《电子技术应用》http://www.chinaaet.com

工业控制系统安全防护体系研究*

赵悦琪[1,2],赵德政[2],林　浩[2],霍玉鲜[2],张　菡[1,2],加舒娟[1]
(1.华北计算机系统工程研究所,北京 100083;2.中电智能科技有限公司,北京 102209)

摘　要：工业控制系统(简称工控系统)广泛应用于水力、电力、石油、交通、军工等各个行业,其安全性和稳定性关系着国家关键基础设置的正常运行。随着工控行业数字化生产、智能制造的推进,工控系统面临着严重的安全威胁。通过分析典型的攻击方式和现有防护措施的弱点,提出和设计一套纵深的工控系统安全防护体系,并从物理安全、数据安全、网络安全、主机与应用安全、控制安全五个方面分别阐述其技术重点,在可信平台的基础之上构建安全综合防护平台,形成了一套自适应的、闭环的、可进行自我防御与恢复的安全模型与机制,立体地维护了工控系统的安全,有利于工控系统的安全稳定运行。

关键词：工控系统;安全;防护;可信平台
中图分类号：TP309　　**文献标识码**：A　　DOI:10.16157/j.issn.0258-7998.200218

中文引用格式：赵悦琪,赵德政,林浩,等. 工业控制系统安全防护体系研究[J].电子技术应用,2021,47(1):69-72,77.
英文引用格式：Zhao Yueqi,Zhao Dezheng,Lin Hao,et al. Research on security protection system of industrial control system[J]. Application of Electronic Technique,2021,47(1):69-72,77.

Research on security protection system of industrial control system

Zhao Yueqi[1,2],Zhao Dezheng[2],Lin Hao[2],Huo Yuxian[2],Zhang Han[1,2],Jia Shujuan[1]
(1.National Computer System Engineering Research Institute of China,Beijing 100083,China;
2.Intelligence Technology of CEC Co.,Ltd.,Beijing 100083,China)

Abstract: Industrial control system(ICS) is widely used in water treatment, power, oil, transportation, military industry and other industries. The safety and stability are related to the normal operation of key national infrastructures. ICS are facing with serious security threats with the advancement of digital production and intelligent manufacturing. This paper proposes and designs a set of in-depth ICS security protection system by discussing the typical attack methods and the weaknesses of existing protection measures, and elaborates its technical focus from five aspects: physical security, data security, network security, host and application security, and control security. And then a comprehensive security protection platform is built on the basis of a trusted platform, forming a set of adaptive, closed-loop, security models and mechanisms that can self-defense and recover, maintain the safety of the ICS in three dimensions.It is helpful for security and stability operation of ICS.
Key words: ICS;safety;protection;trusted platform

0 引言

工业控制系统(以下简称工控系统)是一种借助物理组件、逻辑和网络来管理自动化过程,以及对事件进行控制和监视的业务流程管控系统,主要包括监控和数据采集(SCADA)系统、分布式控制系统(DCS)和可编程逻辑控制器(PLC)等,通常用在水力、电力、石油、交通、军工等行业。工业控制系统的安全性和稳定性关系着国家关键基础设施的正常运行。

近年来,随着工控行业数字化生产和智能制造的推进,工控系统正逐步向开放和互联的方向发展,并不断地渗透传统网络通信领域的互联理念,系统不再有从前的“物理隔离”假设,面临更加严重和复杂的安全威胁,安全事件与日俱增,严重影响着我国诸多行业的安全与稳定[1]。然而我国的工控安全防护工作还处于起步阶段,缺乏自我保护能力,因此做好工控系统的安全防护是现阶段的重中之重[2]。本文通过讨论工控系统所面临的安全威胁,结合典型的攻击方式,针对现有防护措施的弱点,提出和设计一套纵深的工控系统安全防护体系,详细介绍涉及的安全防护技术,为工控系统的安全稳定运行给出良好的解决方案。

1 工控系统所面临的威胁

虽然工控系统种类繁多,诸如 DCS、SCADA 系统、PLC 系统等,但大都可以抽象成如图 1 所示的模型表示。

其中,运营管理层主要负责管理生产过程和生产设

*基金项目:国防基础科研计划项目(JCKY2018211C001)

《电子技术应用》http://www.chinaaet.com

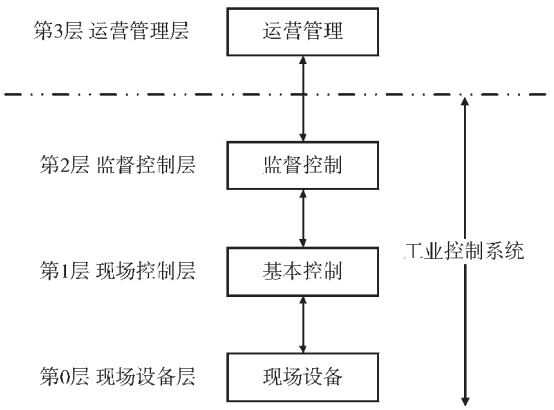

图 1 工控系统典型模型

备，如：生产调度、生产计划、保障系统可靠性、生产现场控制优化等；监督控制层主要实现监督和控制系统各个环节的物理过程的功能，如工程师组态及下装、历史数据存储、故障报警等；现场控制层主要实现面向用户的指令，从传感器读取数据，维护过程历史记录，常用的有控制器、安全和保护系统等；现场设备层包括直接或间接连接到过程和过程设备的仪器仪表等。

分析工控系统的典型模型可知，系统在不同的层面，可能会遭受不同的安全攻击，如：(1)针对现场设备所进行的物理攻击；(2)针对系统关键控制回路所进行的数据截获、数据篡改、数据欺骗等；(3)针对系统网络或设备发起的拒绝服务攻击、病毒入侵攻击、数据篡改、非法获取权限等。这些攻击最终可能会破坏控制回路的正常功能，造成物理感染、设备失控、非正常停机等事故，甚至造成对人身、财产、环境的威胁和社会灾难。

我国的工控安全防护工作还处于起步阶段，分析目前国内的工控系统安全防护措施可以发现：首先，系统安全加密过程普遍存在着弱口令、明文通信、弱认证等问题；其次，系统中所使用的产品的安全服务保障能力弱，极易导致通信信息、设备参数的泄露；另外，在安全机制层面缺乏风险识别、安全监测、安全防御、安全恢复等响应机制，无法抵御上述攻击，影响系统的安全运行。随着攻击手段不断更新，系统结构日渐复杂，无法通过单一的防护措施把所有的攻击都阻拦在外，更无法解决系统自身存在的诸多问题，因此，要保证工控系统的安全，必须采用纵深防御的安全理念，从上述各类攻击出发，结合系统自身存在的隐患、漏洞，融合不同的安全防护技术，针对不同的层面，构建起多层次的纵深防御体系，从而维护工控系统的安全与稳定运行[3]。

2 工控系统安全防护体系

经过以上分析，本文设计了一个纵深的工控系统安全防护体系，这样的防护体系是一个全方位的概念，涉及安全防护技术、应急备用措施、全面安全管理三方面，可以保证系统从设计开发、安装使用、运行维护到退出使用的整个生命周期都受到安全保护，三方面相互支撑、相互融合，形成动态关联的三维立体结构。该系统通过一种自适应的、闭环的、可进行自我防御与恢复的响应模型实现，该模型包括风险识别、安全监测、安全防御、安全响应、安全恢复以及效果评估，各机制层层配合，闭环运行。系统安全防护体系及响应模型图如图 2 所示。

安全防护技术是防护体系的关键内容。从工业视角出发，安全的重点是保障生产的连续性、可靠性，主要保证自动化装备、工业控制设备及系统的安全；而从数字化和智能化角度出发，安全主要负责防止工业数据泄露、保障不同系统的专项定制、实现网络互联等工业互联网应用的安全运行。考虑不同视角下的不同安全需求，所设计的防护体系作用于从工控系统的现场设备层到监督控制层，安全防护技术主要包括五项基本内容：物理安全、数据安全、网络安全、主机与应用安全和控制安全[4]。各部分的防御范围和所涉及的重点技术阐述如下。

3 工控系统安全防护技术

3.1 物理安全

保证物理安全即保证设备自身及其物理运行环境安全，这是最基本的安全防护措施。实现物理安全防护必须为设备选择具有防震、防风、防雨、防火能力的建筑

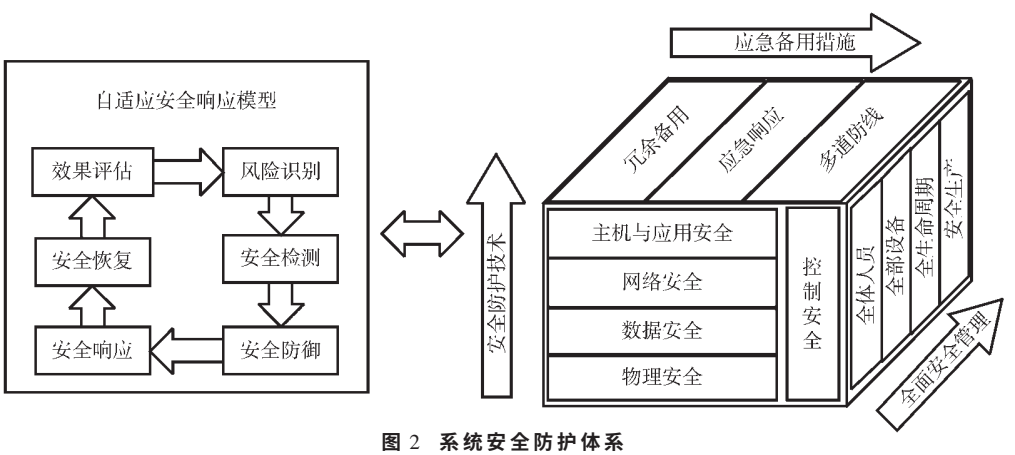

图 2 系统安全防护体系

或箱体，远离强电磁干扰、远离热源，实施防盗和防破坏的防护措施，安排专人看守所选物理位置，对处于无人值守环境的控制器，应通过网络实时监控其安全状态，当发现有物理临近攻击的行为时，应及时采取远程锁定、远程擦除等保护措施。

3.2 数据安全

在保证设备正常运行、不受外界干扰的同时，还必须保证最基本的通信数据安全，即安全地下发控制信息、上传工业数据等，防止信息窃取、伪造控制指令、数据欺骗、干扰和破坏控制功能等攻击事件的发生。保证数据安全的关键措施是密码加密与身份认证技术。

工控系统不同于传统的高性能系统，它在数据传输时指令报文普遍较短，控制回路与输入输出设备、现场执行设备或传感器设备距离较远，控制回路响应时间要求很高，而现有工控系统的嵌入式 CPU 芯片和密码芯片的性能有限、板级通信速率有限，现场总线控制回路中数据防篡改能力差、复杂度高。为了提高传输数据在控制回路中的实时性、安全性，给信息加密是目前较为有效的方法。传统的推荐密码对这种传输指令短、控制回路响应时间要求高的系统是不适用的，所以选用轻量级密码算法进行加解密较为合适。这种算法通过改进密钥长度、加密轮数，降低对处理器计算能力的要求和对硬件资源的开销，但提供的加密性能却并没有降低，性能良好。

为确保通信安全不仅仅要对通信数据进行加密计算，还需要在通信双方在建立 TCP 连接后，通过数字签名与认证证书的方式进行双向的身份验证，通信双方完成身份验证后，通过协商生成随机密码，从而进入下一步的通信阶段。

3.3 网络安全

由于现有工业控制系统的监督控制数据大都需要通过网络传输，因此必须保障控制网络免受外部攻击，实现网络安全。通过研制符合安全要求的工控防火墙、边界工业网闸、工业网络监测审计系统，同时配合漏洞挖掘工具与漏洞扫描工具对网络设备进行实时扫描，实现工控网络全方位的保障。

网络安全由边界工业防火墙、边界工业网闸、工业网络监测审计系统共同实现。其中，边界工业防火墙由基于白名单的访问控制、工业协议精准识别和深度检测等技术实现。边界工业网闸由内、外网处理单元和安全数据交换单元组成，实现了工业网络的边界防护，有效提升防止恶意软件传播与防边界渗透的安全防护能力。部署于工业生产内网的工业网络监测审计系统通过镜像方式分析网络流量，及时地发现网络中存在的安全隐患，可以对工业网络内的安全设备进行状态审计和配置更改，实现工业网络审计功能[5]。

另外依赖漏洞挖掘工具与漏洞扫描工具对网络设备进行实时扫描，对工控设备的已知漏洞进行识别和检测，并及时发现和评估未知漏洞，对风险控制策略进行审核，实现网络设备的安全运行[6]。

3.4 主机与应用安全

系统中有种类不同、数量繁多的工作站、应用节点，在保证通信数据安全和网络安全的基础之上，还必须保证主机与应用的安全。主机安全由主机白名单和配置核查工具箱共同维护。主机安全白名单防护针对工作站、服务器等工业主机进行安全加固，包括移动存储介质管理、程序与文件加载控制、主机状态监控审计、非法外联管控等主机安全防护手段；配置核查工具箱对主机操作系统进行安全基线配置核查，根据相关标准中的要求对被检查对象进行安全评估，并根据评估的结果对主机的配置进行整改，使其满足安全基线的要求。

应用安全依靠主机白名单实现，主机安全白名单防护系统专门为工业应用环境打造，采用高效、稳定、兼容、易于设置的白名单安全防护技术，只允许白名单内的业务应用和软件能够加载和运行，禁止白名单外的所有进程加载和运行，构建主机运算的可信环境，从根本上防御了恶意软件安装和运行的可能，实现防病毒的能力。

3.5 控制安全

控制安全是一个综合的概念，实现控制安全是为了从根本上杜绝后门、木马的威胁，杜绝数据篡改、仿冒现象的发生，工控系统应选择和部署安全可靠的监控组态软件、逻辑组态软件和控制器模块等工控软件和设备，选择经过安全认证或通过安全检测的网络交换机、路由器等网络设备以及防火墙、身份认证系统、漏洞扫描系统和安全审计系统等。同时还应重点关注系统平台的安全性，选择使用符合不同安全等级要求的 CPU、FPGA 等关键芯片、桌面操作系统和嵌入式操作系统、数据库管理系统和中间件，并选择使用具有身份认证、访问控制、权限管理、数据加解密、安全免疫等安全措施的系统和设备[7]。

3.5.1 安全综合防护平台

为了满足以上控制安全的需求，本方案提出一种工控系统网络安全综合防护平台。该平台为数据安全、网络安全、主机与应用安全等提供实现平台，目的是让各个工控系统安全技术防护措施发挥最大效用，更好地支撑企业对办公网络以及生产网络的统一安全监管，实现对工业企业资产、设备、数据的统一管理和信息的集中汇聚，并将信息资产、网络安全风险、脆弱性及威胁进行综合的态势分析、监测与展示，实现风险识别、安全监测、安全防御、安全响应、安全恢复以及效果评估的目的。具体平台具体功能如下：

(1)安全设备统一管理

安全综合防护平台对项目中的安全防护设备进行统一管理，采用策略驱动技术实现对安全设备的统一策

《电子技术应用》http://www.chinaaet.com

略部署，能够根据当前所面临的安全威胁统一定制和部署安全策略及风险识别机制，降低网络安全管理的成本。

(2)安全信息集中汇聚

安全综合防护平台通过 Syslog、FTP、ODBC 等多种方式收集生产网络安全设备、工控设备、管理网络安全设备、服务器等系统的日志数据，利用强大的统计汇总及关联分析工具，实现数据内容的深度钻取、剖析、层层追踪还原攻击事件的整个行为过程，挖掘出潜在的威胁，并做针对性的策略优化，实现安全监测功能。

(3)安全态势可视化呈现

安全综合防护平台通过可视化的统一界面展现各类监测数据、统计数据、告警数据以及所有管控操作。对检测到的安全漏洞和安全风险及时通报，提供多维度、可视化的呈现界面，并提示可操作的安全解决方案与措施，对安全防护情况进行持续跟踪，并显示风险应对效果评估结果。

(4)安全的平台内部通信

安全综合防护平台与各类设备之间采用 TCP 加密通信，保证信息不被窃取及篡改，禁止未经允许或假冒的连接访问系统，防止安全综合防护平台及安全防护体系受到攻击，实现安全防御。

(5)工业互联网平台联动预警、通报

安全综合防护平台综合分析工业互联网企业流量、主机、设备等数据，建立多源融合分析模型，提供 7×24 小时安全保障服务，基于规则库匹配和行为分析实现对各类安全威胁的全天候安全监测，结合企业的工业互联网平台进行及时的联动预警与通报。

(6)安全应急处置

安全综合防护平台根据监测预警结果形成可执行的安全策略，实现安全响应，实现安全设备和安全系统的防护策略配置与修改，在安全隐患造成实际影响之前对其进行阻断，维护系统正常功能。

3.5.2 可信平台的构建

实现安全综合防护平台功能需要构建一个可信的环境，确保系统有安全计算环境、安全区域边界和安全通信网络。可信是指系统要根据软硬件的计算资源构建保护环境，包含 3 个最重要的方面：可信机制、可信策略和可信保障。可信机制是执行可信免疫过程的系统、程序、模块、服务进程和外围安全产品的总和；可信策略是用来定义可信免疫过程中识别和监控具体行为方式的输入语句的总和；可信保障是使用保证可信免疫过程正确执行的可信部件和方法的总和[8]。

安全综合防护平台在可信平台的基础之上实现安全的设备管理、信息汇聚、安全通信态势分析等，安全保护环境功能框架如图 3 所示，该框架描述了各个系统需完成的基本功能和各部分基本连接关系[9]。各级系统的安全保护环境则根据级别的不同设置相应的安全计算环境、安全区域边界、安全通信网络和安全管理中心。

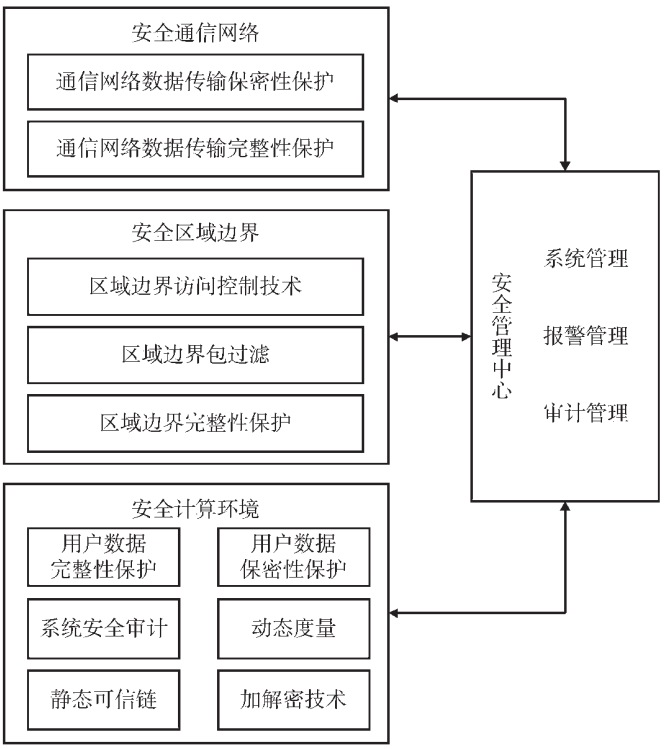

图 3 可信计算安全保护环境功能框架

在构建的可信平台的基础之上，实现安全综合防护平台的功能，有助于保障系统总体控制安全。

4 结论

本文通过讨论工控系统所面临的安全威胁，分析典型攻击方式，根据工控系统的安全需求，提出和设计了一套纵深的工控系统安全防护体系，并从物理安全、数据安全、网络安全、主机与应用安全、控制安全五个方面分别阐述其技术重点。这一安全体系在基础上保证物理安全，采用基于轻量级密码算法的加密、双向身份认证等技术维护数据安全，利用边界工业防火墙、边界工业网闸、工业网络监测审计、入侵检测、集中监管与审计等多种技术，配合漏洞挖掘工具与漏洞扫描工具等多种工具维护网络安全，依靠主机白名单和配置核查工具箱维护主机与应用安全，以可信计算基为基础给出安全综合防护平台，形成了一套自适应的、闭环的、可进行自我防御与恢复的安全模型与机制，立体地维护了工控体系的安全，有利于工业控制系统的安全稳定运行。

参考文献

[1] 王小山，杨安，石志强，等.工业控制系统信息安全新趋势[J].信息网络安全，2015(1)：6-11.
[2] 王宝来，陈安国，肖伟.工业控制系统网络安全防御体系研究[J].网络安全技术与应用，2020(1)：119-120.
[3] 赖英旭，刘增辉，蔡晓田，等.工业控制系统入侵检测研究综述[J].通信学报，2017，38(2)：143-156.
[4] 杨帆，赵少飞.基于企业视角探索工业信息安全解决之

(下转第 77 页)

在实际的电弧炉炼钢过程中，弧长是非线性、时变的，为了更好地模拟出实际弧长，在 t=20 s 时加入了随机白噪声，从而达到实际弧长的非线性以及随机性，添加白噪声的仿真结果图如图 7 所示。由此得出，电极调节系统在扰动下，遗传模糊逻辑控制器相比传统 PID 控制有更好的控制性能。

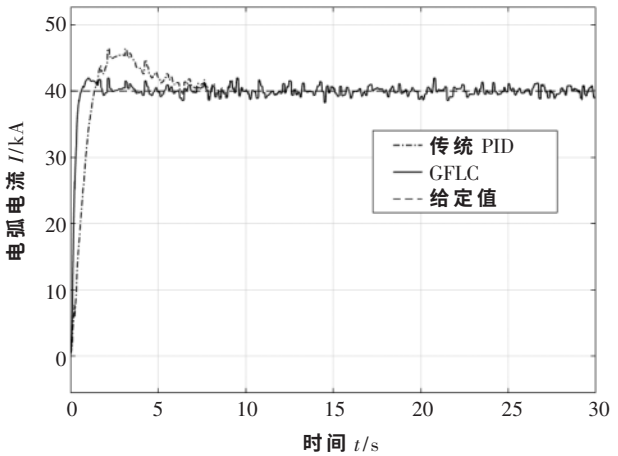

图 7 加入白噪声后的输出响应

4 结论

本文提出了一种 EAF 电极调节系统的非线性控制方法。首先，说明了电极调节器是一个复杂控制系统，针对这种复杂的时变系统，提出了 GFLC 控制算法来进行控制，该方法是利用遗传算法来构造模糊逻辑控制器的双层迭代进化算法。设计了一种新型的编码方式，克服了非线性不好控的问题，使得控制性能更加高效。传统 PID 控制方法针对非线性系统控制效果不理想，而 GFLC 通过选择逻辑规则和调整隶属函数来实时快速控制电极调节参数，从而节约电能，提升炼钢效率。

参考文献

[1] 史旭珊.基于神经网络的电弧炉电极调节控制器设计[D].沈阳：东北大学，2014.
[2] YU F，MAO Z.Recursive identification for electric arc furnace—Electrode regulator system[C].Chinese Control Conference，2017.
[3] Wang Zhengsong，Wang Qingkai，He Dakuo，et al.An improved particle swarm optimization algorithm based on fuzzy PID control[C].International Conference on Information Science & Control Engineering.Changsha，China，2017：835-839.
[4] 任雪，李强.基于模型预测控制的电弧炉智能调节系统[J].电气传动自动化，2016，38(2)：34-40.
[5] 李强，吴朋化，苟智峰.基于模糊神经网络的电弧炉控制系统及仿真[J].控制工程，2012(2)：154-172.
[6] 李强，潘永湘，余健明，等.综合智能控制策略在电弧炉控制中的应用[J].电工技术学报，2003，18(1)：100-104.
[7] 吴志军，刘小河.电弧炉电极调节系统的无模型自适应控制[J].北京信息科技大学学报(自然科学版)，2016，31(1)：33-42.
[8] CHIOU Y C，LAN L W.Genetic fuzzy logic controller：an iterative evolution algorithm with new encoding method[J].Fuzzy Sets & Systems，2005，152(3)：617-635.
[9] 张宝林.电弧炉起弧阶段控制策略的研究[D].沈阳：东北大学，2013.
[10] 鲁军，霍金彪.基于 RBF 神经网络的电弧炉电极调节系统 PID 参数整定[J].电气工程学报，2017，12(4)：18-21.

(收稿日期：2019-12-06)

作者简介：
李强(1964-)，男，硕士，副教授，主要研究方向：嵌入式计算机控制与自动化装置、智能化设备与工业综合自动化系统。
卫敏(1994-)，女，硕士研究生，主要研究方向：控制工程。

(上接第 72 页)

道[J].工业控制计算机，2019，32(12)：:72-75.
[5] 区和坚.工业控制系统信息安全研究综述[J].自动化仪表，2017，389(7)：4-8.
[6] 王朝栋，张雪帆，栾少群.轻量级漏洞扫描技术在工控网络的应用[J].信息技术与网络安全，2019，38(12)：86-89.
[7] 王小山，杨安，石志强，等.工业控制系统信息安全新趋势[J].信息网络安全，2015(1)：6-11.
[8] 张家伟.基于 linux 的可信计算平台研究与实现[D].北京：北京邮电大学，2015.
[9] 邵诚，钟梁高.一种基于可信计算的工业控制系统信息安全解决方案[J].信息与控制，2015(5)：628-633.

(收稿日期：2020-03-23)

作者简介：
赵悦琪(1993-)，女，硕士，主要研究方向：工业控制系统。
赵德政(1985-)，男，博士，高级工程师，主要研究方向：工业控制系统。
林浩(1988-)，男，博士，工程师，主要研究方向：工业控制系统。

《电子技术应用》http://www.chinaaet.com

版权声明

经作者授权，本论文版权和信息网络传播权归属于《电子技术应用》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、DOAJ、美国《乌利希期刊指南》、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《电子技术应用》编辑部

中国电子信息产业集团有限公司第六研究所