工业控制网络安全模型研究*)

王 浩 吴中福 王 平

(重庆大学计算机学院 重庆 400044) (重庆邮电大学自动化学院 重庆 400065)

摘 要 为了减少产品费用和提高生产效率,更多的专用网络被连入IT网络,或更多的IT技术被应用到工业控制网络系统中,网络安全成为一个重要的问题。工业控制网络系统作为国家基础设施的重要组成,一旦受到攻击和破坏,其影响将是灾难性的。因此,保护工业控制网络系统的安全、防御各种攻击和破坏是关系到国家安全的重要内容。本论文结合中国第一个工业以太网标准《用于测量与控制系统的EPA通信标准》,建立了一般的工业控制网络体系结构,研究分析了它的安全威胁,提出工业控制网络的安全要求,构建了基于区域安全的DMZ模型,最后用UML描述了该模型。

关键词 工业控制网络,威胁,安全要求,DMZ模型

Research on Security Model for Industrial Control Networks

WANG Hao WU Zhong-Fu WANG Ping

(College of Computer Science, Chongqing University, Chongqing 400044)

(College of Automation, Chongqing University of Posts and Telecomms, Chongqing 400065)

Abstract In order to reduce production cost and improve productivity, more proprietary networks is interconnected to IT networks, or more IT technologies are applied to industrial automation systems, network security become a significant problem. Industrial control networks become important component of national infrastructure, when it is attacked or broken, its impact is calamity. Therefore, protecting the security of industrial control networks and defending kinds of attacks and threats is the key contents of nation security. Combining the first Chinese industrial Ethernet standard, Standard for Digital Data Communication for EPA-based Industrial Control Systems, This paper builds general industrial control networks architecture, researches and analyzes threats to it, advances security requirements and proposes DMZ model based security zone, finally depict the model with UML.

Keywords Industrial control networks, Security threats, Security requirements, DMZ model

1 简介

工业控制网络(ICN)通常是由专用的硬件和通信组成,是单独的,孤立的系统,用于完成控制功能的计算资源(包括CPU计算时间和内存)都是及其有限的。控制系统的设计需要满足可靠性、实时性和灵活性等性能需求。在工业控制网络中,信息安全的问题还没有凸现出来,信息安全通常都不是一个重要的设计要求,因而为了提高性能要求和节约成本,通常都忽略了信息安全的考虑。此外,信息安全目标有时和控制系统的设计和操作相冲突。

然而,由于技术的快速发展,信息化推动工业化进程的加速,越来越多的计算机技术和网络通信技术应用于工业控制网络中,比如:用通用的计算机设备和数据通信设备取代专用的控制和通信设备;嵌入式技术、监视控制与数据采集系统(SCADA)、企业资源计划(ERP)、生产执行系统(MES)等企业信息自动化的应用;企业信息网络与Internet相连等;Windows操作系统和TCP/IP网络协议,等等;同时,更多的信息网络被集成到工业控制网络中,这种集成互联能提高远程数据获取,允许产品处理和对现场设备远程维护的支持,增加商业分析和决策。我国第一个具有自主知识产权的工业以太网标准《用于工业测量与控制系统的EPA通信标准》已纳入IEC 61784-4 PAS-14。这些技术应用的同时,随之带来了控制网路的安全问题,如病毒、信息泄漏和篡改、系统不能使用等等的安全问题。同时,由于工业控制系统也是国家关键基础设施的重要组成部分,关系到国家的战略安全。因此,保障工业控制系统的保密性、完整性和可用性是本模型的主要目标。

工业控制网络区别于信息网络的主要有以下4点:

1)性能和功能需求不同:信息网络设计以高带宽和可靠响应为目标,高的延迟和抖动是可以接受的;控制网络有较高的实时性和较快的时间响应要求,控制系统和实时操作系统都运行在资源受限的设备上,不可能提供安全措施。

2)人机交互响应时间的不同:对于一些控制网络来说,人机交互的响应时间是很关键的。比如在一些紧急操作情况下,不能要求操作员输入密码或其他认证授权信息而阻碍紧急操作的执行。

3)安全体系的不同:对于信息网络,重要数据都存储在服务器上,我们主要保护服务器上的数据的安全;对于控制网络,正好相反,主要是保护工作站、控制器、传感器等节点设备的数据存储和传输的安全。

4)可用性和可靠性需求不同:由于生产制造过程的连续性,现应用于信息系统的补丁、升级和测试等安全措施不能适用于控制系统。控制系统对网络的可用性和可靠性有了更高的要求。

2 控制区域模型

工业控制区域的组成包括:控制回路(传感器、执行器和控制器)、人机接口(HMI)、远程诊断和维护设备。如图1所示。控制回路包含测量传感器、控制硬件、过程执行器和可变

*)国家863项目:用于工业测量与控制系统的EPA标准(项目编号:2003AA412030)。王 浩 博士生,讲师,主要从事网络安全协议,密码算法等方面的研究;吴中福 教授,博士生导师,主要从事网络安全、网格计算等方面的研究;王 平 教授,主要从事工业以太网、网络控制技术等方面的研究。

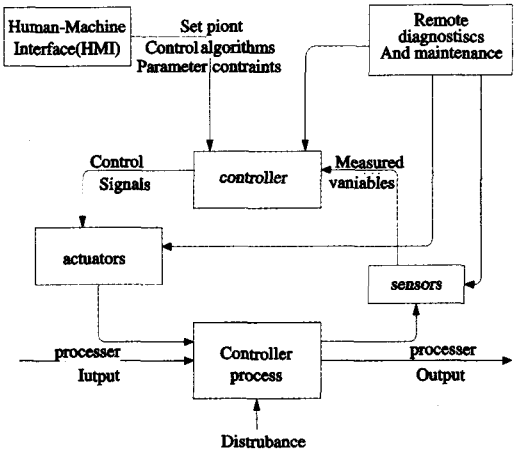

图 1　控制区域一般模型

测量的通信。可变测量从传感器测量得到传输到控制器，控制器解释信号并产生响应控制信号传输给过程执行器。过程变化又会产生新的传感器信号，表示过程的状态，再次被传输到控制器。人机接口允许控制工程师或操作人员配置设置点、控制算法和控制器参数。HMI 还提供过程状态信息展示，包括警示和通知操作员故障的其他方式。诊断和维护工具通常通过 modem 和网络激活接口变成可用，允许控制工程师、操作员监控、维护和改变控制器、执行器和远程位置的传感器件。

典型的工业区域包含许多基于网络协议控制回路，HMI 和远程诊断维护工具。现有的现场总线主要有基金会现场总线、profibus、Interbus、CAN、LonWorks

3　工业控制网络体系结构

工业控制网络由现场控制层和监控层组成，如图 2 所示。在现场监控层的主要设备是执行器、传感器、分布控制系统控制器、网络使能 I/O 设备、可编程逻辑控制器。过程控制设备从传感器读取数据，执行控制算法，发送输出给最终的元件。在本层的通信协议主要是现场总线，如 Lonworks 或 Profibus。在监控层主要设备包括 HMI、PLC 通信模块、以太网微处理器、基于控制器的 PC、普通用途的 RTOS，监控层完成的典型功能：操作人机接口、操作员警示、管理控制功能和历史数据收集。

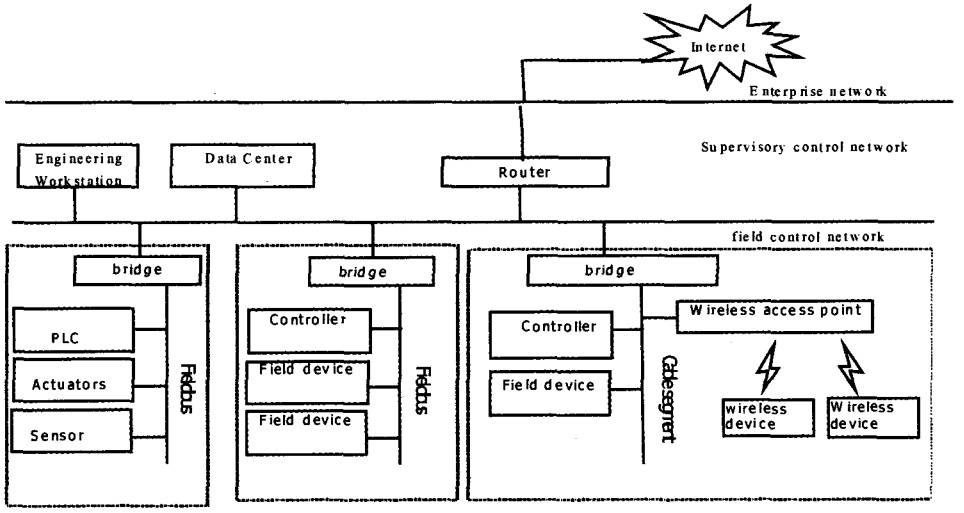

图 2　工业控制网络体系结构图

4　工业控制网络的安全威胁分析

标准系统（特别基于 Windows 系统）和标准网络（以太网和 TCP/IP）在网络系统中越来越多的使用，这些系统易受病毒的攻击。渐增的网络也导致许多可能攻击者能够进入控制系统的入侵点，如网络接入、拨号上网或无线链接、内部网络连接、连接第三方或直接网络连接等等。除了那些新的弱点，许多系统为了性能设计而牺牲了安全性，接入时没有被适当的安全措施保护。结果，非授权的人员能够潜在地侵入控制设备、远程设备、数据库和控制平台。入侵者被雇用来实施不适当的行为，和了解开放操作系统和网络特征知识的恶意攻击者一样。

控制网络入侵者的威胁主要包括：未授权进入、偷窃，或机密信息的误用；过程数据和产品信息完整性或可靠性的丢失；系统有效性丢失；过程扰乱导致次等产品质量，失去产品性能，危及过程安全，或环境；设备损害；人身伤害；违反合法的管理要求；公共健康和信心；影响国家安全。

这些威胁需要安全模型来帮助定义适用于工业控制网络安全措施，和连接其他信息网络一样。

5　工业控制网络的安全模型

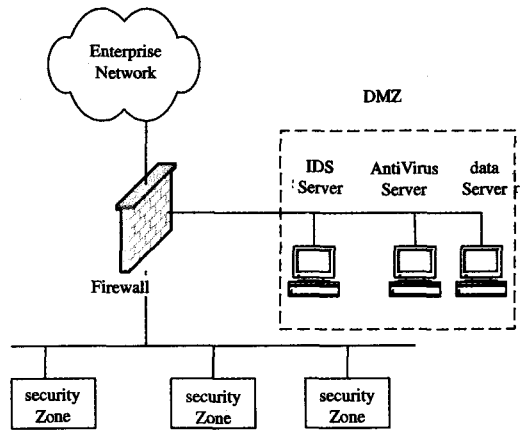

图 3　工业控制网络安全模型

从图 3 可以看出，我们构造了基于安全区域的用于工业控制区域的 Demilitarized Zone（DMZ）模型。至少需要实现状态过滤防火墙功能。DMZ 可以被当作一个代理区用来保护企业网和 ICN 网之间的通信。在 DMZ 上的服务器或者系

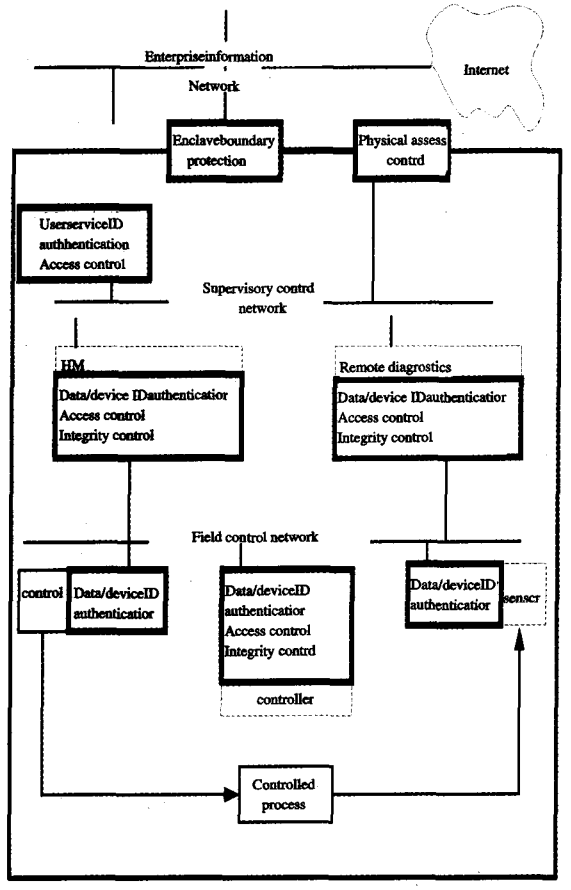

图 4　安全区域模型

统需要被固化并且能被最新的安全补丁和反病毒的文件实时更新。与这些系统之间的通信的最大范围需要由防火墙限制，所有的通信将会通过固化在 DMZ 的服务器指定后才能发生。

在图 4 中显示了安全的区域模型，当用户和服务访问被保护的资源时，我们使用边界保护和物理访问控制来保护连接安全和环境安全以及里面的安全区域，数据/设备标识符鉴别服务被用作一个独立的功能来强调数据和指令信号的鉴定。访问控制和完整性控制用来预防未经授权的用户读或写变量或者参数，或者未经授权的修改以上的值。

6　安全模型的 UML 描述

在图 5 中，我们定义了一些类，以及它的属性和方法。企业网类和工业控制网类来源于 CommNetwork 类，工业控制网类由一些设备类、工作站类、防火墙类、LogHistorian 类的集合而成，我们根据安全区域的定义将鉴定方法和完整性方法加入到设备类和工作站类上，并且描述了与工作站类相关的用户类和操作类的访问权限。我们同样提出防火墙类，它主要描述了在安全模型中防火墙的使用策略。

结论　基于对一般工业控制网络模型的研究和其可能受到的威胁分析，建立了基于安全区域的 DMZ 模型，安全工程师可以根据安全需求配置安全策略，同时可以保护 ICN 网络的信息机密性、系统的有效性和数据的完整性，从而保障国家基础设施的安全。

参 考 文 献

1　ISA-99. 00. 01 Manufacturing and Control Systems Security, Draft 1, Edit 3
2　Falco J, Stouffer K, Wavering A, et al. IT Security for Industrial Control Systems. Intelligent systems Division, NIST
3　PROFIBUS WG18. Profinet Security Guide, Version 0. 8
4　NIST. System Protection Profile-Industrial Control System, Version 1. 0
5　Honeywell Inc. Securing Process Control Network External Communication
6　国家标准．用于测量与控制系统的 EPA 通信标准

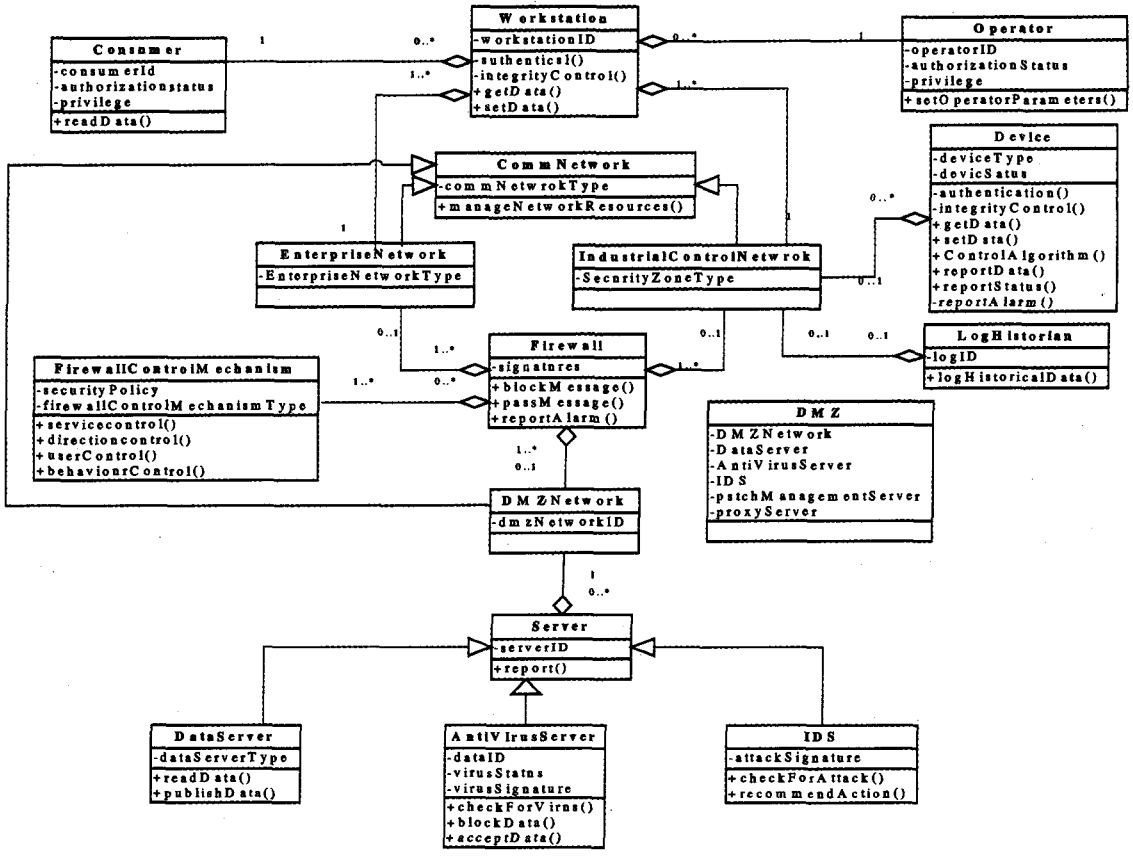

图 5　安全模型 UML 描述