

国

国

国务院

计划单

为

提高我

全,我

通知如

一

人

工业个

需求

重点

推进信息化领域薄弱环节的创新基础能力建设,增  
化优势,为经济结构战略转型与和谐社会建设提供

## 二、专项的建设重点

### (一)信息技术应用方面

1、电子商务交易技术国家工程实验室:针对我  
展过程中面临的共性技术需求,建设相关研究开发  
验环境,开展电子商务交易主体规范管理、市场信息  
测,以及安全电子合同、电子货币、电子发票等领域  
标准研究,为规范电子商务发展、深化电子商务应  
务服务产业发展提供技术支撑,以提高我国电子商  
力,增强我国电子商务国际竞争等优势。

2、电子政务建模仿真国家工程实验室:针对国  
求分析、系统研发和工程建设的技术需求,建设电  
模、逻辑验证、系统模拟和工程仿真等实验平台,研  
和逻辑验证基础理论,开展电子政务系统需求分析  
载计算、动态仿真等关键核心技术研发,以提升国家  
分析和系统研发的整体水平,降低电子政务系统信  
冗余率,提高电子政务投资效益,为国家电子政务技  
术支撑。

3、电子政务云计算技术国家工程实验室:围绕  
我国电子政务建设中的应用,建立完善电子政务公  
研发、测试和实验环境,开展测试验证和承载应用

研究  
身份  
进展  
资源

政务云平台  
和数据管理  
相关标准研究  
整合,提高电

度管理  
术,以  
为云计  
建设的

(二)信息安

信  
官  
办  
公  
室  
网  
站  
运  
行

1、网络安全  
信息安全事件预  
监测预警和应  
存储、数据信息  
级网络安全监  
络安全态势分  
急工作水平,为  
行提供技术支

国家工  
处置的  
的实验  
大规模  
定模、重  
键核  
家信息

2、信息安全

重要信息系统  
研究、示范实验平  
查、集中管控等安  
制、系统结构化、  
关键技术的研  
计算环境、安全区  
术产品,为重要作

关键技  
需求,  
究防范  
策略和  
究安全  
础上研  
、安全通  
安全管

3、互联网城

技术国家

信  
息  
安  
全  
研  
究  
报  
告

障器  
键台  
务域  
通  
究理  
管  
关  
体支  
电  
网  
平  
系  
脱  
业  
标

展的需  
安全十  
究的研  
真实现  
系统,为  
里提供  
互联网  
为网络  
证与测  
全技  
技术,  
究制订  
保障  
控制系  
水厂、  
等病  
工业控  
、嵌  
安全  
用与生  
建立,有

【摘要】随着我国信息化建设步伐的加快,工业控制系统的网络化、数字化、智能化程度越来越高,工业控制系统的安全问题日益突出。本文主要介绍了工业控制系统的安全威胁,并提出了相应的安全防护措施,包括物理安全、网络安全、应用安全、数据安全等方面,旨在提高工业控制系统的整体安全水平,保障工业生产的安全稳定运行。

关键词:工业控制系统;安全威胁;安全防护措施

随着工业4.0概念的提出和智能制造的兴起,工业控制系统作为工业生产的核心,其重要性不言而喻。然而,工业控制系统的安全问题也随之凸显。工业控制系统的安全威胁主要来自网络攻击、恶意软件、硬件故障等方面。这些威胁不仅可能导致生产中断,还可能造成严重的安全事故。因此,研究和提出有效的安全防护措施至关重要。

本文首先分析了工业控制系统的安全威胁,包括网络攻击、恶意软件、硬件故障等。接着,从物理安全、网络安全、应用安全、数据安全四个维度提出了相应的安全防护措施。最后,总结了工业控制系统安全防护的关键点,并展望了未来的研究方向。

### 1. 工业控制系统的安全威胁

工业控制系统的安全威胁主要来自以下几个方面:

- 网络攻击:黑客通过远程控制、木马植入等方式攻击工业控制系统,窃取数据或破坏生产。
- 恶意软件:病毒、蠕虫等恶意软件在工业控制系统中传播,导致系统瘫痪。
- 硬件故障:工业控制系统的硬件设备如PLC、DCS等出现故障,影响生产。
- 人为失误:操作人员误操作导致系统运行异常。

### 2. 工业控制系统的安全防护措施

针对上述安全威胁,提出了以下安全防护措施:

- 物理安全:加强工业控制系统的物理防护,防止未经授权的人员接触设备。
- 网络安全:部署防火墙、入侵检测系统、入侵防御系统等网络安全设备,防止网络攻击。
- 应用安全:对工业控制系统的软件应用进行安全评估,及时更新补丁,防止漏洞被利用。
- 数据安全:对工业控制系统的数据进行加密存储和传输,防止数据泄露。

### 3. 工业控制系统安全防护的关键点

工业控制系统安全防护的关键点包括:

- 安全策略:制定完善的安全策略,明确安全责任。
- 安全评估:定期进行安全评估,发现并及时修复安全漏洞。
- 安全培训:加强对操作人员的培训,提高安全意识。
- 应急响应:建立应急响应机制,提高应对安全事件的能力。

### 4. 结论

工业控制系统的安全问题关系到工业生产的安全稳定运行。只有采取全面、有效的安全防护措施,才能保障工业控制系统的安全,确保工业生产顺利进行。

From:

国家

重要基础

信

6、计算机

需

网络安全

病

,建设计

三

监测与应

特

移动通

核

提取、针

联

技术研

全

应用带

和防范网

### 三、具体

行

(一)请

暂

》(国家

速

行办法》(

报告编制

的

(二)主

关

资金、节

费

附件(如

对其真实

告

(三)请

报告一

川外特

1. 率上

府博

书和产

究研

代及

APD)

信、元

以的知

、博。

照《

4)、《

政府

川外特

川外特

附件

华以

、川外

7.3

附件六

附件七

附件八

附件九

附件十

附件十一

附件十二

附件十三

附件十四

附件十五

附件十六

附件十七

附件十八

附件十九

附件二十

附件二十一

附件二十二

附件二十三

附件二十四

附件二十五

材料。

特此通知。

