文章编号：1005-8451（2020）08-0038-06

建立铁路三位一体网络安全测评指标库研究

司　群[1]，田　文[2]，陈　彤[1]
（1.中国铁道科学研究院集团有限公司　电子计算技术研究所，北京　100081；
2.中国铁路太原局集团有限公司　科技和信息化部，太原　030027）

摘　要：通过对铁路典型的网络安全等级保护测评、风险评估测评和安全检查3类检测方法有机融合，研究建立铁路三位一体网络安全测评体系，重点解决如何高效测评问题。建立铁路网络安全测评指标库是解决上述问题的关键和基础步骤，指标库主要包括通用指标和专用指标，其中，通用指标按照网络安全等级保护2.0标准（简称：等级保护2.0）梳理出安全通用指标、云扩展指标、物联网扩展指标、移动互联网扩展指标和工业控制扩展指标；专用指标重点考虑业务安全，从完整性、保密性、可用性出发梳理铁路重要系统的测评指标。运输调度管理信息系统的专用指标、网络安全测评指标库作为现场开展测评工作的基本依据和参考，具有实际意义。

关键词：测评指标；通用指标；专用指标
中图分类号：U29 : TP393　**文献标识码：**A

Establishment of railway trinity network security evaluation index database

SI Qun[1], TIAN Wen[2], CHEN Tong[1]
(1. Institute of Computing Technologies, China Academy of Railway Sciences Corporation Limited, Beijing　100081, China; 2. Department of Science, Technology and Information Technology, China Railway Taiyuan Group Co. Ltd., Taiyuan　030027, China)

Abstract: Through the organic integration of three typical railway detection methods, which were network security classified protection evaluation, risk assessment and security inspection, this article studied the establishment of railway trinity network security evaluation system, focusing on how to achieve efficient evaluation.The establishment of railway network security evaluation index database was the key and basic step to solve the above problems. The index library mainly included general indicators and special indicators. According to the network security level protection 2.0 standard, the general indicators were sorted out the general security indicators, cloud expansion indicators, Internet of Things expansion indicators, mobile Internet expansion indicators and industrial control expansion indicators.The special indicators were focused on business security and sorted out the evaluation index of important railway systems from the perspective of integrity, confidentiality and availability evaluation index.The special index and network security evaluation index database of transportation dispatching management information system are the basis of on-site evaluation, which has practical significance.

Keywords: evaluation index; general indicator; specific index

国家法律法规明确要求对于交通、能源等重要行业和领域的国家关键信息基础设施应实施重点保护[1]。铁路作为交通行业的重要组成部分，其重要系统被纳入到国家的网络安全重点防护范围，每年需配合国家互联网信息办公室、公安部等部门开展安全风险评估、等级保护测试、攻防演练等工作，遇到重要国事活动，也需对相关地区的铁路局集团有限公司范围内重要系统开展有针对性的网络安全检查。

当前，中国国家铁路集团有限公司（简称：国铁集团）在贯彻国家网络安全相关的法律法规、加强铁路系统安全防护方面开展安全检查和测试工作，但是同一时期针对不同部门的要求，对同一系统可能会开展等保测评、风险评估、安全检查等不同类型的安全测评工作。另外，除等级保护测评可依据国家标准开展相关工作外，安全检查和风险评估工作的检查范围、内容、流程、指标和方法没有统一的标准，各测评机构掌握的尺度不一致，给安全评判工作带

收稿日期：2020-03-30
基金项目：中国铁路总公司科技研究开发计划课题（K2018S002）
作者简介：司　群，工程师；田　文，工程师。

来不确定性。所以，研究提出了铁路三位一体网络安全检测方法，从测评内容、测评方法、测评指标及测评流程几个方面梳理关键检测技术。

1　铁路三位一体网络安全测评体系概述

1.1　典型铁路测评工作介绍

（1）铁路网络安全等级保护测评工作是为了梳理铁路各部门系统重要程度和系统安全保护措施是否合规，结合等级保护 2.0 对系统开展合规性验证；

（2）铁路风险评估测评工作是为了评估系统整体安全风险，结合风险评估标准对系统资产存在的脆弱点、面临的威胁和存在的安全风险进行定量和定性的认识；

（3）铁路安全检查工作是为了全面了解铁路各单位网络安全总体状况和网络安全工作落实情况。

3 类安全检测工作在测评目的、测评对象选择、测评内容、测评流程和数据采集等方面存在着较多的一致性和关联性 [2]，总结如下。

（1）测评目的：均是为了发现铁路系统存在的安全隐患和面临的安全威胁，及时掌握系统安全状况，修复漏洞，降低安全风险，确保系统平稳运行。

（2）测评对象选择：均应覆盖机房物理环境、网络 / 安全设备、主机设备、业务系统 / 网站、各类数据、管理制度规范、安全人员等方面。

（3）测评内容：围绕系统资产开展检查和测评，测评内容包括技术安全测评和管理安全检查两方面。技术安全检测主要包含物理环境安全、通信网络安全、区域边界安全、计算环境安全、安全管理中心和工具测试；安全管理测评主要包含安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理方面内容 [3-4]。

（4）测评流程：均可分为测评准备、方案编制、现场实施、数据分析和报告编制 4 个阶段 [5]。测评准备包括组建项目实施团队，开展系统资产调研；方案编制包括确定测评依据、测评内容和测评范围，编纂测评方案、进度计划，调试检测工具；现场实施包括对被测评对象进行物理、网络、设备、应用、数据和管理等方面的安全检查，识别资产存在的脆弱点和可能面临的安全威胁，梳理已有安全防护措施，记录现场检测结果；报告编制包括对现场采集证据数据和测评结果进行整理分析，通过等保测评结论判定或风险分析模型计算，给出测评结论，编制 3 类测评报告。

（5）数据采集：都可通过漏洞扫描、渗透测试、配置核查等方法和测试工具采集测试数据。

1.2　铁路三位一体网络安全测评体系

尽管等级测评、风险评估和安全检查 3 类测评方法之间保持一致性，但其在分析方法和结果输出方面却存在差异性。

（1）等级测评需要对每个测评对象进行单元测评项分析和整体测评分析，并对被测系统做出安全等级的符合性评价，输出等级测评报告。

（2）风险评估需要结合测评结果对资产赋值、脆弱性赋值、威胁的赋值，依据风险计算模型计算风险值，判定风险等级，对风险进行评价并输出风险评估报告 [6]。

（3）安全检查是根据对抽测对象的检查结果，分析被查单位的网络安全现状，发现单位存在的安全问题，确认单位网络安全措施落实情况，输出安全检查报告。

通过上述分析，等级测评、风险评估和安全检查 3 类测评方法既有共性，又存在差异。所以，需要融合以上 3 类测评方法，形成三位一体测评方法，从其共性出发，结合各自特征，实现通过开展一次性采集数据，同步完成等级测评、风险评估和安全检查不同类检测报告输出的目标。

2　建立铁路三位一体网络安全体测评指标库

2.1　测评指标库结构介绍

本文提出建立铁路网络安全测评指标库，指标库包括通用指标和专用指标，其中，通用指标是按照等级保护 2.0 基本要求和测评要求梳理 [1-2]，专用指标是针对铁路典型重要系统如客票预订与发售系统、货运系统、运输调度管理系统从系统业务应用和日常运维人员关注安全方面梳理。主要指标层次结构，如 1 图所示。

2.2　通用指标

本文提出的通用指标主要的结构是系统安全等

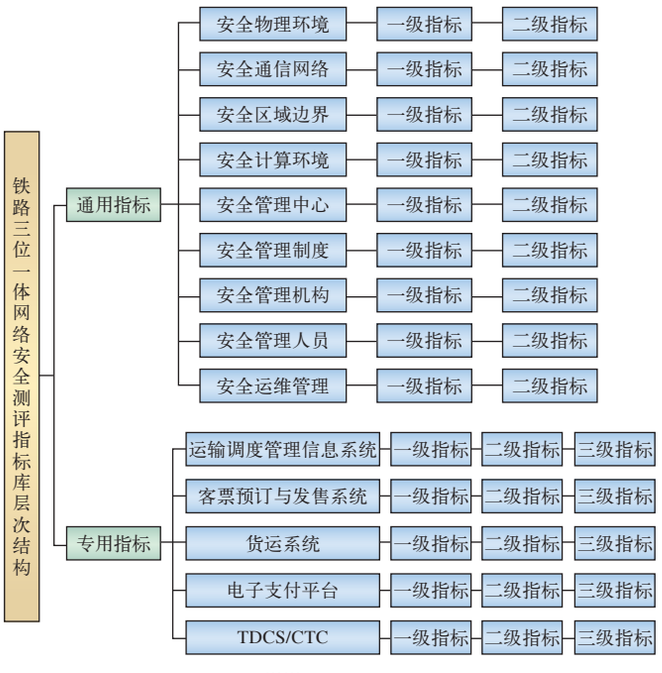

图1　铁路三位一体网络安全测评指标库层次结构

级、安全层面、类别、一级指标、二级指标、关联风险组成，主要是参考网络安全等级保护 2.0 基本要求、测评要求和风险评估规范等国家相关网络安全标准梳理的，其中，铁路系统主要安全级别包括一级系统、二级系统、三级系统和四级系统，安全层面包括技术层面和管理层面。类别又分为安全通用要求、云安全扩展要求、移动互联网安全扩展要求和物联网安全扩展要求。

2.2.1　技术类通用指标

技术类通用指标安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心 5 个技术层面，具体内容，如图 2 ～图 6 所示。

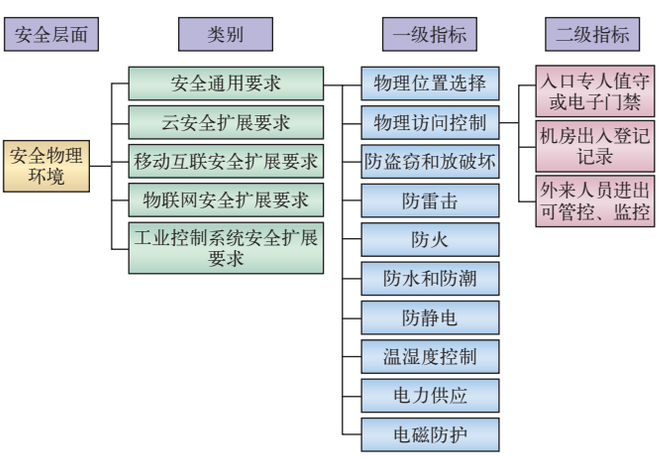

图2　铁路网络安全检测通用指标-安全物理环境

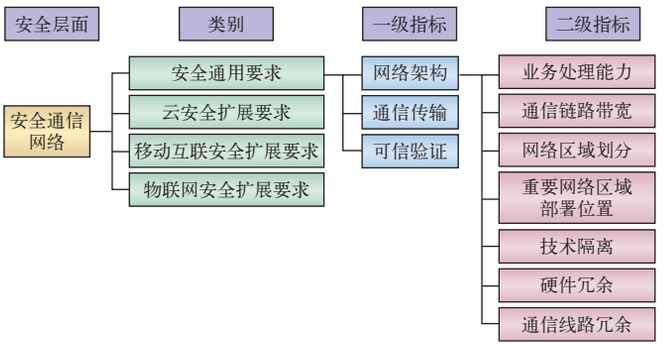

图3　铁路网络安全检测通用指标-安全通信网络

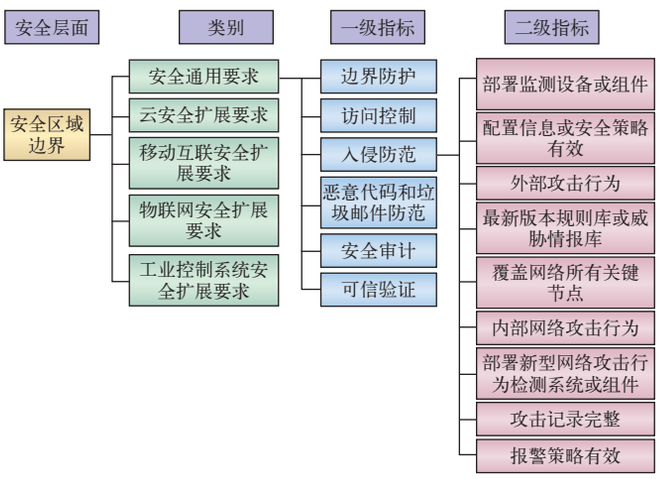

图4　铁路网络安全检测通用指标-安全区域边界

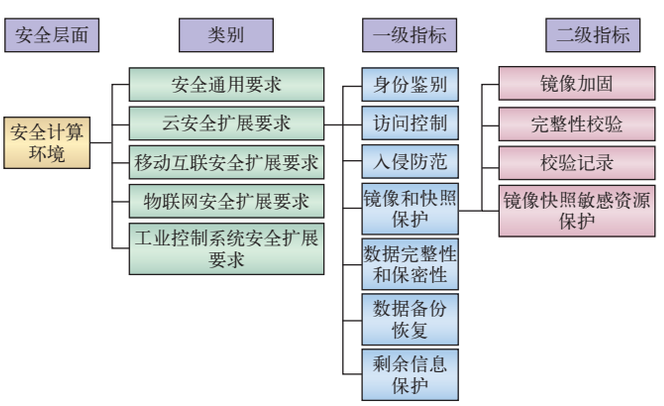

图5　铁路网络安全检测通用指标-安全计算环境

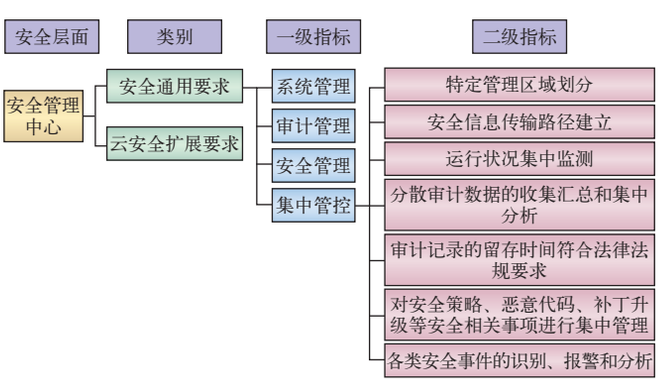

图6　铁路网络安全检测通用指标-安全管理中心

2.2.2　管理类通用指标

管理类通用指标包括安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理 5 个管理层面，具体内容，如图 7 ～图 11 所示。

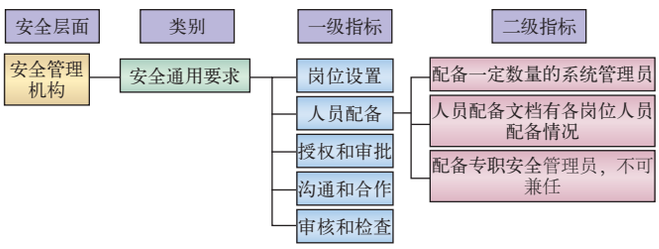

图7　铁路网络安全检测通用指标-安全管理机构

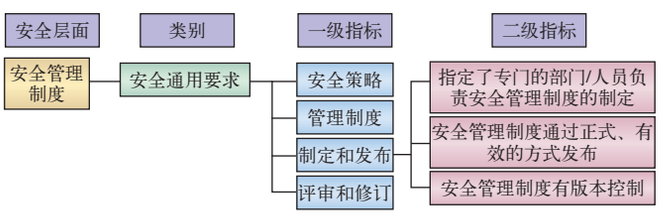

图8　铁路网络安全检测通用指标-安全管理制度

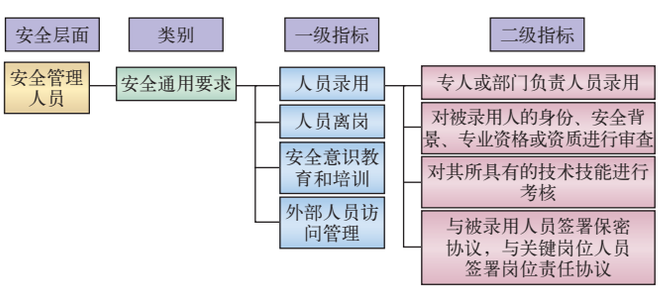

图9　铁路网络安全检测通用指标-安全管理人员

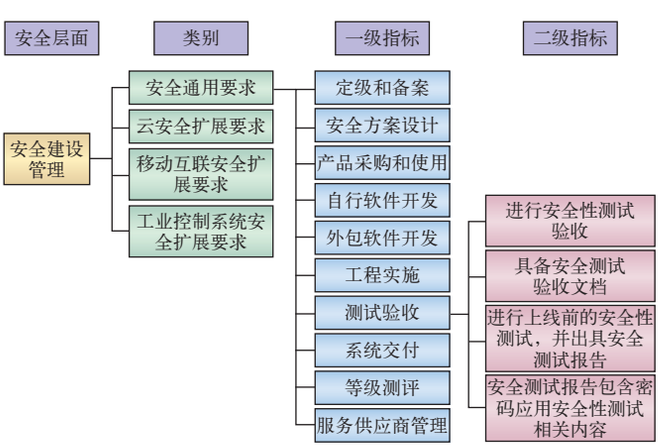

图10　铁路网络安全检测通用指标-安全建设管理

2.3　专用指标

2.3.1　专用指标概念提出

按照网络安全风险经典理论阐述，网络安全基本属性即 3 要素包括完整性、保密性和可用性，为适应业务需求的不断发展变化和网络技术的变迁，可靠性和不可抵赖性等网络安全要求越来越广泛。

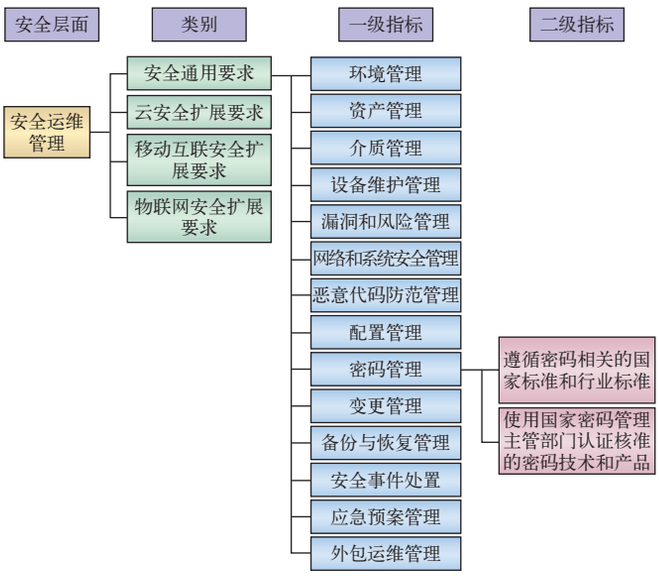

图11　铁路网络安全检测通用指标-安全运维管理

（1）完整性是防止信息未经授权被篡改的特性，重点要求保证信息在产生、存储和传输过程中的原样性。

（2）可用性是信息允许被授权实体访问和按需求使用的特性，是系统面向用户的安全要求，一般用系统正常使用时间和整个工作时间之比来度量。

（3）保密性是指防止重要数据信息非法泄露给非授权用户或供其使用的特性 [7]。

（4）可靠性是系统可以在规定条件下和规定的时间内完成规定的功能的特性，主要表现为抗毁性、生存性和有效性 3 方面。

（5）不可抵赖性，也可称为不可否认性，主要是确认信息交互参与者身份是否真实可信，所有参与方均不可否认或抵赖已经完成的操作和协议。采用数据源证据，为避免发信方否认已发送的消息；采用数据接收证据，为避免收信方否认已经接收的消息。

根据以往开展的安全测评实践经验，发现对于重要系统，单纯按通用安全指标开展测试，往往不能满足系统全面安全检测需要，会遗漏系统某些方面的重要业务安全内容，因此，对于铁路重要的系统而言，需要从业务角度出发，按照保密性、完整性、

可用性、可靠性、不可抵赖性等安全属性，进一步梳理安全测评指标，形成专用指标。

2.3.2 典型铁路系统专用指标研究

业务安全同业务本身具备的形态及其所提供的服务密不可分，业务安全最典型特征是个性化，因此，本文以铁路运输调度管理信息系统（TDMS）作为典型铁路系统，从计划、命令和调度 3 类典型业务研究，梳理出完整性、保密性、可用性 3 方面的专用指标，指标组成，如图 12 所示。

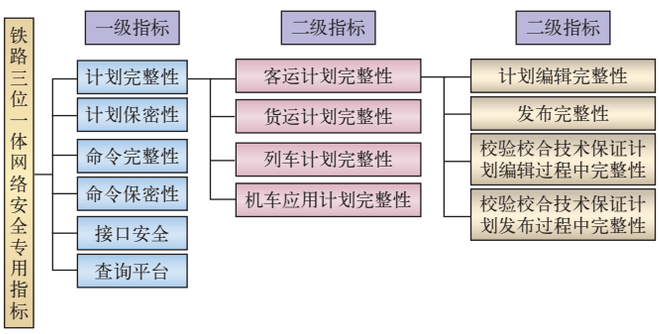

图12 铁路三位一体网络安全专用指标

3 测评指标库要求及应用

3.1 测评指标举例说明

为了更好地开展铁路三位一体网络安全测评工作，梳理出以上测评指标库，其中，通用指标库中的二级指标及专用指标库中的三级指标对于指导现场测试人员编制测评指导书和测评工作具有实际意义。以三级系统安全计算环境的云安全扩展要求为例，介绍测评指标库的要求及内容，并且分析出关联的安全风险，如表 1 所示。

表1 三级系统安全计算环境通用指标-云安全扩展指标访问控制内容

类别	测评项	一级指标	二级指标	关联安全风险
云计算安全扩展要求	应保证当虚拟机迁移时，访问控制策略随其迁移；（是否考虑不用标记）	访问控制	访问控制策略迁移	虚拟机迁移时访问控制策略未随之迁移
			迁移记录及配置	不具备虚拟机迁移记录及相关配置
	应允许云服务客户设置不同虚拟机之间的访问控制策略	访问控制	不同虚拟机间访问控制策略	云服务客户未设置不同虚拟机之间访问控制策略

3.2 测评应用案例

参照以上梳理的通用指标进行现场测试时，比如需对云安全扩展要求的一级指标“访问控制”开展现场测试和报告编写时，可针对访问控制的两个要求项，梳理出 3 个二级指标，其中，要求项 1 包括“访问控制策略迁移”“迁移记录及配置”2 个二级指标；要求项 2 包括“不同虚拟机间访问控制策略”1 个二级指标，可以清晰地了解和掌握基本要求项的关键测评关注点。以下分别从 3 类测评方法判定该“访问控制”项的结果。

（1）按照等级保护测评要求，现场测试中，若二级指标全部满足，则此测评项为符合 [8]，符合程度为 1 分；全部不满足，则此测评项为不符合，符合程度为 0 分；部分满足，则此测评项为部分符合，符合程度为 0.5 分。根据等级保护测评结论计算系统最终得分，判定系统安全状况和等级保护测评结论。

（2）按照风险评估测评要求，二级指标若为符合，则进一步从中识别出系统已有的安全措施；若为部分符合和不符合，则结合系统面临的安全风险项，分析得出系统存在的脆弱点，此脆弱点和等级保护测评中梳理的安全问题相关联，根据风险评估模型或各类算法，对脆弱性进行赋值，结合资产从完整性、保密性和可用性赋值，以及威胁发生的频率，计算系统安全风险值，确定系统总体安全状况 [9-10]。

（3）从国铁集团定期开展的安全检查，检查指标从本文中梳理的指标中进行抽选，结果判定为符合、部分符合和不符合 3 种情况，并结合工具测试和渗透测试的结果对系统进行整体评断。

4 结束语

铁路作为国家关键信息基础设施，其网络安全重要性不言而喻，通过安全方案设计、安全建设整改、安全等级保护测评、风险评估测评、安全检查和安全运维等各种手段保障系统安全稳定运行。为了保证 3 类测评方法可以更高效、更客观地反映系统安全状况，本文提出建立三位一体网络安全测评指标库，包括通用指标和专用指标，通用指标涵盖安全保护等级一级～四级的保护对象，保护对象包括信息系统、云计算平台、大数据、物联网、移动互联网、工业控制系统等铁路重要系统和应用，梳理出一级和二级指标。专用指标针对铁路典型重要系统的业务，从完整性、保密性及可用性梳理出一级指标、二级指标和三级指标。通过指标的梳理，

（下转 P47）

4　结束语

密码技术是网络安全的基石，是解决网络安全有效、可靠、经济的手段。铁路应加大对密码技术的研究，充分发挥密码在系统资源访问控制、数据存储、数据传输、可视化控制、安全审计等方面的支撑作用。加快密码技术与多种技术的融合，构建铁路行业的密码技术体系、管理体系、安全体系，提升铁路整体安全防护能力，推动商用密码技术的快速发展。

参考文献

[1]《商用密码知识与政策干部读本》编委会 . 商用密码知识与政策干部读本 [M]. 北京：人民出版社，2017.

[2] 沈海燕，端嘉盈，王　浩，等 . 云物大智、区块链、CPS 间的关系及在铁路领域研究综述 [J]. 铁路计算机应用，2019，28（2）：1-6.

[3] 王莉菲，兰　天 . 工业控制系统的信息安全与密码应用 [J]. 集成电路应用，2020，37（2）：15-17.

[4] 高志权 . 云密码服务关键技术研究 [J]. 数字技术与应用，2019，37（9）：181-183.

[5] 马小宁，李　平，史天运 . 铁路大数据应用体系架构研究 [J]. 铁路计算机应用，2016，25（9）：7-13.

[6] 徐汉良 . 推动密码与大数据的融合发展 [J]. 中国信息安全，2018（8）：48-50.

[7] 杨国强，丁杭超，邹　静，等 . 基于高性能密码实现的大数据安全方案 [J]. 计算机研究与发展，2019，56（10）：2207-2215.

[8] 武传坤 . 中国的物联网安全：技术发展与政策建议 [J]. 人民论坛 · 学术前沿，2016（17）：47-58.

[9] 郭茂文 . 物联网身份认证解决方案探讨 [J]. 广东通信技术，2019，39（2）：24-28.

[10] 李兆森，杨　洋 . 基于国产密码算法的物联网应用研究 [J]. 信息安全研究，2019，5（10）：924-928.

责任编辑　徐侃春

（上接 P42）

更好地开展现场测评工作，本文梳理的专用指标仅以运输调度管理信息系统为例，还不具备广泛性，需进一步梳理出其他系统的专用指标，并梳理三位一体测评实施流程，提出铁路三位一体网络安全测评实施指南建议。

参考文献

[1] 全国人民代表大会常务委员会 . 中华人民共和国网络安全法 [M]. 北京：全国人民代表大会常务委员会，2017，6.

[2] 李智勇，徐太忠，孙峰岭，等 .“三位一体”的信息安全检测 [J]. 计算机世界，2013（1）：2-7.

[3] 全国信息安全标准化技术委员会 . 信息安全技术网络安全等级保护基本要求：GB/T 22239-2019[S]. 北京：中国标准出版社，2019，6.

[4] 全国信息安全标准化技术委员会 . 信息安全技术网络安全等级保护测评要求：GB/T 28448 -2019[S]. 北京：中国标准出版社，2019，6.

[5] 全国信息安全标准化技术委员会 . 信息安全技术网络安全等级保护测评过程指南：GB/T 28449-2018[S]. 北京：中国标准出版社，2019，6.

[6] 全国信息安全标准化技术委员会 . 信息安全技术信息安全风险评估规范：GB/T 2098-2007[S]. 北京：中国标准出版社，2007.

[7] 李宏亮 . 计算机网络威胁与安全策略浅析 [J]. 数字化用户，2018（26）：1.

[8] 姚洪磊，杨　文 . 三级系统信息安全等级保护测评指标体系研究 [J]. 铁路计算机应用，2015，24（2）：59-61.

[9] 张　彦 . 铁路信息系统安全体系研究 [J]. 铁路计算机应用，2015，24（2）：5-7.

[10] 贾　炜 . 计算机网络脆弱性评估方法研究 [D]. 合肥：中国科学技术大学，2012.

责任编辑　徐侃春