·信息技术·

现代港口信息安全评价体系

吴静媛，周鹏颖
（中交水运规划设计院有限公司，北京 100007）

摘要：从港口信息安全保障工作需求出发，以工作层面、保障要素、指标类型为主要方向，设计一套针对现代港口信息化建设的信息安全三维评价指标体系框架，并结合国家对港口信息安全的相关要求，分析出 56 个具体指标，提出评价指标的量化方法和计算方法，可为港口信息安全自评价提供参考。

关键词：港口信息化；信息安全；评价指标体系
中图分类号：TP 391　　**文献标志码：**A　　**文章编号：**1002-4972(2015)05-0168-06

Evaluation index system for modern port information security

WU Jing-yuan, ZHOU Peng-ying
(CCCC Water Transportation Consultants Co., Ltd., Beijing 100007, China)

Abstract: According to the demand of port information security, we design a set of three-dimensional framework of the evaluation index system considering mainly the work level, security, and index types. Besides, combining with relevant requirements from the state on the port information security, we analyze 56 specific indices and propose the quantitative method and calculation method for the evaluation indices, which may serve as reference for the evaluation of port information security.

Keywords: port informatization; information security; evaluation index system

1　信息安全评价体系的概念及研究现状

信息安全评价体系以实现系统安全为目的，应用系统工程原理和方法，对信息系统中存在的危险、有害因素进行辨识与分析，判断信息系统发生安全事件的可能性及其严重程度，从而为制定防范措施和管理决策提供科学依据。

目前应用最广泛的信息安全管理、评价标准是 ISO/IEC27001 和 ISO/IEC27002 及其标准系列。美国、英国、日本等信息技术先进的国家在信息安全保障评价指标体系方面已经率先开展了研究工作。特别是美国，利用系统安全工程能力成熟度模型 SSECMM 较早地建立了信息安全保障评价指标体系[1]。该模型是一个过程参考模型，关注的是信息技术安全（ITS）领域内某个系统或者若干相关系统实现安全的要求。我国从 20 世纪 90 年代中期即开始制定关于信息安全的标准，GB 17859—1999《计算机信息系统安全保护等级划分准则》是其他标准的基础，为安全保护工程的管理、实施提供指导。2000 年我国开始有计划地研究制定信息安全评价标准，并直接应用于我国的信息安全测评认证工作。目前，我国主要用来对信息系统安全保障进行评价的模型是 2006 年实施的国家标准 GB/T 20274.1—2006《信息安全技术信息系统安全保障评估框架》[2]。

国内外各标准为港口信息安全保障工作的评价提供了一定程度的指导，然而，由于标准是面向各类行业、各类组织的通用性规则，目前在电力行业、石油行业、交通行业等领域，甚至是一些大中型企业中，都有按照标准制定信息安全评价体系的先例，也取得了一定的效果，但由于各

收稿日期：2014-09-17

作者简介：吴静媛（1983—），女，硕士，从事信息工程及信息安全类研究工作。

行业对信息安全评价的需求不同，而标准又通用性较强，缺乏针对性，所以港口企业需要在其指导下进一步细化考核点，形成自身的评价体系。

2　港口信息安全评价现状及需求

港口信息安全保障应贯穿在港口信息系统的整个生命周期中。港口信息安全保障的工作者应针对港口信息系统的发展特点，通过对港口信息系统的风险分析，制定并执行相应的安全保障策略，从多角度、多层面提出港口信息安全保障要求，确保港口信息系统的保密性、完整性和可用性，将安全风险降至最低或可接受的程度。

港口信息化发展重点主要在于对外的数据交换和服务。港口信息安全风险主要来自于港口信息系统自身存在的漏洞和系统外部的威胁。为最大化控制该风险，港口信息系统安全保障工作者应在信息安全保障策略体系的指导下，设计并实现港口信息安全评价体系架构或模型，港口信息安全评价体系的制定应反映港口企业对信息系统安全保障及其目标的理解，其制定和贯彻执行对信息系统安全保障起着纲领性指导作用。港口信息安全评价体系应选用一种折中的机制，在有限资源前提下实现最优选择。防范不足会造成直接的损失，防范过多又会造成间接的损失，在解决或预防安全问题时，要从经济、技术、管理的可行性和有效性上做出权衡和取舍。

从现代港口企业信息安全保障工作者的视角出发，其工作层面无外乎对港口信息安全保障的战略管理、常态监管和应急响应。战略管理体现其信息安全战略的先进性，表现在港口企业对信息安全战略规划的制定情况、港口信息安全管理部门的战略地位和港口企业对信息安全工作的资金保障力度等。这些评价能反映港口企业对信息安全的重视程度，预见港口企业信息安全工作未来的发展前景。常态监管主要指港口信息安全战略的具体执行情况，包括基于对港口业务风险的认识，建立、实施、操作、监视、复查、维护和改进信息安全等一系列管理活动，具体表现为计划活动、目标与原则、人员与责任、过程与方法、资源等诸多要素的集合。应急响应主要包括在一些紧急、无预测的危机下，快速应对、解决问题的能力，度过危机以减少损失或者把损失降低到最低程度。

3　现代港口信息安全评价指标体系框架

为了让指标体系更加科学、全面、综合，力争每个门类的指标定量、定性相结合，笔者选用了工作层面、保障要素、指标类型作为现代港口企业信息安全保障指标体系框架的 3 个维度[3]。现代港口企业信息安全保障指标体系框架如图 1 所示。

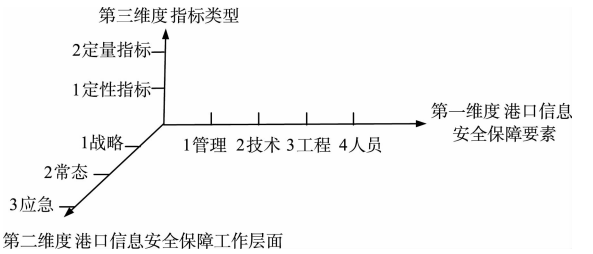

图 1　现代港口信息安全评价指标体系框架

该评价指标体系的主要特点为：

1）从港口信息安全保障工作者的角度出发，将长期战略与日常管理、控制相结合，既反映了决策人员的视角，也反映了管理人员、维护人员的视角。

2）强调综合保障的观念。通过技术、管理、工程和人员的安全保障要求来实施和实现信息系统的安全保障目标。

3）强调科学、客观。合理分配每个考核点的定量指标、定性指标所占比重。定性是个模糊界限，定量则是有清晰的数据分析问题，二者结合，就能更好地制定评价方案。

4　评价指标

按照评价指标体系框架，采用第一维度、第二维度、第三维度逐个相交的方式，对各评价点进行分解，可以设计出适应现代港口企业信息安全保障工作的评价指标体系。为了让指标体系更加科学、可操作，笔者在对上海港、黄骅港等大中型港口调研的基础上，梳理分析，设计出一套普适性较强的评价指标体系。该体系能够较客观、准确、全面地反映港口信息安全工作水平，供港口企业信息安全保障工作者参考（表 1）。

表 1　现代港口信息安全评价指标

第一维度	第二维度	第三维度	评价指标
管理	战略	定性	结合港口企业发展战略,制定了与之相适应的信息安全规划
			有港口企业信息安全工作领导小组
			港口信息安全归口管理部门的职能定义明确
			港口企业信息安全管理体系完善,相关管理制度完备
		定量	信息安全规划年限
			港口企业信息安全工作领导小组成员来自业务部门/业务部门总数
	常态	定性	定期召开信息安全领导小组会议,并有会议纪要
			港口二级部门、二级单位信息安全考评纳入对相关负责人年度业绩考核
			建立了信息安全防护策略,并进行了评审
			定期进行信息安全测评与风险评估
			与第三方服务机构签订有保密协议
		定量	信息安全领导小组会议周期
			信息安全考评分值/考核总分值
			信息安全测评与风险评估周期
	应急	定性	制定了网络与信息安全应急预案,具备完善的信息安全应急防范措施
			定期开展应急预案演习
			是否发生过重大信息安全事件
			发生信息安全事件后是否及时上报信息安全工作领导小组及上级主管部门
			信息安全事件的处理是否及时,控制是否到位
			是否建立有信息安全通报机制及问责机制,开展信息安全通报及问责工作
		定量	信息安全事件数量
			信息安全损失级别
技术	战略	定性	港口企业信息安全标准体系完善,相关标准完备
		定量	港口企业信息安全标准数量
	常态	定性	实现港口应用系统的监测、分析、预警
			实现港口网络设备的监测、分析、预警
			实现港口安全设备的监测、分析、预警
			实现港口主机安全的监测、分析、预警
			实现港口物理安全的监测、分析、预警
		定量	安全产品种类
	应急	定性	是否有本地备份
			是否有异地备份
		定量	备份恢复周期
工程	战略	定性	具有年度信息安全建设计划
			港口信息安全投入有独立的年度预算
		定量	港口信息安全预算占本年度收入的比例
	常态	定性	港口年度信息安全建设计划执行情况良好,各项年度目标均完成
			所有新建系统在设计前开展系统定级工作
			系统设计方案中有对信息安全防护策略的考虑
			外包软件安装之前检测软件包中可能存在的恶意代码
			制定详细的信息安全工程实施方案控制实施过程,并要求工程实施单位能正式地执行安全工程过程;
			系统验收前委托公正的第三方测试单位对系统进行安全性测试,并出具安全性测试报告
		定量	信息安全建设投资占本港口企业年度收入的比例
	应急	定性	制定了信息安全建设的应急预案
		定量	信息安全工程中的安全事件数量
			信息安全工程中的重大安全事件损失级别

续表

第一维度	第二维度	第三维度	评价指标
人员	战略	定性	结合港口企业人才战略，制定了与之相适应的信息安全专业人才引进计划
			结合港口企业人才战略，制定了与之相适应的信息安全专业人才培养计划
		定量	计划年引进/培养信息安全专业人才数量
	常态	定性	在人员招聘、离职环节是否有保密管理规定或签订了保密责任书
			定期开展全员信息安全培训
			定期开展信息安全专业人员培训
		定量	全员信息安全培训开展周期
			信息安全专业人员培训周期
	应急	定性	是否发生过有重大影响的人员泄密事件
		定量	人员泄密事件造成的损失级别

5　评价办法

为保证评价结果可比较，应对港口信息安全评价指标的总值进行量化。

定性指标可将指标的符合程度分解为几个层次，例如“很好、好、一般、差”，即确定评语集为 $\boldsymbol{V}=\{V1,V2,V3,V4\}=\{$很好,好,一般,差$\}=\{100$ 分,80 分,60 分,40 分$\}$。由若干位专家分别对每项指标进行单因素评价，若 50% 认为很好，40% 认为好，10% 认为一般，则该项指标的单因素评价结果 $R_{ij}=(0.5,0.4,0.1,0)\times(100,80,60,40)^{\mathrm{T}}=88$，$j$ 为第三维度 i 中评价指标的序号[5]。

若港口企业为单级组织机构，定量指标的评价可仍采用上述方法；若港口企业为多级组织机构，可采用“比率计算法”，将不同单位机构的同一指标相互比较，求出比率，进而得到该项指标的评价分值[4,6]。

港口企业评价指标的总值为：

$$I=\sum_{j=1}^{n}\sum_{i=1}^{m}R_{ij}W_{ij} \tag{1}$$

式中：W_{ij}为单项指标的权重。

6　实例分析

选取调研中涉及的 3 个港口进行信息安全评价。3 个港口分别为河北省沿海某港口、山东省某沿海港口、长江内河某港口。所有港口均为单级组织机构，借助文中评价方法对该港口信息安全情况给予分值计算。

其中，河北省沿海某港口分值最高，评价指标见表 2。

表 2　河北省沿海某港口信息安全评价实例

第一维度	第二维度	第三维度(i)	R_{ij}	W_{ij}	说明
管理	战略	定性	82	0.025	已完成了规划的基本编制，但内容仍需完善。
			85	0.025	有信息安全工作领导小组，但结构需完善
			88	0.012	信息安全归口管理部门的职能定义基本明确
			88	0.008	具备主要的信息安全管理制度
		定量	75	0.005	信息安全规划年限明确，为三年
			70	0.015	根据实际情况测算
	常态	定性	70	0.015	不定期召开信息安全领导小组会议，会议纪要不完整
			82	0.020	港口二级单位信息安全考评纳入对相关负责人年度业绩考核，但考核机制不严谨
			86	0.020	建立基础的信息安全防护策略，并进行了评审
			70	0.020	信息安全测评一次，风险评估未做
			76	0.010	与部分第三方服务机构签订有保密协议
		定量	70	0.010	信息安全领导小组会议周期不定
			72	0.020	根据实际测算
			78	0.020	信息安全测评与风险评估周期不定

续表

第一维度	第二维度	第三维度(i)	R_{ij}	W_{ij}	说明
	应急	定性	76	0.025	制定有网络与信息安全应急预案
			74	0.025	不定期开展应急预案演习
			82	0.022	基本未发生过重大信息安全事件
			82	0.020	发生信息安全事件后根据情况上报
			82	0.020	信息安全事件处理及时
			82	0.020	有简单的信息安全通报机制及问责机制
		定量	86	0.015	根据实际情况测算
			82	0.025	根据实际情况测算
技术	战略	定性	78	0.020	没有完整的企业信息安全标准体系
		定量	76	0.020	根据实际情况测算
	常态	定性	72	0.010	基本未实现应用系统的监测、分析、预警
			84	0.010	基本实现网络设备的监测、分析、预警
			76	0.010	部分实现安全设备的监测、分析、预警
			76	0.010	部分实现主机安全的监测、分析、预警
			86	0.010	基本实现港口物理安全的监测、分析、预警
		定量	80	0.020	根据实际情况测算
	应急	定性	88	0.020	有本地备份
			70	0.020	无异地备份,但有同城双机房
		定量	88	0.020	根据实际情况测算
工程	战略	定性	76	0.018	有小规模年度信息安全建设计划
			78	0.015	有相对独立的年度预算
		定量	84	0.020	根据实际情况测算
	常态	定性	82	0.020	建设计划执行情况相对良好
			80	0.020	重要系统在设计同期开展系统定级工作
			80	0.020	重要系统设计中有对信息安全防护策略的考虑
			76	0.020	少量外包软件安装之前检测恶意代码
			78	0.020	制定有信息安全工程实施方案控制实施办法
			78	0.020	重要系统验收前委托测试单位安全测试
		定量	80	0.020	根据实际情况测算
	应急	定性	86	0.020	制定了基本的信息安全建设的应急预案
		定量	80	0.020	根据实际情况测算
			80	0.020	根据实际情况测算
人员	战略	定性	72	0.020	没有明确的信息安全专业人才引进计划
			72	0.020	没有明确的信息安全专业人才培养计划
		定量	78	0.020	根据实际情况测算
	常态	定性	78	0.020	在人员离职环节签订保密责任书
			76	0.020	不定期开展全员信息安全培训
			78	0.020	不定期开展信息安全专业人员培训
		定量	70	0.010	开展过一次全员信息安全培训
			70	0.010	开展过一次信息安全专业人员培训
	应急	定性	80	0.020	基本未发生过重大影响的人员泄密事件
		定量	86	0.020	人员泄密事件造成的损失基本可控

评价指标的总值为 $I=79$，与 3 家港口企业评价指标总值相比，信息安全情况总体最优。

7 结语

1）信息安全评价体系对于现代港口评价信息

安全保障工作的完备性，最大化降低、控制信息安全风险，减少技术故障、网络攻击等安全问题对业务带来的影响具有十分重要的作用。

2）以现代港口企业信息安全保障工作为研究对象，遵循科学全面、简单可操作、向导性原则，从工作层面、保障要素、指标类型出发，设计了一套三维评价指标体系框架，并结合国家对港口企业信息安全的相关要求，分析出 56 个具体指标，提出了评价指标的量化方法和计算方法，可为港口企业信息安全自评价提供参考。

3）取 3 个港口的信息安全保障工作情况样本进行评价，对评价分值的取值进行分析。试验表明，该方法能够满足现代港口的信息安全评价需求，简单可操作，具备可行性。

参考文献：

[1] 曹鹏, 张永平. 网络信息安全技术初识[J]. 徐州工程学院学报, 2005, 20(5): 62-64.

[2] 都骏, 刘瑞, 黄孝羽, 等. 石油企业信息安全评价方法的研究[J]. 科技管理研究, 2012, 32(18): 208-213.

[3] 李嘉渊. 信息化建设、信息安全保障和信息安全评价指标体系[J]. 信息通信, 2012(4): 117.

[4] 林正奎. 基于 VaR-Copula 的信息安全评价模型研究[J]. 数学的实践与认识, 2012, 42(8): 85-90.

[5] 周权. 基于代数方法的信息安全风险评估管理模型[J]. 通信技术, 2008, 41(7): 2-3.

[6] 杜雪涛, 李友国, 袁捷, 等. 基础信息安全评估体系及方法研究[J]. 电信工程技术与标准化, 2011(10): 20-24.

（本文编辑　郭雪珍）

（上接第 152 页）

4）长江口的台风造成的航道骤淤量达到数百万立方米，是深水航道回淤量的重要组成部分；

5）大风引起的航道骤淤量主要分布在北槽航道的中下段。

参考文献：

[1] 赵德招, 刘 杰, 吴华林, 等. 近十年来台风诱发长江口航道骤淤灾害的初步分析[J]. 泥沙研究, 2012(2): 63-69.

[2] 顾伟浩. 台风对长江口铜沙航槽回淤的影响[J]. 海洋科学, 1986, 10(1): 60-62.

[3] 顾伟浩. 长江口北槽航槽回淤强度预估[J]. 上海水利, 1996(4): 43-44.

[4] 孔亚珍, 史峰岩, 朱首贤. 长江口南港北槽风暴回淤统计模型[J]. 华东师范大学学报: 自然科学版, 2003(4): 80-86.

[5] 徐福敏, 张长宽. 台风浪对长江口深水航道骤淤的影响研究[J]. 水动力学研究与进展, 2004, 19(2): 137-143.

[6] Kong L S, Wan Y Y. Calculation of typhoon-induced sudden siltation using effective wind energy in Yangtze estuary[C] //OMAE, 2010.

（本文编辑　郭雪珍）

（上接第 167 页）

6　结语

1）根据《规范》对各种船舶长度与吨位拟合，并根据载运量选取船型，所得到的标准船能较好地反映该航道的航运情况，数据比较准确。

2）利用交通流及跟驰理论相结合的方法，对标准船进行运算得出的船速能较具体地表示出航道航速，为航道限速提供了一种较准确的定量化计算方法。

参考文献：

[1] Elisabeth M, Goodwin J F Kemp. The optimal speed of ships[J]. The Journal of Navigation, 1979, 32(3): 291-308.

[2] 洪碧光, 王逢辰, 古文贤, 等. 安全航速与航速风险性分析[G] //中国航海学会海洋船舶驾驶专业委员会论文集(1995—1997). 北京: 中国航海学会海洋船舶驾驶专业委员会, 1997: 103-111.

[3] 杨帆, 刘康, 郭国平. 船舶安全航速的定量模糊研究[J]. 航海技术, 2013(4): 67-69.

[4] 陈国生, 杨皓森, 刘文斌. 基于神经网络的安全航速的计算[J]. 广州航海高等专科学校学报, 2006, 14(2): 13-15.

[5] 张生瑞. 交通流理论与方法[M]. 北京: 中国铁道出版社, 2010: 89-92.

[6] 董宇, 姜晔, 何良德. 内河航道通过能力计算方法研究[J]. 水运工程, 2007(1): 59-65.

（本文编辑　武亚庆）