第 39 卷　第 3 期(671~679)　　中 国 地 震　　Vol. 39　No. 3
2023 年 9 月　　EARTHQUAKE RESEARCH IN CHINA　　Sep. 2023

刘晓雨,黄志斌,周克昌,等. 2023. 地震行业网络安全等级保护建设思路与部署应用. 中国地震,**39**(3):671~679.

地震行业网络安全等级保护建设思路与部署应用

刘晓雨　黄志斌　周克昌　吴天安　谭颖　张维佳

中国地震台网中心,北京　100045

摘要　简要介绍地震部门为积极落实国家网络安全要求,依据“网络安全法”“网络安全等级制度”等相关要求,结合地震行业自身业务特点与安全需求开展地震行业网络安全等级保护工作的规划、设计与部署应用;着重分析地震行业面临的主要安全问题与系统性风险、现阶段行业网络安全的总体规划与“合规性”的建设思路;分析并解决等级保护规划设计中的业务难点、技术难点与实施难点。

关键词:　网络安全　等级保护　合规建设

[文章编号] 1001-4683(2023)03-0671-09　[中图分类号] P315　[文献标识码] A

0　引言

近年来,随着移动互联、云计算、大数据等信息技术的高速发展与广泛应用,信息化已然成为社会经济发展和人民日常工作生活的重要组成部分,同时网络安全也面临着复杂形势与巨大风险的重大挑战。2017 年 6 月 1 日《中华人民共和国网络安全法》正式颁布实施,这是我国第一部有关网络安全方面的法律,首次将网络安全提升到法律高度,其定义了九类网络安全保护制度,其中第二十一条明确规定,实行网络安全等级保护制度是我国的一项基本国策。2019 年 12 月 1 日,网络安全等级保护制度 2.0 标准正式实施,相较之前标准,2.0 标准实现了对涉及新技术、新应用防护对象和安全保护领域的全覆盖,突出技术措施与整体策略,注重全方位主动防御、动态防御、统一防护和精准防护思路,强化“一个中心,三重防护”的安全防护体系,将云计算、物联网、移动互联、工业控制系统、大数据等相关新技术、新应用全部纳入保护范畴(国家市场监督管理总局等,2019),具有良好的防护效果、广泛的技术适用性、完备的测试评价体系、可行的行业推广应用,已经成为国家网络安全的基本制度。

早在“十五”期间,中国地震局已通过重大工程项目实施建设进入了“网络到台站,IP 到仪器”的网络化时代,在后续多年的持续建设与优化升级中,伴随着虚拟化、大数据、云计算等新技术的广泛使用,随之而来的网络安全问题频发,安全风险加剧,严重威胁到地震部

[收稿日期] 2023-07-26　[修定日期] 2023-08-17

[项目类别] 中国地震局网络安全等级保护建设重点工作任务资助

[作者简介] 刘晓雨,男,1981 年生,高级工程师,主要从事地震应急、信息、网络安全方面研究。E-mail:rain_leo@seis.ac.cn

门各类业务应用的稳定运行、日常政务办公的顺利开展和关键数据信息的安全有效。依据国家网络安全相关法律法规与制度要求,地震部门全面开展网络安全建设工作,并确定了“围绕合规性开展等级保护工作,作为现阶段网络安全工作重点”的业务思路。为此,本文梳理了地震行业面临的主要安全问题与系统性风险,依据“网络安全法”“网络安全等级制度”等相关要求,并结合地震行业自身业务特点与安全需求,对开展地震行业网络安全等级保护工作的规划、设计、部署应用进行总结,分析并解决等级保护规划设计中的业务难点、技术难点与实施难点。

1 地震行业面临的主要安全问题与系统性风险

2017 年《中华人民共和国网络安全法》颁布后,地震部门积极落实国家法律法规要求,全面推进网络安全建设工作,依托国家“十五”项目建成了覆盖全国的地震行业骨干网络系统,并依托该技术系统实现了全国数据信息的高速传输、业务应用的升级换代。由于地震部门业务信息化工作起步较早,国家在网络安全方面的诸多法律法规与制度规范在当时尚未出台,造成前期各类工程项目中,网络安全建设未进行规范化设计和有效性实施,防护能力与防护水平较国家最新等级保护 2.0 标准要求存在较大差距,难以通过国家等级保护测评,无法实现地震部门网络安全的合规运转,存在较高法律风险与责任风险。

1.1 主要安全问题

1.1.1 与国家网络安全合规要求存较大差距

(1)基础防护措施不达标。地震系统局属各单位具备一定的网络安全防护能力,按照《中华人民共和国网络安全法》和网络安全等级保护制度 2.0 标准要求,地震系统当时只有少数单位按照“分区分域”的安全防护理念进行边界防护,仅有个别单位采取行业网、互联网有效隔离防护措施,加之绝大多数单位互联网出口管理不严格,导致网络安全风险激增,存在较大安全隐患。

(2)未建设安全管理中心。国家网络安全最新要求是:一个中心,三重防护,即安全管理中心、安全通信网络、安全区域边界、安全计算环境(郭启全,2022)。地震行业在安全管理体系、安全技术体系、安全运维体系和安全服务体系等方面缺乏统一的通信网络安全与运维管理系统,不能做到统一监控全局整体网络安全设备状况,无法保证全行业内各个设备策略防护措施有效、从各单位网络安全设备获取到的情报完整以及网络安全应急指挥及时可靠的需求。

(3)信息系统基本未通过等保测评。由于现有业务系统在建设初期缺乏有效的网络安全建设,对标国家等保 2.0 标准要求,部分单位仍然缺少应有的基本防护措施,部分防护手段也存在设备运行时间过久(2016 年前后部署),加之设备超期服役,设备老化现象较为严重,运行稳定性无法得到保障;对于防护系统、识别库、病毒库等关键技术环节,设备厂家不能提供及时有效的技术支持与更新服务,在防护能力上大打折扣;设备性能无法满足业务量的持续增加,设备功能无法满足业务类型、种类的多样化发展,综合防护指标不符合等保 2.0 标准的最新要求,更不能满足地震部门业务持续发展的需要。

1.1.2 网络安全事件频发

(1)发生多次重大网络安全事件。2016 年以来,地震行业网遭遇两次大范围服务器安全事件,其中 2016 年 1 月木马病毒事件中,有数百台(套)服务器被入侵;2017 年 11 月行业

网内有数百台主机感染勒索病毒变种版本。

（2）攻防演习中暴露诸多问题。自 2019 年开始，地震部门连续参加全国网络安全攻防实战演习，在演习过程中有近一半单位的数十个网络及信息系统存在易被网络攻击的漏洞，其中包括多个核心业务系统。

1.2　主要系统风险

（1）门户网站存在安全隐患。门户网站是单位职能部门信息化建设的重要内容，同时也是对外宣传单位形象、发布行业信息、开展电子政务的主要平台。常见的网络安全隐患包括数据泄露、数据信息恶意篡改、拒绝服务等攻击方式，尤其针对地震信息，一旦被篡改，会造成巨大的政治风险、名誉损失和公信力下降，政府网站安全形势日益严峻。

（2）核心业务存在安全风险。现阶段，中国地震局各类重要业务系统存在安全漏洞、系统脆弱、无运行状态的监控和安全防护设备老旧等问题。加之现有防护设备数量和防护能力严重不足，虽完成了行业网间的边界隔离，但未对二级网络节点线路、外联线路以及内部网络接入区采取相应的边界防护手段，纵深区域边界安全无法得到保障。若外围系统受到攻击，可能会造成地震速报等核心业务系统遭到木马、勒索等病毒的严重损害，地震速报信息若被篡改并发布，将造成严重的社会不良影响。

2　现阶段网络安全“合规性”建设思路与行业总体规划

2.1　网络安全“合规性”建设思路的确定

在国家网络安全法颁布实施后，地震部门也加快了行业网络安全建设。通过多方调研与分析论证，在“绝对安全”与“合规安全”两种方式上，最终确定围绕“合规性”开展等级保护，作为现阶段地震行业网络安全建设的总体思路。

网络安全的实质是对抗，是人与人、攻击方与防守方、红队和蓝队间的较量，与网络通信互联、数据存储应用、业务软件开发使用、技术系统故障处置有本质的区别，网络安全是随着参与各方人的思维体现的，而其他信息系统是按照设定参数、预定代码、设计指令执行的。了解网络安全的本质则不难发现，网络安全不是一成不变的，而是动态的、变化的。一个新建成的系统配套合理的防护措施，在一定时间段内可能是安全的，但随着时间的推移，系统中的漏洞被发现、被利用，系统就不再安全，需要进行相应的补救措施，进而从不安全再到安全（图 1）。因此，就现阶段而言，“绝对安全”技术难度大、投入高，且很难实现。“合规安全”围绕国家相关制度要求和等级保护制度标准开展，具有设计科学性、内容合理性、技术有效性、投资经济性、实施可操作性以及评估量化性等特点，符合现阶段地震行业开展网络安全的业务需求与管理要求。

2.2　行业网络安全总体规划设计

依照网络安全“合规性”建设思路，全面完成地震行业各单位的网络安全等级保护建设是基本要求，更是底线要求，是全面推进地震部门网络安全工作的首要任务。同时，按照国家网络安全“三化六防”的最新理念，在安全合规的基础上，整合推进技术防护体系与运行监管体系的统一平台化融合。通过建设网络安全运行管理平台，实现网络安全从被动向主动、从静态到动态、从单点到整体、从粗放到精准防御的转变，形成国家、省二级网络安全运行管理体系，进而实现对地震行业网络系统安全威胁的提前感知与预测预防。通过对正在发生

图 1 网络安全本质属性

的安全事件进行实时防御和响应处置，对潜在的安全威胁进行持续监测，以及对已发生安全事件的分析溯源（陶源等，2020），并通过信息通报平台上传、下达各类预警信息，确保各类异常事件及时、有效、有序处理，在满足合规运行的基础上，逐步实现能力提升和安全运营，进一步推动地震网络安全发展的现代化进程（图 2）。

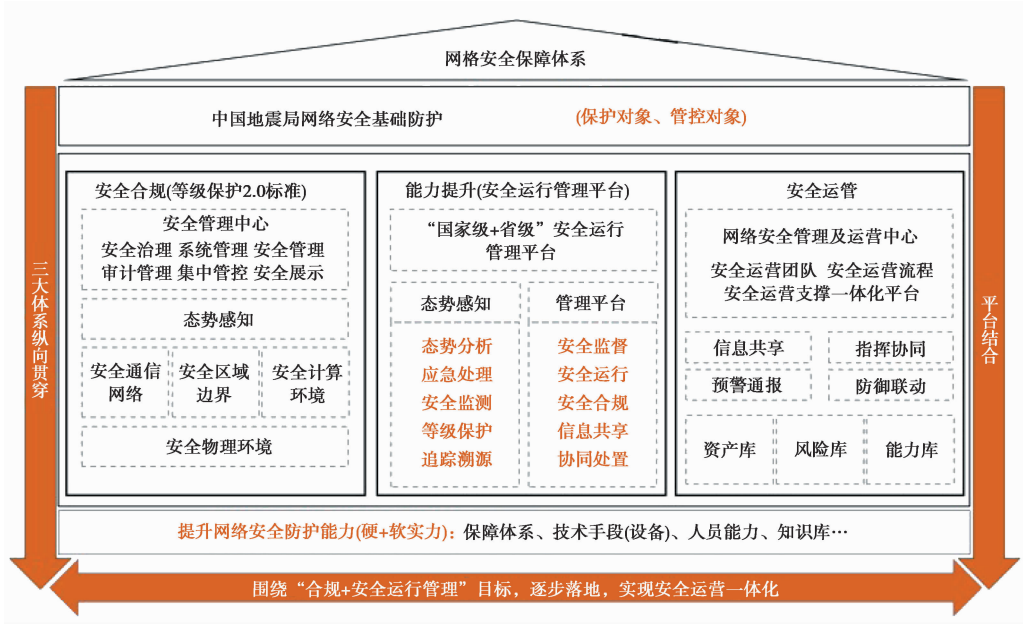

图 2 地震行业网络安全保障体系

3 行业等级保护规划设计

针对信息系统等保建设，网络安全等级保护制度 2.0 标准设计五个环节，包括系统定级、系统备案、实施建设、测评整改、监督检查。其中前四个环节需要系统建设管理单位负责完成，测评由专业机构负责；系统监督检查则由公安部门根据网络安全法的要求开展。

在行业等级保护规划设计过程中，如何合理规划定级（保业务）、如何开展实施建设（保安全）、如何通过等保测评（保合规）是设计难点和重点，实施成本及后续运营成本控制更是关键点（可行性与持续性）。

3.1　系统定级规划设计

3.1.1　存在问题

地震部门于 2007—2008 年按照国家要求开展了首次信息系统定级备案工作，但当时针对等级保护政策要求的学习和认识普遍不足，对自身系统安全需求分析不充分，未按照科学合理的要求开展定级备案工作。对标等级保护制度 2.0 标准，地震行业各单位普遍存在定级系统数量过多、定级对象过于分散、定级标准不统一、定级等级虚高、未能全覆盖等问题。据统计，地震行业各单位定级备案系统近 300 个，其中三级及以上系统超过 100 个，甚至还有四级系统（国内四级系统主要涉及类似阿里云、腾讯云等全国性大型互联网运营服务系统），未定级系统数量百余个。上述问题造成等级保护建设实施的两大问题难点，致使行业内等保建设工作无法直接开展。

问题难点一是系统定级备案数量过多。等级保护建设需要通过等保测评实现安全合规的基本要求（李超，2013），系统测试工作由第三方机构有偿提供，其收费标准为三级系统每个 8~12 万元，二级系统每个 5~8 万元。系统定级备案数量过多，势必造成测评费用过高，且等保三级及以上系统国家强制每年测评一次，后续运行成本巨大，现有财政预算很难支撑，等级保护建设缺乏可行性与连续性。

问题难点二是系统定级等级普遍过高。按照等级保护制度要求，系统等级越高，防护要求越高；等保测评项越多，实现合规建设越难。在前期等级备案中，由于系统定级随意，致使许多未达到等保三级防护要求的系统定级备案为三级，对照等保相关要求，单位自身的防护能力、安全运行管理能力差距较大，故很难通过等保测评。如果按照虚高等级开展建设，必然造成过度防护、经费预算浪费、后续运行管理成本过高等问题。

3.1.2　问题难点分析

通过调研分析，造成各单位系统定级数量过多、定级级别过高的主要原因有以下两点：

（1）对等级保护制度要求理解认知不足。等级保护制度是国家关于网络安全合规建设体系化、标准化、科学化的权威标准，由于对该项制度的学习和认识不足，在初期开展的定级备案工作中，地震行业各单位普遍认为定级系统越多越好，其能突出本单位业务多、任务重的特点；此外，认为定级等级越高越好，定级高能突出业务的重要性，且等级越高，系统越安全，后期国家投入更高，因此造成初次定级系统等级虚高，后续等保建设整改、测评等工作难以开展。

（2）没有行业统一的规划设计。地震部门的业务具有全国一致性、关联性的特点，由于没有针对行业开展统一的等级保护规划设计，各单位各自为战，无法形成科学合理、行业一致的系统定级策略和方案。例如，同样一个业务系统，在有的单位定为三级系统，有的单位定为二级系统，有的单位则不定级。又如统一业务系统，在不同单位不但定级等级不一致，甚至系统名称也不一致，造成内部网络安全统一管理困难，外部则无法形成具有业务一致性的地震行业网络安全等级保护策略。

3.1.3　技术思路

为解决定级备案中“系统多”“定级高”的问题，需要对等级保护制度、技术要求和测评要求进行深入学习和研究。在地震行业全面开展等级保护建设，则需要结合业务特点，深入分析各类业务的关联度、业务运行服务要求以及基础支撑环境等关键因素，制定全国统一的

地震行业网络安全等级保护定级业务标准,技术思路有以下几个方面。

首先是优化整合,科学减少系统数量。其中思路一是从自身业务角度分析考虑。按照等级保护相关技术要求,可以将业务模式、功能、流程类似以及基础运行环境相同的多个系统整合成一个等保信息系统,进行打包整合定级,这样可以大幅减少系统定级数量,同时又符合网络安全等级保护技术要求。思路二是从网络安全角度分析考虑。在等级保护制度中存在等保一级系统,该系统安全级别最低,由系统建设运行单位自行管理,无需到公安机关备案,不强制要求开展等保测评,在地震行业各单位如果有安全需求与等保一级系统相符的系统,可以按照等保一级定级管理,以减少备案、测评环节,等同于减少等级系统数量。

其次是分类分级,合理规划系统等级。在网络安全等级保护制度中,判断系统等级高低的重要业务指标有两项:信息安全保护等级(既系统中数据信息的安全性要求)和系统服务安全保护等级(既系统连续运行的安全性要求)。要降低系统等级,同样有两个技术思路。思路一是对业务应用进行合理分类。地震部门的业务划分包括地震监测、预报、应急以及电子政务、公共服务等,依据信息安全保护等级和系统服务安全保护等级两项指标,对比上述业务应用发现目前决定地震部门业务应用定级等级高低的主要因素为“系统服务安全保护等级”指标,越是核心业务系统,对系统的连续运行率要求越高,其系统等级越高。例如,在业务实践中地震速报预警等测震业务对系统连续率要求最高,其在网络安全等级保护中的定级等级相对要高。思路二是对业务应用进行合理分级。地震部门业务应用多为自下而上的星型结构,即地震台站采集数据信息,各省局单位汇集省内的各台站数据信息,开展省级业务应用,国家中心汇集全国各省数据信息,开展国家级业务应用。从重要程度来看,在全国层面,单一台站故障不会造成全省或全国性业务影响,其业务影响是单点的;单一省局故障也不会造成全国性业务影响,其业务影响是局部的;而国家级业务系统作为业务中枢,其业务安全性在行业内是最高。综上,在业务安全等级方面,台站业务系统安全等级<省级业务系统安全等级<国家业务系统安全等级。

3.1.4 地震行业信息系统等级保护定级规划

依据国家等级保护制度要求,结合地震部门现有业务应用,按照优化整合、分类分级的业务思路设计了覆盖地震行业国家级、省级两级架构的地震行业信息系统等级保护定级规划,如表 1、表 2 所示。

3.2 安全防护与等保测评

统一规划行业系统定级后,安全防护与等保测评是完成等级保护工作的重点。在该部分设计规划中,结合地震部门网络安全实际情况,同样需要解决诸多问题难点。对标等级保护相关技术防护与测评要求,地震部门现有网络安全防护主要的问题难点是网络安全防护能力薄弱、与等保要求差距较大;地震行业各单位信息系统存量规模较大,同时网络安全经费投入有限,短时间内很难实现全方位网络安全建设。

综合上述情况,通过分析研究,从以下两个方面技术手段提升现有系统网络发安全防护能力。

一是充分发挥已有系统的安全防护能力。针对已有的网络设备、安全防护设备以及服务器主机操作系统、数据库、中间件等应用软件,充分发挥其安全功能和安全特性,依据“安全基线”的技术要求(郭鑫,2020),深入挖掘各类产品、设备、软件、应用的安全防护能力,包括路由

表 1　　国家级信息系统规划

业务分类	业务系统	业务描述	数据安全性等级	业务连续性等级	安全防护等级
国家级基础设施类	中国地震行业云平台	由位于北京的中国地震台网中心、位于西安的中国地震局第二测中心、位于广州的广东省地震局三家单位构成的地震行业云平台，可为全国地震行业相关业务应用提供基础云平台支撑服务	第三级	第三级	第三级
公共信息服务类	门户网站	中国地震局门户网站	第三级	第二级	第三级
	地震信息网	中国地震局对外科技门户网站	第三级	第二级	第三级
	公共信息服务平台	包括地震微信、微博、APP 客户端、12322 等由国家级业务单位运行，面向全国的新媒体服务系统	第三级	第三级	第三级
政事办公类	OA 系统	地震部门内部政务办公自动化系统	第二级	第二级	第二级
	邮件系统	中国地震局统一邮件系统，服务全国地震行业各单位，包括政事邮件服务与业务邮件服务两部分	第二级	第二级	第二级
	发展与财务管理信息系统	地震部门全国统一财务信息系统	第二级	第二级	第二级
	其他政事办公系统	地震部门人事、科技管理等其他政事办公系统	第二级	第二级	第二级
业务系统类	国家测震台网业务系统	由地震实时波形传输系统、地震速报信息交换系统以及地震行业骨干网组成；用于地震数据传输、共享与交换	第二级	第三级	第三级
	国家地震烈度速报与预警业务系统	地震烈度速报与预警信息系统国家中心，包括数据处理、应急信息发布、通信网络中心三部分	第三级	第三级	第三级
	国家地震应急业务系统	主要包括应急触发系统、应急地震预评估系统、应急产出系统、应急基础数据库管理系统、应急视频会议系统，为政府救灾决策提供灾害快速评估结果和协助决策建议	第三级	第二级	第三级
	国家地球物理台网业务系统	汇集、管理全国地震定点观测台站的各类地球物理数据及信息，为地震预报业务提供数据保障	第二级	第二级	第二级
	中国大陆构造环境监测网络业务系统	中国地震局及五部委联合建设运行的内部系统，汇集中国大陆构造环境监测网络台站的观测数据，并进行数据处理、存储、分发、分析和产品产出	第二级	第二级	第二级
	国家地震科学数据中心共享服务平台	为行业用户提供地震科学数据共享服务的信息系统	第二级	第二级	第二级
	国家强震动台网数据管理系统	提供强震动观测、数据分析等信息服务功能，实现全国强震动观测数据的处理、管理和发布的信息系统	第二级	第二级	第二级
	国家地震分析预报信息系统	为地震预报业务人员提供数据共享、交换服务	第二级	第二级	第二级
	国家活断层信息系统	提供国家活断层信息数据服务	第一级	第二级	第二级

表 2　　省级信息系统规划

业务分类	业务系统	业务描述	数据安全性等级	业务连续性等级	安全防护等级
公共信息服务类	门户网站	局属单位门户网站	第二级或第三级	第二级或第三级	第二级或第三级
	公共信息服务平台	局属单位地震微信、微博、APP 客户端、12322 等新媒体服务系统	第二级	第二级	第二级
政事办公类	政事办公系统	局属单位 OA、人事、科技管理、财务等政事办公系统	第一级或第二级	第一级或第二级	第一级或第二级
业务系统类	地震综合业务系统	包括省级地震监测、地震应急、分析预报等业务系统	第二级或第三级	第二级或第三级	第二级或第三级
	地震烈度速报与预警系统	省级地震烈度速报与预警系统，主要包括通信网络系统、数据处理系统、紧急地震信息发布服务系统	第三级	第三级	第三级

器、交换机等网络设备的终端主机准入功能、访问控制功能等，操作系统的用户强认证功能、账号密码强口令功能，系统防火墙、主机安全软件、数据库软件的安全访问控制、安全审计功能，应用系统的访问控制、权限细化设计、安全代码检测完善，优化防火墙访问控制策略，细化访问控制列表，可着重解决“账号弱口令、服务器漏洞、网络边界防护”等高危问题，大幅提升已有业务系统在基础网络环境、网络安全边界、应用防护、业务审计等方面的安全性。

二是统筹复用网络安全防护系统，发挥网络安全系统“同网共享”技术策略。在同一网络系统和网络环境中，网络安全设备可实现共同使用，共同复用。在网络安全经费预算有限的情况下，多个同网运行的业务系统安全经费可统筹使用，每个系统分别保障部分必要的安全手段，多个系统的多种安全手段组合后，可形成一套满足等保防护要求的安全防护体系，每个业务系统均符合网络安全防护要求，解决经费不足的问题（图 3）。

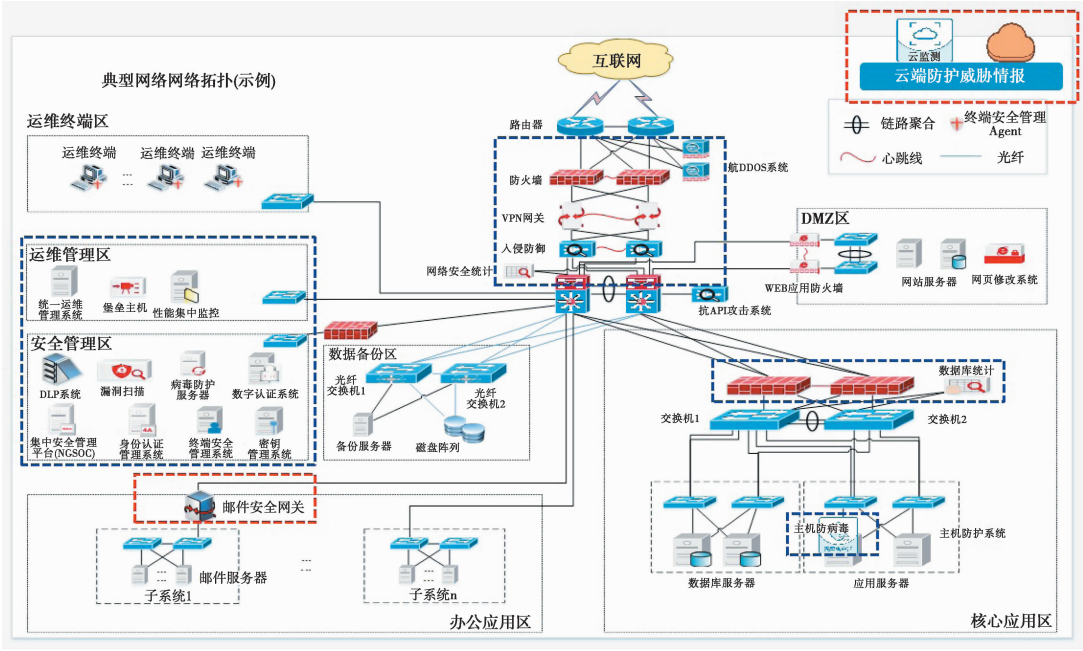

图 3 典型网络系统安全区域设计与防护措施配置

4 部署应用及成效

通过等级保护规划设计，解决了地震行业前期“系统定级数量多、定级等级高”的核心问题。经过技术策略的优化调整，在现有网络安全防护基础上，依托有限经费，基本可实现行业各单位的网络安全等级保护要求达标。在此基础上，中国地震局为加快推进行业各单位等级保护建设工作，依托地震行业等级保护规划设计编制形成《地震部门网络安全等级保护定级工作指南》，同时为保障行业各单位等保定级备案工作顺利开展，经过与国家网络安全主管部门公安部商榷，《地震部门网络安全等级保护定级工作指南》于 2018 年 12 月由中国地震局、公安部同步印发，为后续各单位在当地公安部门系统备案起到了关键作用。

2019—2022 年的 4 年中，地震行业各单位积极开展等级保护建设工作，在“定级指南”的引导下，依托各类项目完成地震行业网络安全等级保护建设。在信息系统数量方面，全国

信息系统总数降低约 40%；在信息系统等级方面，三级系统数量降低 82%，无四级及以上系统；在等保覆盖范围上，行业内无未定级系统，实现了“系统整合降数量，系统优化降等级”的设计规划目标，各单位均完成系统等保建设并通过测评，实现了地震部门网络安全合规的既定目标；在经济效益方面，通过防护系统的统筹复用，充分利用各项目的安全投资经费，合理规划了系统数量和等级，尤其是大幅度减少等保三级系统数量后，首次测评费用节省超过 30%，后续每年等保测评费节省近 90%，保证了有限经费的利用率和长期等保工作的连续性与可实施性，实现了地震系统网络安全阶段性既定目标。

5　结语

等级保护工作在地震行业的全面实现标志着地震部门网络安全工作取得了关键进展，实现了网络安全合规。同时，在当下网络安全态势日趋严峻的背景下，地震部门网络安全工作在合规之后需要继续依照国家相关要求并结合行业应用特点，在数据安全、关键信息基础设施防护方面持续开展业务实践，针对核心业务、关键领域进行重点防护和精准防护，将静态防护措施逐步提升到主动探测、快速发现、准确定位、处置有效的主动防御体系，切实持续提升地震行业网络安全整体防护能力和应急处置能力，为地震部门高质量发展保驾护航。

参考文献

国家市场监督管理总局，国家标准化管理委员会. 2019. GB/T 22239-2019 信息安全技术　网络安全等级保护基本要求. 北京：中国标准出版社.

郭启全. 2022. 网络安全等级保护基本要求（通用要求部分）应用指南. 北京：电子工业出版社.

郭鑫. 2020. 信息安全等级保护测评与整改指导手册. 北京：机械工业出版社.

李超. 2013. 信息系统安全等级保护实务. 北京：科学出版社.

陶源，李末岩，郭俸明. 2020. 超大型互联网平台网络安全等级保护技术原理及应用实践. 北京：电子工业出版社.

Construction and Implementation of Network Security Level Protection in the Earthquake Industry

Liu Xiaoyu, Huang Zhibin, Zhou Kechang, Wu Tianan, Tan Ying, Zhang Weijia
China Earthquake Networks Center, Beijing 100045, China

Abstract　In this paper we first briefly introduced the earthquake departments actively implementing the national network security requirements, with accordance to the relevant requirements such as network security law and network security hierarchy, and combination of the characteristics and security requirements of the earthquake industry, in order to carry out the planning, design and deployment of network security level protection in the earthquake industry. Then we analyzed the main security problems and systemic risks faced by the earthquake industry, the general planning of network security and the construction idea of compliance in order to solve the operational technical and implementation problems in the planning and design of level protection.

Keywords: **Network security**; **Classified protection**; **Compliance construction**