工业控制系统信息安全审计系统分析与设计

陈 庄 黄 勇 邹 航
(重庆理工大学计算机科学与工程学院 重庆 400054)

摘 要 目前工业控制系统(Industrial Control System,ICS)广泛应用于电力、水利、交通运输、大型制造行业以及国家基础公共设施,已经成为国家安全战略的重要部分。传统的信息安全防护技术(如防火墙技术、入侵检测技术等)因其技术原理和适用协议的差异,使工业控制系统不能取得很好的防范效果。为了有效地提高ICS的安全防护能力,该文针对ICS的数据特点以及协议特点设计了一款ICS信息安全审计系统,该审计系统主要由数据采集模块、内容检测模块、异常行为判断模块、行为处理模块、审计响应模块等组成。实验结果表明,本系统能够对ICS进行全方位的安全审计,能够极大程度地提高ICS的安全防护能力。

关键词 工业控制系统,安全审计,异常行为检测
中图法分类号 TP39 **文献标识码** A

Analysis and Design of ICS Information Security Audit System

CHEN Zhuang HUANG Yong ZOU Hang
(College of Computer Science and Engineering, Chongqing University of Technology, Chongqing 400054, China)

Abstract At present, Industrial control system(ICS) is widely used in electric power, transportation, water conservancy, large manufacturing industry and national critical infrastructure. ICS has become the important part of the national security strategy. However, the traditional information security technology(such as firewall technology, intrusion detection technology, etc.) has the different technical principle and the different network protocol, and doesn't have a good protection effect in ICS. In order to effectively improve the Industrial control system information security(ICSIS) protection, based on the specific data and protocol and the highly real-time requirement, this paper designed an ICSIS audit system, which mainly includes data acquisition module, content detection mo-dule, abnormal behavior judgment module, behavior handling module, audit response module. The testing results show that the ICSIS audit system can comprehensive audit the ICS, and the use of ICSIS audit system can greatly improve the ICS safety protection ability.

Keywords Industrial control system, Security audit, Abnormal behavior detection

1 引言

工业控制系统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[1]。工业控制系统广泛应用于我国电力、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[2]。

目前工业自动化市场上还鲜有专门针对工业控制系统安全的防护产品。为了防护工业控制系统的安全,国内外主要采取工业防火墙技术。该技术存在4个不足:一是不能阻止感染病毒的程序和文件的传输;二是无法防止绕过它的攻击行为,一旦恶意代码通过移动存储等介质进入系统内部之后,工业防火墙的防护将相当乏力;三是不能防范全新的威胁,更不能防止可接触的人为或自然的破坏;四是没有对整个系统进行监控,不能很好地记录攻击的时间、特点以及造成的影响,使得网络管理员不便对工业控制系统网络进行安全加固。

ICS信息安全审计系统能很好地对工业防火墙技术进行补充,安全审计即是产生、记录并检查按时间顺序排列的系统事件记录的过程。具体作法为:利用技术手段,不间断地将计算机网络上发生的事件记录下来,用事后追查的方法保证系统的安全[3]。

2 ICS信息安全风险分析及安全审计系统需求分析

作为国家关键基础设施自动化控制的基本组成部分,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。

2.1 ICS信息安全风险分析

我国工控系统的安全风险主要体现在下列几个方面。

本文受科技型中小企业技术创新基金项目(12C26115116106),重庆理工大学研究生创新基金(YCX2012102)资助。
陈 庄(1964—),男,博士,教授,主要研究方向为企业信息化管理、网络与信息安全,E-mail:zhuang.ch@gmail.com;黄 勇(1989—),男,硕士,主要研究方向为网络与信息安全;邹 航(1979—),男,硕士,实验师,主要研究方向为网络与信息安全。

2.1.1 操作系统漏洞

目前大多数工业控制系统的工程师站、操作员站、HMI等都是Windows平台的。为保证工业控制系统的相对独立、稳定、安全运行，并考虑到工业控制系统与操作系统补丁的兼容性问题，通常企业在系统正式运营后不会对Windows平台安装系统补丁，从而导致ICS会带着风险运行[4]。

2.1.2 通信协议漏洞

信息化与工业化的深度融合以及物联网的快速发展使得TCP/IP协议和OPC协议等通用协议越来越广泛地应用在工业控制系统网络中，随之而来的通信协议漏洞问题也日益突出。

2.1.3 应用软件漏洞

由于应用软件的多种多样，很难形成统一的防护规范以应对信息安全问题；当应用软件面向网络应用时，就必须开放其应用端口。这样一来不但增加了管理上的难度，也给ICS的信息安全带来了相当大的风险[5]。

2.1.4 病毒、黑客组织的攻击

当前的网络攻击行为体现为攻击定向化、组织化。黑客的行为不再是个体行为，而是组织行为甚至国家行为，他们锁定特定目标(如针对特定国家、政府机构、企业或组织)，长期有计划性、有组织性窃取情报。工业控制系统又密切涉及国计民生，一旦其遭受攻击，将导致大量的人员伤亡以及财产损失，工业控制系统已经成为木马、病毒、黑客等的重要攻击目标。

2.2 工业控制系统信息安全审计系统需求分析

随着企业信息化进程不断深入，企业的业务系统变得日益复杂，由内部员工的违规而操作导致的系统安全问题日益突出。工业防火墙等常规的安全产品可以解决一部分安全问题，但对于内部人员的违规操作却无能为力。最新统计资料表明，对企业造成严重攻击的事件中，有70%是来自于企业的内部人员。

一般来说，系统管理员都是从各种系统日志去发现是否有人侵后留下的“蛛丝马迹”来判断是否发生过安全事件。从系统变更的角度来看，审计日志比系统日志在定位系统安全问题上更可信。

为了确保工业控制系统信息安全，工业控制系统用户需要对员工的操作行为进行监控并对网络传输内容进行审计。掌握工业控制系统的安全状况：对工业控制系统网络传输信息的实时采集、海量存储；对工业控制系统网络传输信息的统计分析；攻击行为后期取证；对工业控制系统网络潜在威胁者予以威慑。

综上所述，急需专门针对工业控制系统的安全审计策略对整个工控系统进行全程审计，以掌握ICS安全健康状态，找出系统的脆弱点，从而进行有针对性的安全防护。

3 ICS信息安全审计系统的设计

3.1 ICS信息安全审计系统的体系架构

如图1所示，工控安全审计系统可以视为“3+5”体系架构，即基于“3”个特征库(协议库、行为特征库、审计数据仓库)的“5”层架构(含数据采集层、内容检测层、行为检测与判断层、行为事件处理层、行为审计层)。以下简要说明图中的主要要件。

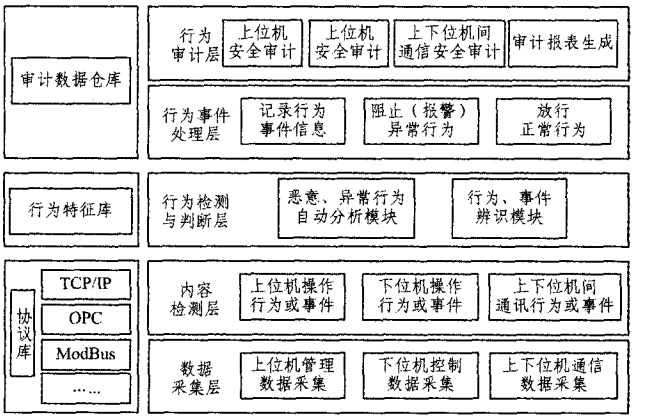

图1 ICS信息安全审计系统体系架构图

(1)协议库。协议库是指是工业控制系统所采用的通信协议，如Modbus、OPC、TCP/IP、CAN、RS485、RS232等。

(2)行为特征库。行为特征库是指上位机操作行为、下位机操作行为、上下位机间通讯的通讯行为的“行为特征”，如访问控制行为、请求错误行为、系统事件、备份和恢复事件、配置变化行为等。

(3)审计数据仓库。审计数据仓库是指存储在数据库中的工业控制系统某一时间段、所有行为的审计信息。

(4)异常行为分析模块。通过把可疑行为的不同部分关联起来并不断更新行为特征库，最终确定恶意代码的新型攻击行为。

3.2 ICS信息安全审计系统的功能设计

3.2.1 数据采集与分析功能

数据采集包括：上位机的管理数据采集、下位机控制数据的采集、上位机和下位机间的通信数据采集。

数据采集主要是基于数据链路层的数据包获取，并根据定义的策略及系统的需求分析，过滤掉无需审计的数据包，有选择的进行保存处理。数据采集并保存生成的数据文件为ICS安全审计系统提供主要的数据源。数据采集是安全审计的首要环节，是数据解析和处理的基础。上位机的系统日志以及下位机反馈给上位机的控制数据同样是数据采集的重要组成部分。

系统通过对采集到的审计数据进行分析与处理，实现对整个系统的行为审计功能，其核心技术是协议分析。通过对ICS特有的协议以及传统的通信协议进行分析，将采集到的审计数据分为3类：上位机操作行为或事件、下位机操作行为或事件、上下位机通讯行为或事件。此功能对审计结果正确与否起到决定性的作用。

3.2.2 异常行为检测与判断功能

本系统的异常行为智能分析技术主要采用“行为关联性技术”，综合考虑操作行为(或事件)，确定其是否属于恶意或异常行为。单一可疑行为(或事件)似乎没有什么危害，但是如果同时进行多项行为(时序相关)，就会导致恶意攻击行为的产生。因此，需要按照主动防御的观点来判断其是否实际存在入侵、攻击等威胁，检查潜在威胁在不同组件之间的相互关系。通过把可疑行为的不同部分关联起来并不断更新行为特征库，最终确定恶意代码的新型攻击行为。

行为、事件辨识技术主要采用自适应多维函数$Y=k*f(X_1,X_2,\cdots,X_n)$，其中$X_n$为某个行为风险权值，$k$为行为类

别风险权重，Y 为整个行为的风险值。该函数同专家知识相结合，自动辨识行为之间的逻辑关系，自动判定行为的合法性，实现恶意代码、异常行为的智能辨识。

3.2.3 行为审计功能

行为审计主要包括如下 3 个功能：

①上位机安全审计功能主要有账号访问和创建记录安全审计、工控软件更新记录安全审计、移动介质访问记录安全审计、网络访问记录安全审计、补丁日志记录安全审计、设备安全配置审计、上位机安全档案管理审计、系统安全故障检测和异常恢复审计等。

②下位机安全审计功能主要有安全区域的划分审计、下位机访问控制行为审计、下位机在线状态审计、下位机安全状态审计、下位机自动发现及资产管理审计等。

③上下位机间通讯安全审计功能主要有上下位机通信协议的审计与检测、OPC 通信的内容检查和连接行为审计、OPC 客户端和服务器通信行为审计、VPN 远程访问 OPC 服务器通信行为审计、区域间隔离状态审计、区域间通信管控审计等。

3.2.4 审计报表功能

网络中每天会产生大量的日志信息，巨大的工作量使得管理员手工查看并分析各种日志内容是不现实的，必须提供一种直观的分析报告及统计报表的自动生成机制来保证管理员能够及时、有效地发现网络中各种异常状况及安全事件。

本系统的审计报表功能主要包括异常行为及审计响应报表、异常行为统计报表、设备安全配置审计报表、移动介质访问记录审计报表、工控软件更新记录审计报表、VPN 远程访问 OPC 服务器行为审计报表、OPC 通信的内容检查和连接行为审计报表等。

3.3 ICS 安全审计系统的实现流程

工控安全审计系统的处理流程如图 2 所示。它主要包括以下 5 个流程。

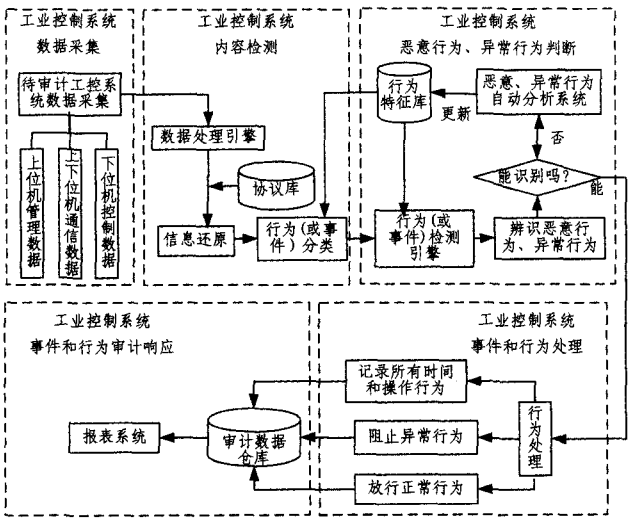

图 2 ICS 信息安全审计系统的审计流程图

(1)工业控制系统数据采集。实现待审计的工控系统数据采集，包括上位机的管理数据采集、下位机控制数据的采集、上位机和下位机间的通信数据的采集等 3 部分数据。

(2)工业控制系统内容检测。将采集的数据还原成上位机操作行为或事件、下位机操作行为或事件、上下位机间通讯的通讯行为或事件，如访问控制行为、请求错误行为、系统事件、备份和恢复事件、配置变化行为等。

(3)工业控制系统恶意行为、异常行为判断。根据第(2)步所获得的行为信息或事件信息生成相应的行为事件，并通过行为特征库、行为检测引擎来辨识是否为恶意或异常行为，若能直接辨识则进入第(4)步；否则，利用恶意、异常行为自动分析模块更新行为特征库，以能识别未知行为。

(4)工业控制系统事件和行为处理。根据行为特征进行智能处理，即对于异常行为进行阻止并报警；对于正常行为则放行；同时，还要记录所有的事件和操作行为信息。

(5)工业控制系统事件和行为审计响应。将事件信息和行为信息存入审计数据仓库，并根据用户的需求生成相应的审计报表。

4 ICS 信息安全审计系统的实现

4.1 ICS 信息安全审计系统的部署

ICS 信息安全审计系统的部署图如图 3 所示。本系统可直接安装在上位机(如 SCADA 服务器、DCS 服务器)与下位机进行数据交换的交换机上，可以对上位机的系统日志、上位机对下位机所下发的控制指令数据以及下位机反馈的控制数据进行数据采集和安全审计，部署简单，可操作性强。

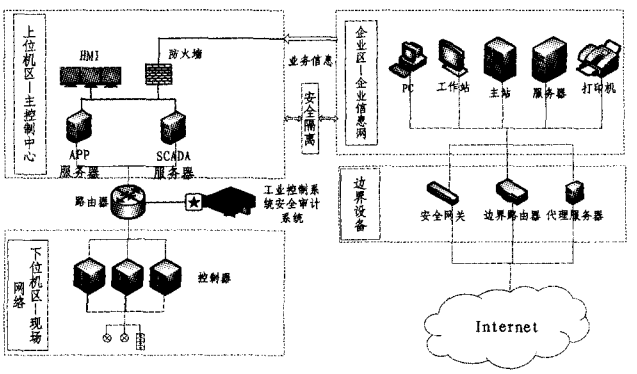

图 3 ICS 信息安全审计系统布置图

4.2 第三方权威机构检验测试

本系统通过了第三方权威机构(重庆科技检测中心、机械工业工业过程控制系统产品质量监督检测中心，该检测中心具有 MA、CNAS、ML 等权威系统检测资质)的检验测试，结果表明，本系统的设计完全符合工业控制系统的独有特点，能够提供上下位机系统的安全审计、工业控制系统报警审计、上下位机通信协议的审计、程序异常行为检测及审计、审计报表的生成等功能。

在系统性能上能够达到：1)支持的原始日志和事件的存储容量达到 500 万条；2)可以通过自身的调节达到负载均衡，支持双机热备实时同步；3)支持工业控制系统特定接口、协议，如 OPC、Modbus 等常用工业通信协议，RS-422/485、RS-232 等工业控制系统常用接口。

结束语 本文针对工业控制系统的安全现状以及防护要求，设计了一套 ICS 信息安全审计系统。本 ICS 信息安全审计系统能够全面实时地收集来自工业控制系统下位机区网络终端设备(PLC、智能仪表、工控机)、工业控制系统上位机区设备(SCADA 服务器、数据库、MES 以及管理控制主机、工作站等)、企业办公区内所有节点终端设备(网络交换机、路由器、防火墙等)的日常操作与管理事件，进行安全审计分析。

具体贡献如下：

(1)分析了当前 ICS 的安全风险,并由此引出了工业控制系统信息安全审计系统。

(2)对 ICS 信息安全审计系统进行需求分析,分析了 ICS 信息安全现状及需求,并对工业控制系统用户的需求进行了详细分析。

(3)针对 ICS 信息安全现状以及系统特点,有针对性地设计了一套 ICS 信息安全审计系统,该系统能够极大程度地提高 ICS 的防护能力,并能提供十分丰富的审计报告。

(4)ICS 信息安全审计系统的实现。研究了系统的部署方法,并通过了相关权威机构检验。该系统在第三方权威机构的检验测试结果表明,该系统能够对工业控制系统进行全方位的安全审计,能够极大地提高工业控制系统安全防护能力。

ICS 信息安全不是一个单纯的技术问题,而是一个从意识培养开始,涉及到管理、流程、架构、技术、产品等各方面的系统工程。ICS 信息安全更是一个动态过程,需要在整个工业基础设施生命周期的各个阶段中持续实施,不断改进。为了进一步提高工业控制系统安全防护能力,下一步我们将进一步开展 ICS 相关防御技术研究。

参 考 文 献

[1] IEC 62443-2-1 ED. 1.0 EN:2010,Industrial communication networks - Network and system security - Part 2-1:Establishing an industrial automation and control system security program[Z]. 2010

[2] 石勇,刘巍伟,刘博. 工业控制系统(ICS)的安全研究[J]. 网络安全技术与应用,2008(4)

[3] GB 17859-1999. Classified criteria for security protection of computer information system[S]. 1999

[4] 张帅. 工业控制系统安全现状与风险分析——ICS 工业控制系统安全风险分析之一[J]. 计算机安全,2012(1)

[5] 王文宇,刘玉红. 工控系统安全威胁分析及防护研究[J]. 信息安全与通信保密,2012(2)

(上接第 329 页)

表 2 诊断结果

诊断算法	节点数	诊断错误数	诊断正确率%	平均正确率%
RVM- Mexican	60	3	95.0	95.6
	120	5	95.8	
	180	8	95.6	
	240	10	95.8	
SVM-RBF	60	5	91.7	92.4
	120	8	93.3	
	180	14	92.2	
	240	18	92.5	
ANN-RBF	60	10	83.3	84.2
	120	19	84.1	
	180	28	84.4	
	240	36	85.0	

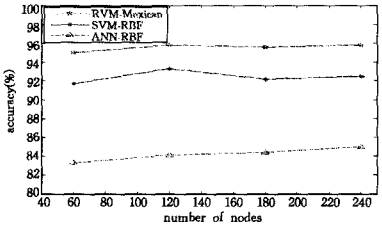

图 5 RVM,SVM 及 ANN 诊断结果比较

神经网络是基于传统统计学的基础上的,而传统统计学主要研究样本数据趋于无穷多时的统计性质,因此较上述算法有较弱的对策泛化能力。从表 2 可见,其平均诊断精度为 84.2%。

从图 5 可见,在无线传感器网络不同样本数下,诊断算法的诊断精度一致表现为:RVM-Mexican>SVM-RBF>ANN-RBF。结果说明,对无线传感器节点的诊断使用 RVM-Mexican 算法会明显好于 SVM-RBF 和 ANN-RBF。

结束语 本文将相关向量机及支持向量机算法应用于无线传感器网络的节点故障诊断研究,在分析传感器节点故障类别的基础上以 4 个分类器区别正常节点及 4 类故障节点,并与人工神经网络等算法进行了比较。仿真实验表明,相关向量机算法比支持向量机和人工神经网络有更高的诊断精度。

参 考 文 献

[1] Pottie G J, Kaiser W J. Embedding the Internet: Wireless integrated network sensors[J]. Communications of the ACM, 2000, 43(5):51-58

[2] Tipping M E. Sparse Bayesian learning and the relevance vector machine[J]. The Journal of Machine Learning Research, 2001, 3:211

[3] Vapnik V N. The Nature of Statistical Learning Theory(2nd ed)[M]. New York, USA: Springer-Verlag, 1995

[4] Scholkopf B, Alexander J S. Learning with Kernels: Support Vector Machines, Regularization, Optimization, and Beyond [M]. London: The MIT Press, 2001

[5] Vladimir N V. The Nature of Statistical Learning Theory[M]. New York: Springer, 1995

[6] Kropotov D, Ptashko N, Vasiliev O, et al. On kernel selection in relevance vector machines using stability principle[C]// The 18th International Conference on Pattern Recognition (ICPR 06). 2006

[7] Zhang Q, Benveniste A. Wavelet networks[J]. IEEE Trans on Neural Networks, 1992, 3(6): 889-898

[8] 闫丹. 基于人工免疫的无线传感器网络节点故障诊断[D]. 成都:电子科技大学, 2009

[9] Vapnik V N. Estimation of dependencies based on empirical data [M]. Berlin: Springer-Verlag, 1982

[10] Zhang L, Zhou W D, Jiao L C. Wavelet support vector machine [J]. IEEE Trans Syst Man Cybern Part B, 2004, 34(1): 34-37

[11] 何飞,黎敏,等. 基于小波相关向量机的产品质量模型[J]. 北京科技大学学报, 2009, 31(7): 934-938

[12] Zhao Cheng-lin, Sun Xue-bin, et al. Fault diagnosis of sensor by chaos particle swarm optimization algorithm and support vector machine[J]. Expert Systems with Applications, 2011(38): 9908-9912