省级地震应急指挥中心信息安全体系建设初探*

李 敏，李永强，曹彦波

（云南省地震局，云南 昆明 650224）

摘要：通过对应急指挥信息系统规划、建设、管理、运行中可能存在的信息安全隐患进行分析，结合目前主流信息安全技术，从系统设计、硬件造型、抗侵害的容灾备份、虚拟技术应用等方面综合提出针对省级地震应急技术系统的信息安全体系建设的参考建议和新观点。

关键词：地震应急；技术系统；信息安全

中图分类号：P315－392 **文献标识码**：A **文章编号**：1000－0666(2013)03－0395－06

0 前言

近年来，随着地震应急指挥体系开放性、共享性、互联程度的不断扩大，地震应急信息安全保障问题逐渐成为各级地震应急技术平台体系应用、运维的核心业务工作。

“十五”项目建设以来，我国在地震应急指挥决策领域开展了较多的研究工作，包括地震应急指挥模式、应急指挥技术体系、地震应急管理、地震快速评估等（姜立新等，2003a，b）。在“中国数字地震观测网络工程”的推动下，建成了覆盖国家、区域、重点城市、灾害现场的4级应急指挥技术系统，促使应急指挥模式发生了较大变化，应急响应从传统分散型的应急模式转化为集现代计算机、网络通讯、灾害评估和指挥决策等技术为一体的综合性应急体系工作，实现了地震震情、灾情的应急指挥决策快速响应，灾害损失的快速评估与动态跟踪、辅助决策的信息服务和可视化指挥等系统工程。系统建成以来，为地震应急指挥提供丰富的理论基础和实践经验，大大提高我国的地震应急响应能力。在提高破坏性地震的快速响应、应急产出服务能力方面发挥了积极的作用（帅向华等，2009）。

随着地震应急指挥体系开放性、共享性、互联程度的不断扩大（林山，刘凤仙，2011），地震应急信息安全保障问题逐渐成为各级地震应急技术平台体系应用、运维的核心业务工作。对于国内大多数同类地震应急信息系统来说，如何在充分利用信息化优势的同时，更好地保护自身信息资源，防御外来恶意攻击和内部资源窃取，已经成为一个严峻的挑战，甚至成为制约各级地震应急管理部门应急指挥信息化进程的一个难题。

2009年，根据中华人民共和国公安部《信息安全等级保护管理办法》文件的评定，省级地震应急指挥中心信息系统为信息安全保护三级系统，发生安全责任事故将对国家安全、社会秩序和公共利益造成严重损害（中华人民共和国公安部，2007）。

本文通过针对应急指挥信息系统规划、建设、管理、运行中可能存在的信息安全隐患进行分析，结合目前主流信息安全技术，综合性提出针对省级地震应急技术系统的信息安全体系建设的参考建议和新观点。

1 应急指挥信息系统安全隐患分析

国际标准化组织（ISO）定义信息安全为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原

* **收稿日期**：2012－12－10.

基金项目：公益性行业科研专项——西南地震应急对策新模式与关键技术研究（201108013）和云南省地震局科研类青年基金《州市地震应急指挥系统建设技术指南调研》共同资助.

因而遭到破坏、更改和显露”。主要表现在信息的保密性、完整性、可用性、可控性和不可否认性等方面（周璐，2005）。地震应急指挥信息系统作为一个信息化体系，它在继承了通用信息系统对入侵防护、数据加密和容灾备份等信息安全要素的需求的同时，又对系统稳定性和实时响应效率有着特殊的要求。笔者通过对标准化信息安全体系的研究，结合现有运行管理经验，认为应急指挥信息安全的主要隐患包含以下主要因素：

（1）强制物理连接。指对隔离的地震应急基础数据库运转平台进行强制物理连接，连接对象可以是集群平台网络设备，服务器，终端等，连接方式可以是通过光纤收发器、STP/UTP 双绞线、移动存储介质等。此类信息安全隐患主要是由于缺乏完善的应急指挥中心管理机制，特别是中心机房及信号控制室运维管理制度。

（2）非法授权访问。指对地震应急指挥技术平台网络设备及信息资源进行非正常使用或越权使用等。导致此类安全隐患的原因主要是未对整个技术平台采取强制物理隔离，而采用逻辑隔离或伪物理隔离（物理隔离卡等）技术手段，另外内部操作员安全配置不当，或由于用户安全意识不强而共享、转借涉密账号等也可能导致该隐患的发生。

（3）破坏性入侵和干扰性入侵。指使用非法手段对地震应急基础数据系统进行删除、修改操作，或采用编织逻辑炸弹等方式干扰系统正常运行，改变系统正确运行方法，恶意占用系统资源，使得诸如地震应急指挥命令调度、地震快速评估与辅助决策等有严格响应时间要求的合法业务不能及时得到响应，极大影响指挥技术系统正常运转。

（4）计算机病毒入侵和软件漏洞。指地震应急指挥技术平台网络系统感染病毒造成网络拥塞，系统运行缓慢，核心业务无故宕机等，此类安全事故破坏性非常高，在日常运行维护中极易发生。

（5）外部环境破坏。指对应急指挥技术平台运行外部环境的破坏，例如对机房电力系统、恒温空调系统、通风系统、消防系统等的破坏，间接影响系统核心业务功能运行。

（6）新型入侵窃密手段。指使用电磁脉冲发生器、软件驱动嗅探器、硬件磁感应嗅探器等新型技术手段对技术平台进行入侵和干扰。

2 应急指挥信息安全体系设计分析及建设建议

为建立健全省级地震应急指挥中心信息安全体系，实现入侵防御和漏洞堵塞，就要对整个地震应急平台的操作系统安全、网络安全、数据库安全实施整体规划和设计。概况而言，就是要完善独立的硬件平台建设，建立全平台通行的身份识别系统，实现针对地震应急指挥技术系统操作人员的授权统一管理，同时通过权限对应急操作人员和数据资源之间进行严格的访问控制，各类应急数据库信息传输必须采用 SSL、SET、PGP 等数据加密技术以保证传输数据的完整性和保密性，并且需要建立一整套网络安全审计（NSAS）、入侵检测（HIDS/NIDS）及漏洞扫描机制，对整个应急指挥技术平台运转进行实时监控和防护，最终形成全局的安全管理体系。

2.1 管理机制建设

地震灾害具有突发性、难以预见和破坏力强的特点，应急处置的时效性强，震后数小时的有效处置对于挽救生命和减轻灾害损失尤为重要（苗崇刚，聂高众，2004）。在应急期内，地震应急指挥技术系统将承担应急指挥命令调度、震情快速评估与分析、灾情信息的快速获取与处理、紧急指挥决策评估和应急通讯保障等应急响应工作。基于以上职能，应结合自身业务需求，建立震时应急响应技术流程、日常机房管理制度、运维值班制度、系统巡检及灾备管理机制等，把技术手段和行政手段融为一体，首先从管理机制上完善信息系统安全保障能力。

2.2 物理环境配置

指挥中心信息系统是省级应急指挥技术平台进行灾情、震情数据汇集、分析、整合、共享、发布的重要设施，是场地、工具、流程的有机组合。在应用层面上，包含有震情快速评估、震区基础信息判断与展示、灾情分析与辅助决策等诸多应急响应相关应用技术平台。基于地震应急响应工作的特殊性，应用层业务对时效性、稳定性的要求远远高于一般信息系统的业务需求。因此，

在物理环境层面，应具备独立的供电、空调、消防及综合布线系统。根据服务器负载功率因素、负载率、逆变器效率等综合计算，在保证至少双市电接入的情况下，配备断电系统全负载运行不小于 4 小时的 UPS 供电系统。（$P = S/T$，当 UPS 核定容量 S 为固定值时，供电时间 T 与系统负载功率 P 成反比）。在综合布线方面，所有设备链接线缆应为六类 STP（屏蔽双绞线），网络设备机柜、应用服务器机柜、数据库服务器机柜应采用电磁频闭机柜。

2.3　系统布局和硬件选型

健全、完善的硬件平台是实现整个应急指挥中心核心系统信息安全的基础，合理的系统布局和硬件选型不仅从根本上巩固系统信息安全，更能从整体上为系统运行维护带来快速便捷的管理。图 1 为某省级地震应急指挥中心信息系统原型示意图。

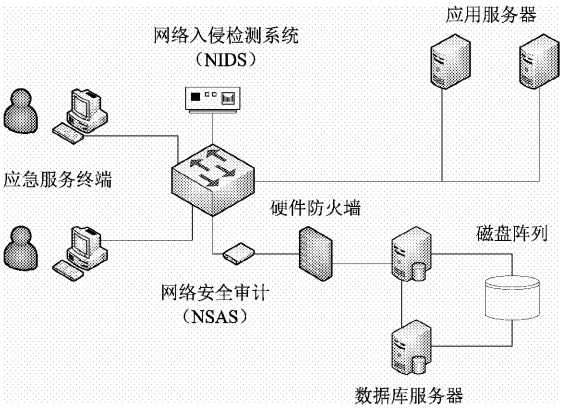

图 1　某省级地震应急指挥中心信息安全系统示意图

Fig. 1 Schematic diagram for information security system of a provincial earthquake emergency response commanding center

该原型系统的设计具备较高的信息安全等级，如图 1 所示，原型系统整体处于物理隔离状态，两台图形工作站作为灾情应用服务器和基础地理数据库服务器的访问终端，在数据库服务器等涉密核心网段前端装配硬件防火墙，阻断来自终端的非授权访问和干扰性入侵。

系统配置基于应急信息来源、数据分析引擎和快速响应组件三部分组成的网络入侵检测系统（NIDS），以系统总线日志、震情快速评估及辅助决策程序日志等作为数据源对象，通过收集和分析地震应急信息系统中若干关键节点的信息（如 ArcGIS Server 组件、IMS 端口、ArcSDE 服务等），检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。

全系统配备基于网络的硬件安全审计系统（NSAS），24 小时不间断运行，可根据与预设定条件库对地震应急快速评估系统中操作性数据流、分析性数据流策略进行审计，通过知识库对数据进行分析，识别出包括 TCP、UDP、ICMP、IPX、HTTP、FTP、telnet、SMTP、NFS、DNS、POP2、POP3、IMAP、TFTP、finger、SSL、NETBIOS 等协议类型的入侵行为（吴毅，2004），如异常登陆、Web 服务器 DDos（Distributed Denial of Service）攻击、缓冲区溢出攻击等。可以有效的防止内部涉密信息的泄漏和非法信息的传播，并可以及时发现和响应网络攻击行为。同时，SAS 与 NIDS 的联动功能也使得整个应急技术系统信息安全品质得到很大的提升，从而在技术上为应急管理人员建立了一套基于事件的发现、响应、制止、分析和责任追究的防范机制，有效的防止外部入侵及内部涉密信息泄漏。

2.4　抗侵害及灾害备份能力

容灾技术是系统高可用性技术的一个组成部分，容灾系统更加强调处理外界环境对系统的影响，特别是灾难性事件对整个应急指挥信息体系的影响。应急指挥中心作为破坏性地震的应急指挥产所，承担地震应急指挥、通讯保障、快速评估、辅助决策等震时科技保障工作，基于以上工作职能，整体系统对数据灾难备份服务的需求比较明确，对灾难备份服务等级要求较高。在容灾备份标准方面，除了国家标准、行业标准之外，笔者还主要衡量和参考了两类国际通用标准，The Uptime Institute 白皮书（Tier 4）：《Tier Classifications Define Site Infrastructure Performance Background》，美国通信工业协会（TIA）发布的关于数据中心电信基础设施标准《ANSI/TIA－942－2005 Telecommunications Infrastructure Standard for Data Centers》（张飘，侯福平，2007），同时，笔者结合现有指挥中心技术系统运行管理经验，认为可采用两大类操作性和实践性较高的信息灾备模式。

2.4.1 基于整个应用的容灾备份机制

这种机制是传统的、投入最大的灾备机制。方法是建立两套或多套功能相同的应急指挥应用软件、数据库系统，互相之间可以进行健康状态监视和功能切换，当某一处系统因意外（如火灾、地震等）停止工作时，整个地震应急信息系统可以切换到备份单元，使得应急指挥信息系统功能可以继续正常运转。

基于整体地震应急指挥应用的容灾备份机制，其原理是利用专用的存储网络将关键数据同步镜像至备份中心，地震应急基础数据库数据不仅在原应急指挥信息系统进行确认，同时可以在备份中心进行确认。这一方案在本地和镜像的所有数据被更新的同时，利用了双重在线存储和完全的网络切换功能，不仅保证应急数据的完全一致性，数据存储和网络环境也具备了应用的自动切换能力。通常情况下，两套系统中的光纤设备连接中还提供了冗余通道，以备常规应急数据通道出现故障时及时接替工作。

图 2 为采用基于 SAN 网络（存储区域网络）的系统全灾备方式。该技术可以通过一个高性能网络（光纤通道），为地震应急模拟触发、快速评估、辅助决策等诸多服务器和基础数据库系统提供一个应急区域存储空间，通过容灾备份线路连接备份系统，SAN 网络凭借中央阵列服务器来应对各种地震应急指挥过程中的诸多存储需求，为应急镜像系统提供实时数据备份和其他诸如数据快照等功能，使得当主系统出现应用程序宕机或数据丢失时，可快速启用镜像系统完全恢复地震应急指挥技术系统功能。上述此类容灾备份机制属于灾难恢复最高级别的应用级容灾备份，具有最高的系统安全性和恢复运行效率，但此类灾备机制对硬件环境的投入具有较高需求。

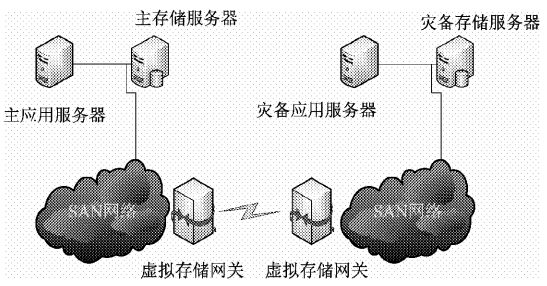

图 2 基于 SAN 网络的容灾备份机制

Fig. 2 Disaster recovery backup mechanism based on SAN network

2.4.2 基于虚拟机技术的容灾备份机制

该类灾备机制采用基于虚拟技术系统灾备方式实现。使用硬件的镜像技术和软件数据复制技术，实现应用站点与备份站点的数据同步更新。其原理如图 3 所示，该技术通过虚拟硬件运行环境，将地震应急指挥技术系统核心业务功能并行运行在单个或多个物理服务器上，对地震快速评估及辅助决策系统等多个系统核心业务来说，该服务器能够提供更加有效的底层硬件使用。同时，应急基础数据库数据在两个站点之间相互镜像，由远程异步提交来实现同步更新，该机制的优点在于使用了双重在线存储，因此在灾难发生时，几乎不会发生数据丢失问题，同时数据恢复响应时间可以被降低到分、秒级。

在虚拟系统中，中央处理器将分段划分出用于地震快速评估、应急辅助决策、甚至应急基础数据库运行的存储区域，整个应急关键业务平台部分（操作系统和各类应急评估程序）均运行在“保护模式”环境下，具有较高的安全性和稳定性。本方案是在本地系统完备的情况下对数据安全做的考虑，它还具备以下特性和优点：

首先，从各级地震应急技术平台现有的设备资源和计划投入的设备成本上考虑，最大化利用

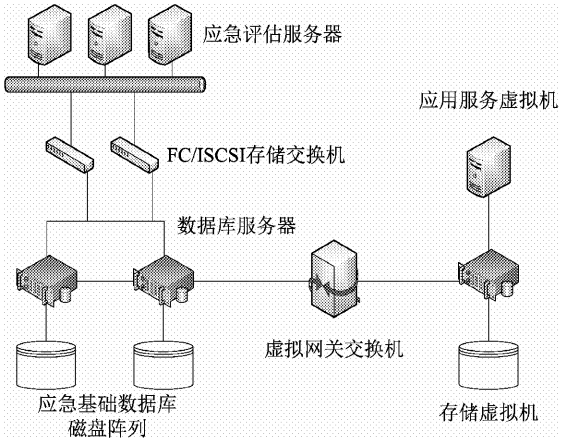

图 3 基于虚拟机技术的容灾备份机制

Fig. 3 Disaster recovery backup mechanism based on virtual machine technology

物理硬件的性能，并为以后更加规范化、简易化的设备管理，可对拥有多核高性能的物理服务器做虚拟化设置。虚拟化技术可以扩大硬件的容量，简化软件的重新配置过程，并且地震应急快速评估应用程序都可以在相互独立的空间内运行而互不影响，从而显著提高虚拟服务器的工作效率。

其次，在此基础上，再与另外一台相同配置和设置的服务器做双机热备操作，可以防止出现服务器的计划性停机与非计划性宕机造成的地震应急快速响应程序终止等问题，这样就有效的避免了应急指挥工作出现不必要的隐患和损失。

综上，这种方案在保证不影响当前应急业务运转的情况下，又能实时复制应急评估系统产生的数据到异地镜像，具有较好的系统安全性和一定的恢复运行效率，同时，这种数据灾备机制对硬件环境资源的投入较少，适合国内多数地震应急技术平台的推广应用。

3　总结和思考

目前，云南地震应急指挥中心已经建立了一套针对涉密数据系统的信息安全保障体系，并在实践中不断的健全、完善，但仍旧存在许多亟待改进的问题。例如指挥中心行业信息网及卫星通讯网的信息安全屏障，需要更多的依赖于行业卫星中心、卫星公司、地震行业网内连接的各省局信息中心的协同应对、共同努力，整个网络系统中任何一个节点或者终端遭到入侵，则整个网络的安全性都将不复存在；在体制规程方面，目前同时也缺乏信息安全防护指南等相关指导性文档，日常事务工作和相关业务部门的信息安全工作的开展往往各自为阵，缺乏更加具体化、规范化的指导；并且，在目前我国的诸多信息类项目建设初期，大多缺乏针对信息安全体系建设的设计和投入，导致系统建成运行后，难以开展整体性的信息安全保障工作。总之，应急指挥中心信息安全体系建设是一项复杂的系统工程，很多问题，有技术层面上的，也有存在于体制建设方面的，各省级地震应急指挥中心要适应新时代应急工作发展要求，提升自身地震应急科技保障水平，必须做到管理和技术并重，加强对信息安全风险防范意识的认知，重视安全策略管理的施行及安全教育工作。各类安全技术必须结合自身管理措施，充分考虑灾害备份和恢复机制，为应急技术系统指定适合自身实际情况的信息安全解决方案和管理机制，保障各省级应急指挥技术系统处于应有的健康状态。

参考文献：

姜立新，聂高众，帅向华 . 2003a. 我国地震应急指挥技术体系初探[J]. 自然灾害学报，12(2)：1－6.

姜立新，帅向华，张建福，等 . 2003b. 地震应急指挥管理信息系统的探讨[J]. 地震，(2)：117－122.

林山，刘凤仙 . 2011. 企业网络安全方案设计[J]. 福建电脑，(4)：117－119.

苗崇刚，聂高众 . 2004. 地震应急指挥模式探讨[J]. 自然灾害学报，13(5)：48－54.

帅向华，杨天青，马朝晖 . 2009. 国家地震应急指挥技术系统[M]. 北京：地震出版社 .

吴毅 . 2004. 军工企业信息安全建设方案[J]. 信息安全与通讯保密，(8)：71－72.

张飘，侯福平 . 2007. 数据灾难备份中心机房的规划与建设[J]. 电信技术，(9)：59－62.

中华人民共和国公安部(国务院令 147 号). 2007. 中华人民共和国计算机信息系统安全保护条例[S].

周璐 . 2005. 我国电子政务信息安全建设探讨[J]. 理论与现代化，(7)：107－108.

Preliminary Research on the Information-security System Construction of the Provincial Emergency Command Centers

LI Min, LI Yong-qiang, CAO Yan-bo

(*Earthquake Administration of Yunnan Province*, *Kunming* 650224, *Yunnan*, *China*)

Abstract

Analyzing the possible information security problems in the stage of planning, construction, management, and operation of the information-security system of the provincial emergency command centers, and combining with the current mainstream information-security technology, we comprehensively propose the reference solutions and new viewpoints to the information-security system construction of the provincial emergency command centers in terms of system design, hardware selection, anti-inbreak disaster recovery backup, virtual technology application etc..

Key words: earthquake emergency; technology system; information security