

工业控制系统信息安全状况量化分析的研究

□ 浙江温州市公用事业投资集团有限公司 (325000) 傅弘弼

摘 要: 为有效而直观的表现各单位工业控制系统信息安全状况,采用传统信息安全风险评估思路,结合工业控制系统特点,定义信息安全各关键要素并采用相乘法计算出安全风险值。实例证明,该方法易于掌握,简单明了,能有效反映安全风险。为技术人员掌握企业内部工业控制系统安全风险状况提供简便有效的方法。

关 键 词: 工业控制系统 信息安全 风险评估 量化分析

Quantitative Research on Status for Information Security of Industrial Control System

Fu Hongbi Wenzhou Public Utilities Investment Group Co.,Ltd

Abstract: It is perform status for information security of Industrial Control System in each company. The risk assessment method for information security of Industrial Control System based on traditional ideas on risk assessment for information security and characteristics of industrial control systems. The key element was defined for information security of Industrial Control System and used a calculate method. The practical example indicates that the method is easy and effectively quantitative the security risks. It can provide a simple and effective method for technical staff on Information security of Industrial Control System.

Keywords: Industrial Control System Information Security Risk Assessment Quantitative Analysis

1 引言

供水、供气、排水涉及到千家万户的日常生活,假如供水、供气、排水的调度系统、DCS等工业控制系统遭到攻击,停水、停气、漏气、爆管等任何一件事事故发生,都将产生严重的后果。工信部〔2011〕451号文件《关于加强工业控制系统信息安全管理的通知》明确城市供水供气作为与国计民生紧密相关的

重点领域加强工业控制系统信息安全管理要求。由于工业控制系统涉及的行业和控制面不同,系统结构和原理千差万别、系统所起的作用又各不相同,同时各企业管理人员技术水平参差不齐,因此本人研究设计一种简便有效的方法快速、准确的判断本企业内部各工业控制系统信息安全状况,近而为实施恰当的安全防护提供有力依据。

由于国内外还没有一套行之有效的针对工业控制

系统信息安全风险量化评估方法,本人采用传统信息安全风险评估思想,结合本单位供水、供气等工业控制系统特点,定义一套工业控制系统量化评估方法。

2 信息安全风险分析

信息安全风险评估围绕资产、威胁、脆弱性和安全措施这些基本要素展开,在工业控制系统的风险评估过程中,需要针对工业控制系统的特点有针对性的识别出资产、威胁、脆弱性,进而采用信息安全风险分析原理,计算出安全风险值。如图1所示。

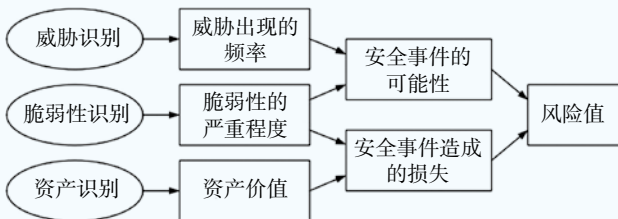


图1 信息安全风险分析原理

2.1 资产识别

工业控制系统的资产价值主要在于该系统对工业生产的作用,而它的价值主要体现在生产过程中对该系统的依赖程度。通过分析生产过程中对工业控制系统的依赖程度定义三个等级,分别为高、中、低,如表1。

表1 系统依赖程度

依赖程度	描述
高	完全依赖系统,全自动控制生产
中	由人员参与,半自动控制生产
低	系统作为辅助手段,仍全部由人员进行操作

2.2 脆弱性识别

工业控制系统脆弱性识别主要从系统设计结构、产品安全性、管理3大方面进行识别。

(1) 系统设计结构:通过检查系统架构、拓扑,网络结构等直观分析和判断。定义系统设计结构的安全程度分三个等级,分别为高、中、低,如表2。

(2) 管理安全性:通过核对、检查是否针对工业控制系统建立相应的规章制度,明确安全责任,规

表2 系统设计结构安全性

安全程度	描述
高	采取多手段、多种技术进行安全保护
中	采取了一些安全手段进行安全保护。但仍表现出部分的脆弱性
低	没有采取任何相关安全手段进行保护,结构上存在多方面脆弱性

范操作流程,从管理角度判断系统防护的安全性。此项定义分为有和无二个等级,如表3。

表3 管理安全性

管理安全性	描述
有	以文字形式明确了相关安全管理制度
无	无任何针对系统的安管理制度

(3) 产品安全性:通过查找相关材料对工业控制系统相关产品如PLC、SCADA、组态软件等已公开的漏洞进行确认,来判断该系统的安全性。此项定义产品安全性分为两个等级,分别为高和低,如表4。

表4 产品安全性

产品安全性	描述
高	未被发现或公开的安全漏洞
低	已被发现存在可被用于攻击的安全漏洞

2.3 威胁识别和分类

工业控制系统威胁主要来自外部环境和人为因素。外部环境威胁主要表现为软硬件故障、网络攻击、严重自然灾害如地震、火灾等物理环境影响;人为因素主要表现为管理不到位、越权、操作失误、非授权访问或操作。根据威胁可能发生的频率将主要威胁分为三个等级,分别为高、中、低,如表5。

表5 威胁的识别和分类

威胁频率	描述
高	外部环境和人为因素的威胁发生的频率非常高
中	外部环境和人为因素的威胁发生的频率中等
低	外部环境和人为因素的威胁发生的频率非常低

3 安全风险的量化分析

3.1 各要求要素赋值

资产价值主要依旧生产过程对系统依赖程度，高、中、低进行赋值，如表6。

表6 资产价值赋值

依赖程度	标识	分值
高	A1	5
中	A2	3
低	A3	1

脆弱性要素从系统设计结构、产品安全性、管理安全性3个方面分别进行赋值，具体见表7。

表7 脆弱性各要素赋值

脆弱性要素	等级	标识	分值
系统设计结构	高	V11	1
	中	V12	3
	低	V13	5
管理安全性	有	V21	1
	无	V22	5
产品安全性	高	V31	1
	低	V32	5

威胁要素分类赋值，如表8所示。

表8 威胁要素分类赋值

威胁性	标识	分值
高	T3	5
中	T2	3
低	T1	1

3.2 安全风险计算公式

本量化评估计算方法参考《BG/T20984-2007信息安全风险评估规范》，采用相乘法计算风险值。相乘法主要用于两个或多个要素值确定的一个要素值的情形，即 $Z=f(x, y)=\sqrt{x \times y}$ 。

安全风险的计算的过程如图1，计算发生安全事

件的可能性和安全事件的损失，然后 再计算得到安全风险值具体公式如下：

发生安全事件的可能性：

$$f(\text{威胁}, \text{脆弱性}) = \sum \sqrt{\text{威胁} \times \text{脆弱性}} / 3$$

计算安全事件的损失：

$$f(\text{资产价值}, \text{脆弱性}) = \sum \sqrt{\text{资产价值} \times \text{脆弱性}} / 3$$

计算安全风险值：

$$f(\text{安全事件可能性}, \text{资产损失}) = \sqrt{\text{可能性} \times \text{损失}}$$

定义一张安全风险值与安全状况对应表，可以更直观简单的表述系统安全状况，如表9 所示。

表9 安全风险值与安全状况对应表

风险值	0~2.0	2.01~4	4.01~5
安全状况	到位	一般	差

4 实例论证

我集团下属燃气公司燃气调度系统部署在燃气公司信息中心，通过实时接收全市43个监测点的燃气管网压力数据，场站阀门数据分析判断全市燃气供应情况、燃气压力。燃气公司调度中心工作人员依据调度系统数据分析判断并进行指挥调度。燃气公司信息安全管理人员依据量化评估方法对燃气调度系统进行安全要素识别，安全风险计算。

4.1 系统安全相关要素描述

(1) 系统依赖程度

燃气公司调度中心采用人工调度方式进行燃气送气调度，燃气调度系统进行数据采集，起到决策参考作用。

通过访谈交流，我们可以知道系统只作为辅助调度的参考，即使系统故障无法显示或者数据显示错误，调度中心仍可通过电话联系现场工作人员综合判断进行调度。所以从生产过程对此系统的依赖程度来讲，可以定义为低。

(2) 系统设计结构

燃气调度系统场站监控组态软件采用IFIX，管网压力检测采用某厂商的GCI软件，采用PLC终端数据

采集和发送装置,场站数据通过电信光纤传输到机房服务器,管网压力数据通过移动GPRS传输到机房服务器。机房部署一台数据库服务器和一台数据采集服务器。具体网络拓扑如图2。

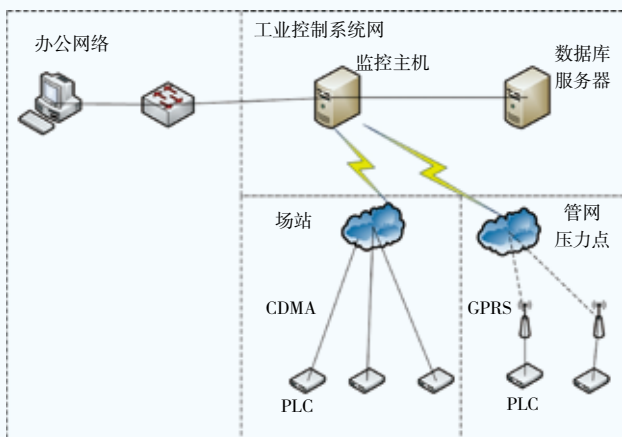


图2 调度系统网络拓扑图

通过对网络拓扑分析我们发现系统存在如下问题:

系统直接与办公网连接,工业控制网与办公网直接连接无任何隔离措施。

数据库服务器和数据采集服务器均为单机运行,无备用设备。

PLC数据采用GPRS通过互联网传输,未使用加密和防篡改技术。

根据系统描述,管网调度系统仅采用了简单的安全措施,存在多种脆弱性,因此该系统的安全程度定义为低。

(3) 产品安全性

燃气调度系统采用某厂商GCI组态软件和IFIX组态软件,通过比对产品型号和版本,查找VCE漏洞库发现IFIX产品发现多处漏洞,所以安全可靠性的定义为低。

(4) 系统管理

燃气公司针对燃气调度系统制定了《计算机和网络数据安全管理制度》、《网络运行及设备管理制度》、《机房管理制度》、《调度管理系统操作规范》因此从管理方面的安全措施定义为有。

4.2 威胁分析

根据以上描述分析,燃气调度系统可能存在网络

攻击、软硬件故障等威胁,相关威胁发生的可能性定义为高。

4.3 系统安全状况确定

该资产价值: $A3=1$; 脆弱性表项: $V13=5, V21=1, V32=5$; 威胁性表项: $T3=5$

通过计算公式:

计算安全事件发生可能性: $\Sigma \sqrt{\text{威胁性} \times \text{脆弱性}}/3$

$$=(\sqrt{T3 \times V13} + \sqrt{T3 \times V21} + \sqrt{T3 \times V32})/3=4.07$$

计算安全事件的损失: $\Sigma \sqrt{\text{资产价值} \times \text{脆弱性}}/3$

$$=(\sqrt{A3 \times V13} + \sqrt{A3 \times V21} + \sqrt{A3 \times V32})/3=1.82$$

计算安全风险值: $\sqrt{\text{可能性} \times \text{损失}}=2.72$

根据安全风险值与安全现状对应表,燃气调度系统安全保护现状一般。

5 结束语

本文针对工业控制系统信息安全风险评估问题,结合传统IT系统信息安全风险评估理论和工业控制系统特点,定义了一套量化评估方法,通过该方法可以简单明了的判断工业控制系统安全状况,且对于分公司众多,工业控制系统各不相同的行业,通过简单评估可以很好的对比和掌握情况。但该方法在确定各安全要素进行赋值时,仍存在受主观不确定因素影响,需要进一步细化和量化,以达到很好的准确性。

参考文献

中国国家标准委员会 GB/T 20984-2007 信息安全技术信息安全风险评估规范[S]. 中国标准出版社

主办:中国城市燃气协会信息委 咨询电话:010-62032933



燃气
资讯

为促进会员单位信息的交流和发展服务