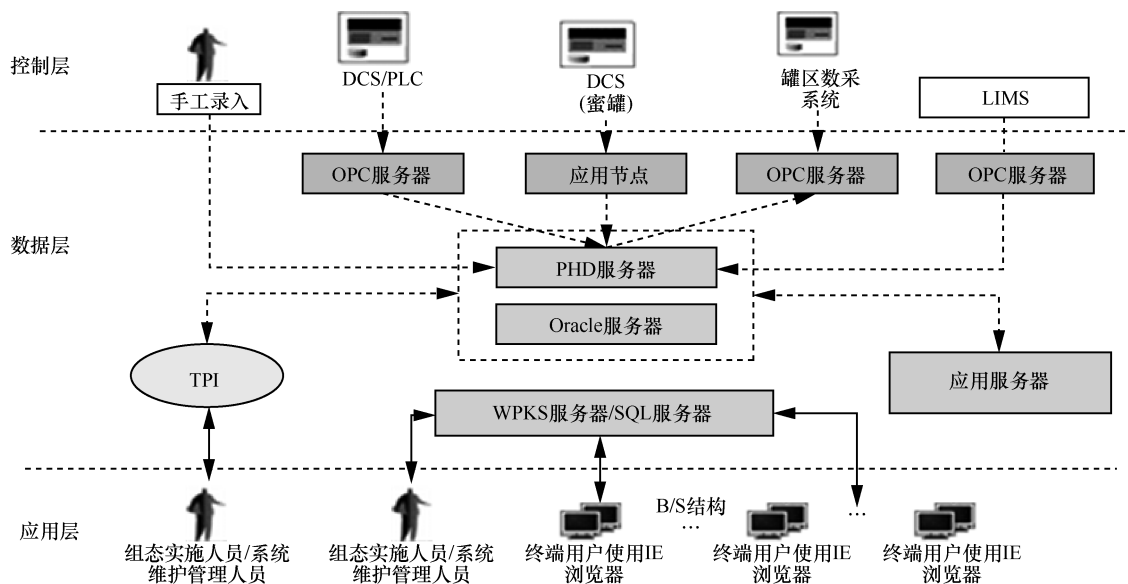


图1 PHD 系统架构

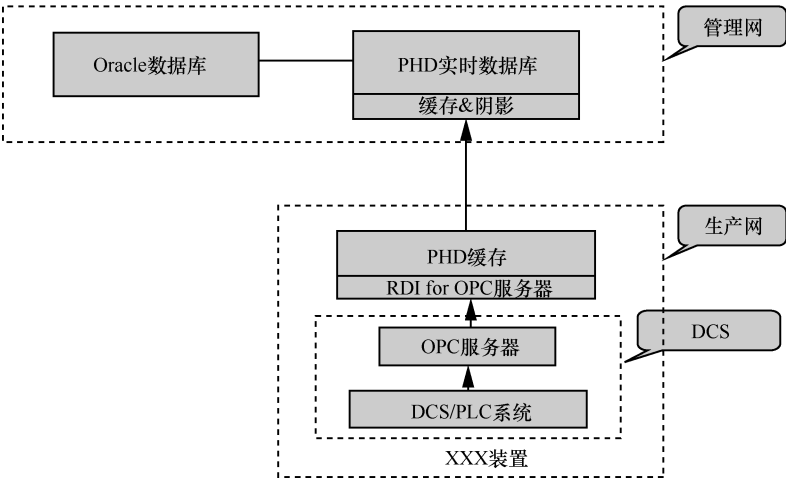


图 2 基于 OPC 服务器的 DCS/PLC 数据采集

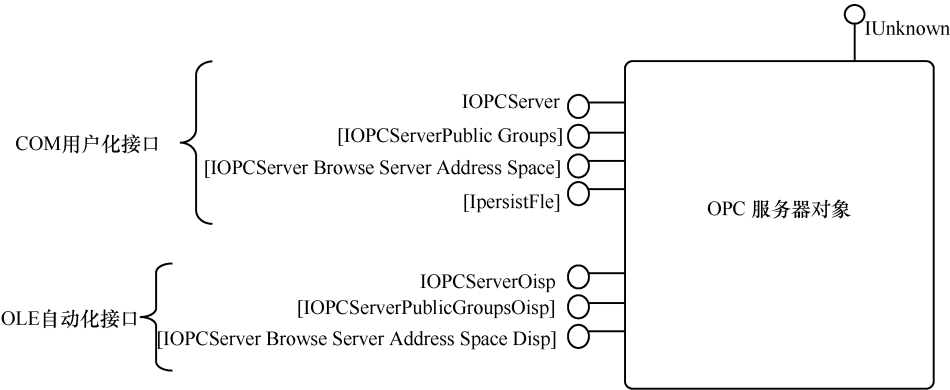


图 3 OPC 服务器对象

OPC 服务器仅仅面向 OPC 服务器的技术细节，基本独立于实时数据源，OPC 服务器的开发过程中，数据的组织结构与数据源属性与具体数据源有关，没有涉及任何计算机病毒的防范，仅需要从用户处获取信息。因此，任何厂商的 OPC 服务器都是为了实现脱离具体设备，没有考虑计算机病毒对 DCS/PLC 系统的影响。

3.2 数据采集的实施风险

目前，主流的 DCS/PLC 系统都运行在 PC+Windows 平台的环境下，上层应用基本使用 TCP/IP 实现数据交换。

由于 DCS/PLC 系统操作软件的特殊性，操作站的 Windows 系统不能升级，Microsoft 的各种漏洞补丁不能安装在这些操作站上，否则 DCS/PLC 操作软件不能正常运行；另外，为了保证 DCS/PLC 操作软件的正常运行和效率，DCS/PLC 操作站基本上不安装防病毒软件。

基于 DCS/PLC 系统的特殊性，可以看到突出的安全隐患主要体现在以下方面。

- Windows 操作系统：缺乏安全方面考虑，RPC、cookie 等系统安全漏洞频繁出现，恶意代码通过这些漏洞可获得系统完全控制权，安全事故时有发生。
- TCP/IP：设计基础是相互信任，仅考虑互通互联和资源共享，没有涉及网络中、网际间的安全问题，先天存在致命的安全漏洞，如用户身份鉴别、路由协议鉴别认证。
- 应用软件：面向网络应用，应用软件必须开放相应端口，如，OPC 远程通信 DCOM 协议、完全开放 135 端口，由此导致防火墙、网关等通用网络安全设备丧失防御能力。

炼化 MES 常规数据采集架构如图 4 所示。

例如，冲击波(Worm.Blaster)病毒就是利用 RPC(remote procedure call)漏洞，通过 135 端口攻击计算机。RPC 本身在处理通过 TCP/IP 的消息交换部分有一个漏洞，该漏洞是由于错误地处理格式不正确的消息造成的，会影响到 RPC

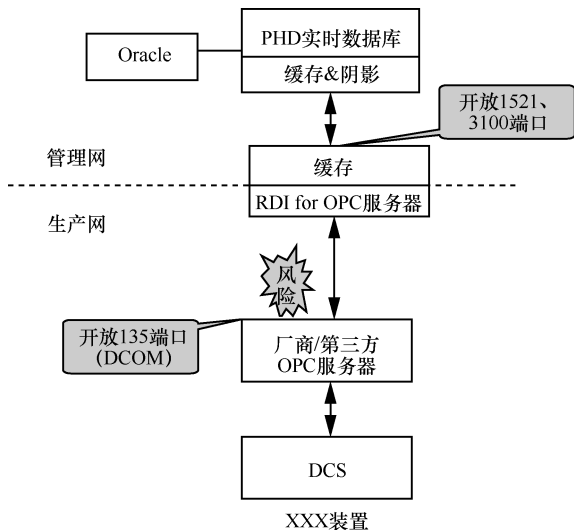


图4 炼化MES常规数据采集架构

与 DCOM 之间的一个接口,接口侦听的端口就是 135。

4 安全隔离的采集方案

4.1 现有措施缺陷

目前管理网和生产网之间,使用了诸多的网络安全措施,如:防火墙、网关等,但由于MES数据采集的实时数据采集基于DCOM(135端口)协议通信,采用防火墙、隔离网关作为安全防护手段,均存在局限性,分析内容见表1。

通常应用的网络安全技术,入侵检测技术(IDS)、虚拟专用网络(VPN)、防病毒、防火墙等,均不能实现网络在OSI 7层上的完全隔离,不能有效保证MES对DCS控制系统不造成安全性风险。

4.2 采集方案设计

吉林石化公司在MES项目实施应用过程中,为了确保DCS/PLC系统安全,在二级分厂的DCS系统与生产网之间部署高安全级别的防护设备:天御6000安全隔离与信息交换系统。MES安全数据采集网络架构如图5所示。

该安全隔离系统由内网关、外网关和硬件隔离控制器

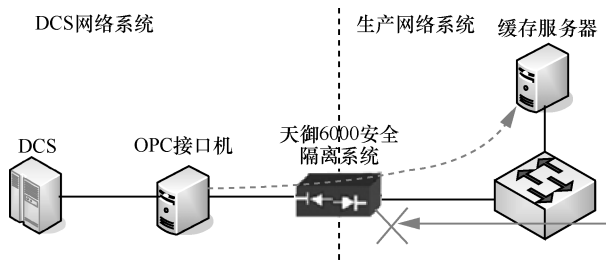


图5 MES系统安全数据采集网络架构

3部分组成,实现两个安全区之间的非网络方式的的安全的数据交换,同一时间点内外网不直接联通。天御6000安全隔离系统硬件架构如图6所示。

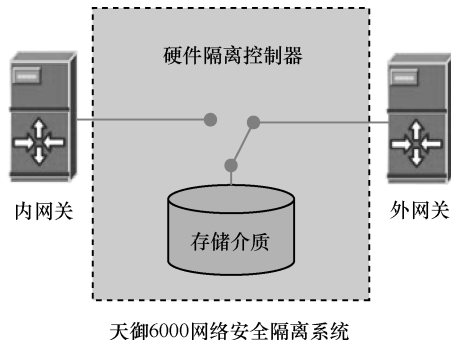


图6 天御6000安全隔离系统硬件架构

该安全隔离系统内、外网关采用RISC专用网络处理器,中间硬件隔离控制器的主要采用专用数字处理芯片构成;硬件隔离控制器通过对RAM的存储转发和电子开关的切换实现安全隔离和单向控制,同时具有对外网数据分组的过滤和阻断功能。安全隔离控制器的硬件框架如图7所示,存储介质主要由双端口RAM和控制器构成,在外网端只有读信号,屏蔽了写信号,安全隔离控制器保证数据只能从一个方向写入存储器从另一个方向读出,从硬件上保证数据的单向传输。

在软件架构上,石化行业安全隔离系统由OPC数据采集模块、安全隔离模块、OPC数据服务模块3部分组

表1 现有安全防护手段的主要局限性

标题	防火墙	隔离网关
工作原理	基于TCP/IP协议体系,以数据分组过滤技术为基础,对内网和外网间、专网与公网间通信信息进行处理,拦截不需要的数据分组,允许需要的数据分组通过	网关主要用于两个协议不同的网络互连,在使用不同协议的网络区域间转换通信协议,对收到的信息重新分组,以适应目的系统的协议需求
主要局限	不能保证通讯放行数据分组的安全性,难以阻止已经感染病毒的程序和文件传输 只能控制网络四层以下的数据分组,无法阻止因系统漏洞带来的攻击,难以有效防范应用层内蠕虫等病毒	网关可根据不同场合融合不同的协议转换技术和网络安全功能,具有重要且独特的保护作用,但仍存在TCP/IP自身协议缺陷 安全网关虽然具有防火墙的功能,具有一定的入侵检测防御、流量控制等功能,但只能实现逻辑上的网络隔离,不能实现物理意义上的网络隔离

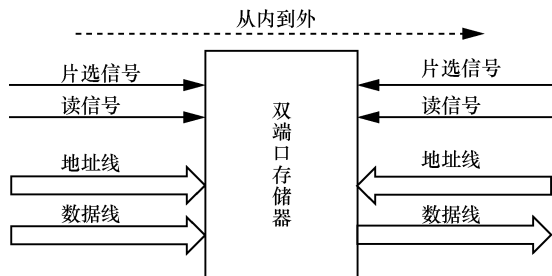


图 7 天御 6000 安全隔离系统单向存储 RAM

成,如图 8 所示。DCS 数据通过 OPC 数据采集模块采集后,转换为自定义协议通过安全隔离模块发送到 OPC 数据服务模块,实现了 OPC 数据安全高效的单向传输,保证了 DCS 不受外来网络的干扰,保证了运行的绝对安全。

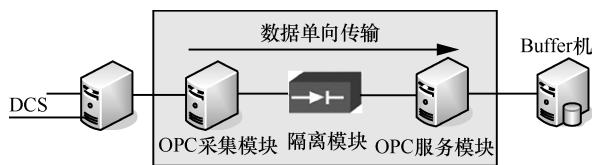


图 8 天御 6000 安全隔离系统软件架构

该安全隔离系统在保证用户生产与管理网安全隔离的情况下,实现安全高效的数据传输;核心功能是提升用户生产网的高安全级别,阻止针对生产网络与工业控制系统的已知攻击和未知攻击,满足各行业对高效率、高可用性和高可靠性的需求。

技术特点主要体现在以下方面。

- 2+1 结构设计,双主机系统+硬件隔离控制器,采用非 Intel 指令集的网络处理器。
- 中间隔离部件通过电子开关实现物理层隔离,同时具有对外网数据分组的过滤和阻断功能;单向存储介质从硬件上保证外网病毒和攻击的入侵。
- 设备具有安全、固化的操作系统,采用裁剪的嵌入式 Linux 内核,规避 Windows 系统缺陷。
- 内、外网之间采用私有通信协议(非 TCP/IP)实现数据转发;避免了协议漏洞。
- 采用双电源设计支持双机热备份,保证设备的安全、可靠、稳定运行。

4.3 性能和安全效果

在测试中,单向安全隔离系统能在 15 s 时延的时间范围内能达到 25 000~30 000 点的数据采集能力,天御 6000 单向安全在实际应用中达到了 32 000 点的采集能力。在

安全方面,由于单向网络安全隔离系统的物理隔离性能,安全扫描软件探测不到被保护的 DCS 主机。

隔离设备接入前,用专业扫描软件绿盟科技远程安全评估系统可以扫描到 DCS 主机并扫出主机的相关漏洞;离设备接入后,扫描设备不能发现 DCS 主机。

4.4 发展方向和趋势

工业和信息化部下发的《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)中有关明确重点领域工业控制系统信息安全管理要求,断开工业控制系统同公共网络之间的所有不必要连接。对确实需要的连接,系统运营单位要逐一进行登记,采取单向隔离、防火墙等措施加以防护,并定期进行风险评估,不断完善防范措施。

因此,在网络安全日益严酷的环境下,按照国家相关法规要求,MES 采集生产装置的实时数据,需要制定安全防护方案。而防火墙等采用逻辑隔离的方案不能从根本上解决问题,采用物理隔离的技术解决两个不同安全域网络的互联问题,完善工控系统安全防护已成为一个刻不容缓的课题和发展趋势。

5 结束语

为了确保 DCS 的安全,吉林石化公司在 MES 的实施应用过程中,通过部署天御 6000 安全隔离与信息交换系统,实现 DCS 到生产网络的数据单向传输,仅允许 DCS 数据单向传送到生产网,生产网到 DCS 的一切网络主动请求均被拒绝;完全抵御来自生产网络中的病毒、黑客或恶意代码等对 DCS 网络的攻击及破坏。

(1)工作原理上,应用跨平台操作系统、非 TCP/IP 专有通信协议、单向数据传输 3 项核心技术,针对生产网与管理网“两网融合”的安全隐患,提供了从根本上有效解决 MES 系统安全问题的解决方案。

(2)实施过程中,不改变现有 MES 数据采集架构,不更改阴影和 OPC 服务器配置,采用无扰接入的工作方式实现产品接入,不影响 DCS 正常运行,具备“即插即用”的显著特点。

(3)应用效果上,通过使用天御 6000,有效隔离生产网与管理网,阻止对生产网的非法攻击、黑客入侵、病毒与恶意代码,规避了“两网融合”的安全隐患,保障 DCS 安全运行,基于嵌入式系统的稳定性和专业性,提高整个系统的安全性与稳定性。



参考文献:

- [1] 崔振伟, 王华. PHD 实时数据库在 MES 中的应用[J]. 石油规划设计, 2009, 20(4): 34-37.
- CUI Z W, WANG H. The application of PHD real-time database in the MES [J]. Petroleum Planning and Design, 2009, 20(4): 34-37.
- [2] 黄至辉. 基于霍尼韦尔的制造执行系统可靠性增长工程理论及技术研究[J]. 计算机技术与发展, 2009(6): 19-22.
- HUANG Z H. The theory and techniques of Honeywell's manufacturing execution system reliability growth engineering [J]. Computer Technology and Development, 2009 (06): 19-22.
- [3] 毛国栋. 流程型制造业企业的 MES 系统设计和实现[J]. 电脑开发与应用, 2009, 22(4): 52-55.
- MAO G D. The design and implementation of process manufacturing enterprises MES [J]. Computer Development & Applications, 2009, 22(4): 52-55.
- [4] 肖波, 叶文华. 工装 MES 生产调度和进度跟踪模块的研究与开发[J]. 机械制造与自动化, 2009(2): 21-23.
- XIAO B, YE W H. The research and development of tooling MES production scheduling and progress tracking module [J]. Machine Building & Automation, 2009(2): 21-23.
- [5] 刘羽飞. 钢铁 MES 系统的设计与实现 [D]. 上海: 上海交通大学, 2012.
- LIU Y F. The design and realization of steel MES system [D]. Shanghai: Shanghai Jiaotong University, 2012.
- [6] 李良才. 实时数据库安全访问的研究 [D]. 武汉: 华中科技大学, 2015.
- LI L C. The research of the access to the real-time database security [D]. Wuhan: Huazhong University of Science and Technology, 2015.
- [7] 剑思庭. 浅谈实时数据库安全性 [J]. 可编程控制器与工厂自动化, 2011(9): 28.
- JIAN S T. Talking something about the real-time database security [J]. PLC and factory automation, 2011(9): 28.
- [8] 张继永. 网络隔离技术与信息安全 [J]. 中国信息界, 2010(9): 25-26.
- ZHANG J Y. The network isolation technology and information security [J]. China Information Times, 2010(9): 25-26.

[作者简介]



尚振阳(1965-),男,中国石油天然气股份有限公司吉林石化分公司信息管理部副经理、高级工程师,负责公司信息化项目建设及维护工作,主要从事信息管理系统开发及实施、工业数据采集等技术研究工作。



杨瑞先(1979-),女,吉化集团信息网络技术有限公司高级工程师,主要从事工业实时数据库方向研究与 MES 项目实施工作。