灾难恢复系统模型研究*)

王 琨[1] 袁 峰[2] 周利华[1]
(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)[1]
(国家信息安全工程技术研究中心 北京 100093)[2]

摘 要 根据某电子政务试点示范工程对业务可持续性的具体要求,论文提出一种灾难恢复系统模型。模型强化了通信保障能力,提供安全可靠的灾难恢复控制;创新地提出自我监测能力,实现对灾难恢复系统自身的完整性和安全性监测;使用GIS、GPS、RS技术使灾难恢复系统更易于使用、管理和维护。模型具有突出的安全性、健壮性和可管理性,适用于电子政务、银行等安全级别较高的环境。在RDRSM的指导下,某电子政务灾难恢复系统已经建设完毕并运行了一年。实践尤其验证了模型中灾难恢复计划、系统监测、通信保障的重要性。

关键词 电子政务,持续服务,灾难恢复,风险评估,备份

Study on Disaster Recovery System Model

WANG Kun[1] YUAN Feng[2] ZHOU Li-Hua[1]
(Ministry of Edu. Key Lab. of Computer Networks and Information Security, Xidian Univ., Xi'an 710071)[1]
(National Information Security Engineering and Technology Research Center, Beijing 100093)[2]

Abstract According to the requests of continuous service capability of a certain E-government Experimental and Demonstration Project of china, the paper presents a new Robust Disaster Recovery System Model. RDRSM strengthens the ability of safe communication and guarantees the secure command on disaster recovery. Its self-supervision capability can monitor the integrality and security of disaster recovery system itself. Using real-time visible platform provided by GIS, GPS and RS, the model can make disaster recovery system easier to use, manage and maintain. The model possesses features of security, robustness, controllability, and can be applied to highly security-critical environments such as e-government and bank. Conducted by RDRSM, an e-government disaster recovery system has been constructed over one year. Practice verifies the significance of some components in the model, such as disaster recovery planning, system supervision, communication support.

Keywords E-government, Continuous service, Disaster recovery, Risk assessment, Backup

1 引言

随着各种应用日益严重依赖信息技术,一旦信息系统失效会直接影响到应用。对于一些关键应用,即使是短时间的失效也是无法忍受的,因此必须建设灾难恢复系统,保障关键应用具备持续服务能力[1]。如何更好地保护系统,提供灾难恢复和持续服务能力已经成为国际上的研究热点。为保证系统的持续可用性,所需的灾难恢复级别日益提高,对灾难恢复的可靠性也有更高要求。应该以合理的代价保护应用系统数据的完整性和安全性,在灾难发生后尽快恢复运行,减少或尽可能消除业务停顿时间。这涉及一系列的关键技术,例如系统和网络的拓扑结构、设备冗余与系统备份、灾难恢复计划等[2]。灾难恢复系统模型研究就是非常关键的研究之一。

目前已经有一些灾难恢复模型,例如Business Continuity Planning(BCP)[3]、RoboCup-Rescue[4]、CoStore[5,6]、Disaster Management System (DMS)[7]、Continuity of Operations Planning (COOP)[8]和基于应用服务供应商的模型[9,10]。BCP是一种过程驱动的通用模型,通过分析和更新商业持续计划实现灾难恢复。由于它侧重于商业领域,因此对一些安全问题涉及不够,不能保障系统自身的安全性和完整性,不适用于对安全性要求非常高的环境。它不便于系统的使用与维护。RoboCup-Rescue论述了使用机器人和人工智能技术应对灾难的重要性,在系统的可视化方面有较好的表现。CoStore论述了建设可靠、高可用的存储系统,适用于校园网规模的网络环境,可以在不影响系统性能的情况下,提高存储系统的待命性。DMS用于减少重大灾难中人员生命损失,降低灾难恢复的代价。COOP目的是保障政府处理和应对各种突发事件的能力,它和DMS都不是专门为保护信息系统和为信息系统提供持续服务能力而设计的。总之,这些灾难恢复模型有的不是专注于保护信息系统,有的模型虽然可以用于保护信息系统,但是它基于应用服务供应商,安全性不高;有的模型无法承受重大灾难;还有的模型不便于使用、管理和维护。

中国"十五"某电子政务试点示范工程(EEDP,E-government Experimental and Demonstration Project)要求保障核心政府部门在重大灾难时具备持续服务能力。由于对安全性、可靠性、系统性能和互操作性要求非常高,加之国内缺乏可借鉴的成功经验,在深入研究中国电子政务体系[11]、多种灾难

*)基金项目:国家"十五"重点科技攻关计划(2002AA1Z67101)。王 琨 博士研究生,研究方向:网络与信息安全。袁 峰 高级工程师,研究方向:网络与信息安全。周利华 教授,博士生导师,研究方向:网络与信息安全,网络多媒体。

和灾难恢复系统(DRS,Disaster Recovery System)的基础上，论文提出并论述了健壮的灾难恢复系统模型(RDRSM,Robust Disaster Recovery System Model)，用于指导 EEDP 中 DRS 的建设。RDRSM 强化了安全性和可靠性，它在如下方面区别于其它模型：提出系统模拟与监测，实现对系统自身的完整性和安全性监测和对灾难的模拟；RDRSM 格外强调通信系统的可靠性；它重视结合 GIS 提供实时的 2D、3D 操作平台，更易于 DRS 的使用、管理和维护。

2 EEDP 简介

建设 DRS 之前，必须深入研究系统需求、需要应对的灾难、需要保护的资源及系统弱点。EEDP 必须能够应对众多人为、自然因素灾难[3,12]和安全威胁，尤其是 NRC(National Research Council)重点强调的恐怖主义袭击，它们破坏性巨大，而且在灾难恢复过程中还继续存在人为干扰和破坏。EEDP 的网络连接如图 1，系统由 ATM 交换机构成主干网，连接下级政府部门、上级政府部门和它的异地分支部门、异地备份中心。通过专线电话、PSTN、无线电话网、有线计算机网络和卫星通信提供可靠的通信保障。EEDP 的 DRS 在灾难发生后能够实时完成系统切换、通信、指挥、调度操作；结合密码技术，实现系统数据、通信、指挥控制等的认证、保密性、完整性和抗抵赖性；提供详尽的灾难恢复计划，以迅速、适当地应对灾难；使用地理信息系统(GIS, Geographic Information System)和决策支持系统(DSS, Decision Support System)，使 DRS 更易于使用、管理和维护。

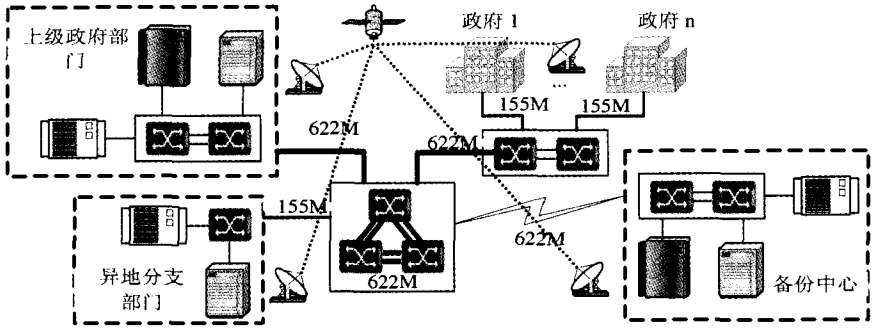

图 1 EEDP 网络连接图

3 健壮的灾难恢复系统模型

RDRSM 模型如图 2 所示，它包括咨询与培训(CT,Consultation and Training)、风险评估(RA,Risk Assessment)、灾难恢复计划(DRP,Disaster Recovery Planning)、模拟与检测(SS,Simulation and Supervision)、灾难恢复控制(DRC,Disaster Recovery Control)和系统管理(SM,System Management)这几个环节。

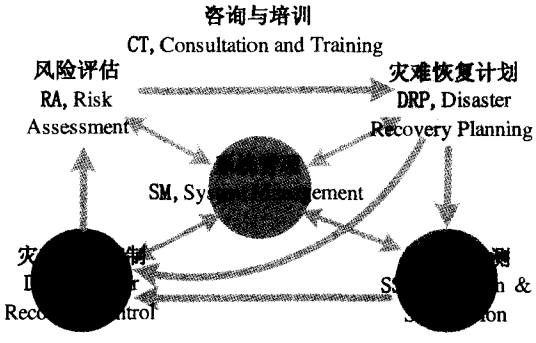

图 2 健壮的灾难恢复系统模型图

由于性能、安全性、带宽等众多因素的互相制约，为实现业务的可持续性，设计 DRS 上的应用系统时不得不权衡高性能与高可靠性之间的关系。对于高安全性的应用可以使用 2-safe，它的原子特性能保证数据中心与备份中心数据的一致性，避免损失已经处理完毕的事务。但它会增加资源竞争的冲突，减少吞吐量，而且备份中心出现故障时，数据中心必须改变它正常的工作方式。1-safe 可以减少由于资源竞争带来的事务处理延迟，即使备份中心不可用时数据中心仍然可以正常工作，更容易实现一个数据中心支持多个备份中心，但是灾难发生时会丢失一部分未来得及传输的事务。为实现安全性与系统性能的折中，可以在关键部分使用 2-safe，次要的地方使用 1-safe。此外，在保障 DRS 及时有效地切换系统、指挥调度、故障排除的同时，为确保 DRS 的安全、可靠和易用，RDRSM 还有如下总体要求：

1)安全可靠的通信保障是灾难恢复的关键，必须尽可能利用多种通信手段，确保通信的畅通无阻。尽可能采用不同安全级别的密码技术保护数据的存储、传输和访问控制。

2)采用 DSS 分析海量数据，为决策者提供科学的决策依据。

3)DRS 通常覆盖范围较大，使用 GIS 提供直观的操作平台，便于 DRS 的使用、管理和维护。

3.1 咨询与培训

CT 是 DRS 中非常重要，并且最容易被忽略和出问题的环节。EEDP 之所以进展顺利，首先得益于在项目建设及系统运行过程中，始终有良好的咨询与培训。DRS 涉及面非常广、牵扯行业非常庞杂，这迫切要求聘请众多领域的资深专家。CT 的内容涉及 DRS 及所有相关的问题，例如政策、法规等。

灾难恢复方面，在咨询、培养信息安全专家的同时，还要普及安全教育，课程设置要理论与实践相结合。灾难恢复往往需要不同部门的工作小组共同协作才能完成，必须使 DRS 中所有协调人员都具备必要的安全理念，使 DRS 中所有设计、开发、使用、管理和维护人员掌握熟练的专业技能，能够互相协调应对意外灾难。与传统的安全培训不同，灾难恢复的培训主要集中在新安全技术的设计、开发和使用方面。需要强调的是，由于人们很难直接解决所有的问题，因此还要着重培养学生判断和识别信息保护程度，以及在适当情况下与相关部门协调工作的能力。

3.2 风险评估

风险指某个安全威胁发生的可能性，以及由此而引起的经济、信誉和商业伙伴损失等，需要建立长期的风险评估机制评估应用和灾难类型。RA 是 DRP 的基础。另一方面，RA 能够收集 DRC 的反馈信息，使 DRS 总结经验教训，不断提高系统性能。EEDP 中把灾难抽象成安全威胁和危害级别。

在发生现场 L，具有某种危害动机 M，采用危害行动 A，某个危害实施者 D 会对系统造成危害，安全威胁是四元组 (D,M,A,L)。危害级别 G 是对安全威胁可能造成的破坏等级的评估。

$$G=(D,M,A,L) \tag{1}$$

必须明确标识所有安全威胁和需要保护的应用与资源，通过分析不同安全威胁对不同应用与资源的破坏程度，应用与资源对破坏的时间、经济敏感度，区分应用与资源的优先级。这对于 DRP 非常重要。

3.3 灾难恢复计划

DRP 通过有序的计划应对意外灾难，它包含许多子灾难恢复计划(SDRP，Sub DRP)。DRP 需要与 DRC、RA、SS 和 SM 交互，它协助 SM、DRC 管理、控制和维护 DRS；它协助 SS 模拟灾难，发现系统的不足，不断完善系统。RA 对安全威胁、资源及其优先级分析完成后，就可以开始 DRP 了。虽然 DRP 至关重要，目前人们却更侧重于开发灾难恢复的软硬件工具，而在 DRP 方面的研究还远远不够。EEDP 的经验证明：设计一个好的 DRP 是非常重要的，同时也是非常困难的。

DRP 包括商业影响分析和恢复计划设计。商业影响分析研究某个应用或资源的中断对其它应用的影响。主要有两个度量：一个度量是某个应用或资源崩溃后，其它应用还能持续正常运行的最大时间；另一个度量是恢复崩溃应用需要占用的资源。应该尽量要找到两者的最佳接合点，优化灾难恢复。恢复计划设计涉及灾难恢复中的许多策略和计划，例如数据备份策略，组建救援维护小组，资源维护计划，权衡维护或替换损毁设备的代价等。

必须确保 DRP 中没有遗漏任何重要资源，保证所有 SDRP 需要的人力、物力、甚至时间等资源是都可行的，不同 SDRP 之间不会产生冲突。信息系统在灾难发生时出现的故障具有大批量的特点，因此在 DRP 的设计中应制订排除大量并发网络和系统故障的计划。必须避免 SDRP 单独可行，不同 SDRP 在相同时刻却由于资源竞争冲突导致它们在一起时却不可行这种现象。由于 DRS 本身固有的复杂性，仅凭直觉和经验要从众多可选的 SDRP 中选择最优的子集用于灾难恢复几乎是不可能的，因此，迫切需要对 DRP 进行深入研究，建立数学模型，对 DRP 进行精确量化的分析，帮助决策者控制灾难恢复。此外，作为一种特殊的项目，DRS 也具有所有项目的共性，这意味着很可能由于不可预见的因素 DRP 中某些部分会失败，从而影响灾难恢复。

3.4 灾难恢复控制

借助于 DRP、SM 的帮助，DRC 最终实现灾难恢复。正常情况下业务运行在数据中心，当数据中心某些子系统发生故障时，系统会自动快速切换到数据中心的正常设备，实现本地故障恢复。当数据中心崩溃时，备份中心会接管数据中心继续提供服务，同时，DRC 广泛采集各方面的数据，控制系统从灾难中恢复过来。数据中心修复后，备份中心将数据和运行状态同步回数据中心，将业务处理切换回数据中心。系统由正常工作状态进入灾难恢复状态有自动控制和人为控制两种方式，让 DRS 自动区分瞬时故障与灾难是非常困难的，因此，通常需要人为控制使系统进入灾难恢复状态。

根据系统安全需求，备份中心应与数据中心保持足够远的距离，并且使用足够的带宽相互连接；备份中心必须具备足够的计算能力接管数据中心的业务；两个中心之间应用的切换必须快速可靠。EEDP 中备份中心建设在五百公里之外，通过 622Mb/s 带宽链路与数据中心相连，两个中心的配置基本相同，并且同时运行相同的软件，以减少灾难发生时备份中心装载软件所带来的延迟，实现迅速切换。

通信安全事关灾难恢复的成败。出于安全原因，目前中国政务涉密网禁止使用无线计算机网络。EEDP 中结合密码技术，使用多种有线、无线通信系统保障安全可靠的通信。必须在网络中保持适当的冗余，由于 PSTN 拥有大量的冗余节点和链路，结合密码技术，有时它反而比专线通信更安全。

3.5 模拟与监测

SS 包括灾难模拟和系统监测。SS 与 DRP、SM 和 DRC 交互，通过 2D、3D 操作平台模拟灾难，或者根据以往灾难中采集的数据重放灾难。模拟结果会反馈给 CT、DRP、SM、DRC，在灾难前及早发现、解决 DRS 中技术、管理、协作等方面存在的问题。

系统监测用于不断发现和排除系统在功能、性能和安全方面的隐患。作为一个健壮的系统，DRS 需要运行在安全的环境中，这就需要本地和远程攻击监测。EEDP 中就部署了很多防病毒、防火墙、入侵监测、日志审计等系统。此外，SS 中还包括网络性能监测、安全性能监测和业务性能监测等。

需要格外注意的是由于对 DRP 进行完整的测试非常困难，因此首先必须集中监测 DRP 中的所有 SDRP，保证所有 SDRP 单独可行。在此基础上根据实际情况尽量制订多种联合监测方案，确保多个 SDRP 在一起时也是可行的，从而在某种程度上确保 DRP 的有效性。

3.6 系统管理

与 CT 一样，SM 也是非常重要，而又容易被忽视的环节。DRS 往往由于管理上的缺陷而导致整个系统达不到预期目标。EEDP 特别加强了这一环节，除日常使用、维护人员外，还建立了专业的应急事件响应小组，制订了应急事件响应工作流程框架。采用良好的管理工具更有助于管理各环节中的资源和灾难恢复的实施。必须牢记：技术不能解决一切问题，管理同样非常重要。

结束语 根据某电子政务试点示范工程的建设要求，论文提出并论述了健壮的灾难恢复系统模型。模型中自我监测和实时可视平台使 DRS 更易于使用、管理和维护；模型加强了安全性与健壮性，适用于安全级别较高的环境。在 RDRSM 的指导下，该电子政务工程的灾难恢复系统已经建设完毕并且投入使用了一年。实践尤其验证了模型中灾难恢复计划、系统监测和通信保障的重要性。

参 考 文 献

1 King R P, Halim N, Garcia-Molina H, Polyzois C A. Overview of Disaster Recovery For Transaction Processing Systems. In: Proc. of 10th Intl. Conf. on Distributed Computing Systems, 1990. 286～293

2 Andrews R A. An Ounce of Prevention: Guidelines for Preparing a Disaster Recovery Plan. In: Proc. of the IEEE 1994 National Aerospace and Electronics Conf. 1994. 802～806

(下转第 124 页)

系统对公司的风险监管分为两类：一类是对基本指标(如流动负债)的实时监管，只需在系统中预先为其设置好预警值即可；一类是对公司风险的综合监管，它需要结合债权、债务、收入、支出等各类数据建立风险监管模型，以确定公司的抗风险能力，下面就对这个监管模型加以说明。

系统的综合风险预警模型借鉴了美国 Edward I. altman 博士提出的 Z-Score 预警模型，并根据期货公司的特点，确定风险预警模型：

$Z=3.1X_1+0.9X_2+1.8X_3+1.6X_4+0.2X_5$

其中，X_1= 净资产/保证金余额 =(所有者权益+风险准备-一年以上账龄的应收款项-待摊费用-固定资产净值-无形资产-开办费及长期待摊费用)/保证金余额

X_2= 风险准备金余额/客户保证金余额

X_3= 风险准备金余额/净资产

X_4=(货币资金+短期投资)/保证金

X_5= 封闭圈内自有资金余额/监管部门最低要求

在该模型中，Z-score 越小，表明该期货公司面临的风险就越大，在系统中当 Z-Score 小于 1.6 时，就开始对其进行预警，并要求监管人员对其各个指标进行详细分析，得出风险产生的具体原因。利用 OLAP 技术，可以方便地根据期货公司财务、监管数据计算和分析其 Z 值大小，从而对公司可能出现的风险提出预警。

4.3 安全控制

由于期货公司风险监管系统的特殊性，因此系统对于安全性的要求比较高。系统从“物理层”、“系统层”、“数据层”三方面对数据的安全性进行了控制。

物理层：通过物理隔离网闸+防火墙技术和入侵检测/网管系统，可以保证系统内部网资源与外部资源的双重隔离和监控。当外部网络需要访问内部网络时，需要通过网闸和防火墙才可以进入。系统的通信安全可通过 SSL(Security Socket Layer，安全套接字协议层)安全机制使用数字证书来实现。SSL 位于 HTTP 层和 TCP 之间，建立用户与服务器之间的加密通信，确保所传递信息的安全性。

系统层：系统中的安全控制通过角色与权限管理来实现。角色同组织关联，也即是允许不同组织的同一角色存在不同的权限，这样给组织定义自己的角色以更大的灵活性。系统中角色包括两类：一种是实际中存在的角色，如证监会用户、各地证监局用户，它们被赋予相应的权限。另一种是虚拟角色，这种角色仅代表一定权限的集合，是为了方便权限管理和权限赋予而设定的。另外系统管理员可以根据工作需要单独为部分用户添加、删除某些权限。系统把各子系统、模块中的操作权限按照树型结构进行了细分，在权限关系上模仿实际中的继承关系，便于对角色和用户进行权限配置。用户所属角色的权限决定了该用户能够完成的对象操作。系统根据用户的角色和权限为其分配相应的二级菜单项和显示不同的用户界面。

数据层：对于每一个角色相同的用户其访问的数据库权限也有许多不同，如证监局管用户可以访问自己片区的期货公司及营业部的情况，而期货公司用户只能访问自己公司和下属营业部的情况。用户在数据报送和审批管理中，对任何一个信息进行修改，系统都会自动留痕(记录用户名、原始信息、修改原因和日期)，以便进行责任追踪，这些功能都在数据库设计及代码具体编写中实现。

结论 J2EE 的优点在于跨平台、可复用、安全性；MVC 和数据持久层的优点在于降低了系统各部分之间的耦合性，增强了系统的可扩展维护性；OLAP 的优点在于能对各类数据进行整合、分析，并给用户一个智能、友好的交互界面，所以，期货公司风险监管系统是一个优势的有机结合。

基于 J2EE 的期货公司风险监管系统的开发，使中国证监会对期货公司、营业部和交易所的监管工作完全实现数字化，监管工作更加规范、科学和全面。基于 Web 界面的客户端操作方便、直观，可以进行快速查询和智能风险预警，提高了工作效率。该系统经正式使用后，取得了良好效果，极大地提高了我国对期货公司的监管力度，降低了监管成本，为我国期货市场的健康、快速发展提供了强劲动力。本系统也是解决大型金融监管问题的一个有益尝试，研究和开发其体系结构、相关技术具有重要的意义。

参 考 文 献

1 Cattell R, Inscore J. J2EE Technology in Practice: Building Business Application with Java 2 platform, Enterprise Edition [M]. Upper Saddle River, NJ: Addison-Wesley, 2001

2 刘大康. 层次分析法在市场细分中的应用[J]. 西南师范大学学报，2003，28(4)：55～57

3 Hastie T, Tibshirani R, Friedman J. 范明，柴玉梅译. 统计学习基础——数据挖掘、推理与预测[M]. 北京：电子工业出版社，2004

4 倪晓秋，季民，王光伟，等. J2EE 案例开发[M]. 北京：中国水利电力出版社，2005

5 孙卫琴. 精通 Strtus：基于 MVC 的 Java Web 设计与开发[M]. 北京：电子工业出版社，2004

6 江平，左春，陈宝兵. 基于 J2EE 体系结构的保险电子商务系统的设计研究[J]. 计算机应用研究，2004，21(3)：18～20

(上接第 104 页)

3 Lam W. Ensuring Business Continuity. IT Professional, 2002, 4(3): 19～25

4 Kuwata Y, Shinjoh A. Design of Robocup-Rescue Viewers - Towards a Real World Emergency System. Lecture Notes in Computer Science, 2001, 2019: 159～168

5 Chen Y, Ni L M, Xu C Z, Yang M Y, Kusler J F, Zheng P. CoStore: a Reliable and Highly Available Storage System Using Clusters. In: Proc. of thel6th Annual Intl. Symposium on High Performance Computing Systems and Applications. Los Alamitos, California, USA, June 2002. 3～11

6 Chen Y, Ni L M, Yang M Y. CoStore: a Storage Cluster Architecture Using Network Attached Storage Devices (Dissert). East Lansing, USA: Michigan State University, 2002

7 Uddin N, Engi D. Disaster Management System for Southwestern Indiana. Natural Hazards Review, 2002, 3(1): 19～30

8 Ehrlich R L, Droneburg J W. Preparing for an Emergency: COOP Planning for State Agencies. Maryland State Agencies Continuity of Operations Planning Manual. Available at: http://www.umaryland.edu/healthsecurity/docs/Manual%20Final.pdf. Jan. 2004

9 Liu B J, Cao F, Zhou M Z, Mogel G, Documet L. Trends in PACS Image Storage And Archive. Computerized Medical Imaging and Graphics, 2003, 27(2-3): 165～174

10 Liu B J, Cao F, Documet L, Sarti D, Huang H K. A Fault-Tolerant Back-up Archive Using an ASP Model for Disaster Recovery. In: Proceedings of SPIE - The International Society for Optical Engineering, 2002. 89～95

11 国家信息安全工程技术研究中心，国家信息安全基础设施研究中心. 电子政务总体设计与技术实现. 北京：电子工业出版社，2003

12 Fallara P. Disaster Recovery Planning. IEEE Potentials, 2004, 22(5): 42～44