统一灾难备份中心的业务调度模型

吴 俊
(上海信投建设有限公司 上海 200040)

摘 要 针对灾难备份中心必须达到对客户恢复目标的承诺,研究了灾难恢复主要量化目标——恢复点目标。研究发现传统数据复制方式对达到恢复点目标的风险,从而提出恢复点目标风险模型,并按照实际需求改进为业务调度模型。将模型应用在日常灾备工作中,实现了灾备中心对多用户多业务的灾备作业进行有效管理,确保了灾备中心的正常运营。

关键词 灾难恢复 灾难备份中心 数据复制 恢复点目标 恢复点目标风险模型 业务调度模型

中图分类号 TP3 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2013.12.087

BUSINESS SCHEDULING MODEL OF UNIFIED DISASTER REDUNDANCY CENTRE

Wu Jun
(*Shanghai SII Construction Co., Ltd., Shanghai 200040, China*)

Abstract For disaster redundancy centre must meet the commitment of customer's recovery objectives, in light of this, we study the main quantified target of disaster recovery——recovery point objectives, and find the risks of traditional data replication mode in achieving the recoverypoint objectives, then present the risk model of recovery point objective, and update it to the business scheduling model based on the practical need. The model is applied in day-to-day disaster redundancy work, and achieves the effective management of the disaster redundancy centre on the disaster recovery operations with multi-user multi-service, it ensures the normal operation of the centre.

Keywords Disaster recovery Disaster redundancy centre Data replication Recovery point objective Recovery point objective risk model Business scheduling model

0 引 言

在政府、行业和企业的关键业务系统几乎全部信息化的今天,保持业务运行的连续性已成为首要考虑因素,人们清楚地看到信息系统容灾是何等重要[1]。同时,为了有效利用集约化的资源,上海市集中建设统一的电子政务灾难备份中心。

项目的定位是数据级的远程灾难备份系统,利用上海市电子政务外网网络这样一个广域网平台,建设面向全市范围各家委办局单位的集中式同城的灾难备份中心。

传统的灾备模式均是系统"一对一"[2,3]的容灾,即生产系统与灾备系统组成两个基本同构的系统进行灾难备份和恢复。但是,上海没有统一的电子政务数据中心,要建成统一的电子政务灾难备份中心,必须面对分散在全市的几十家委办局单位,上百个系统节点,千余个信息系统的灾备数据及其灾备作业。为了能够在物理上、逻辑上同时提供统一容灾服务的灾备中心,达到集约化、高效率、低成本的建设目标,项目打破传统灾难备份系统"一对一"的实现方式,创新了"一对多"的数据级同城灾难备份中心模式。在这种模式下,灾备中心为了达到对用户的服务承诺,在有限的资源约束下,使灾备任务达到承诺目标,必须设计适应管理不同用户多个作业的灾备业务调度模型和调度系统。

本文探讨灾备系统与"恢复点目标"之间的关系,研究 RPO (recovery point objective)风险模型,结合项目需求设计了一个业务调度模型的实例,解决了单个灾备中心对多个用户任务进行有效调度的问题。研究结果可以用于各类采用异步方式的灾备系统。

1 衡量灾备中心恢复能力的量化标准与实际需求

衡量灾备中心恢复能力的主要量化标准是"恢复点目标"和"恢复时间目标",根据国家标准[4]的定义:

恢复点目标 RPO 和恢复时间目标 RTO(recovery time objective)是衡量灾备中心恢复能力等级的量化指标,可以作为灾备中心提供给各类用户服务承诺的目标标准。

RPO:灾难发生后,系统和数据必须恢复到的时间点要求。

RTO:灾难发生后,信息系统或业务功能从停顿到必须恢复的时间要求。

RTO/RPO 与灾难恢复能力等级的关系具体见表 1 所示。

收稿日期:2013-05-05。上海市财力投资项目(沪发改投(2009)第 237 号文)。**吴俊**,工程师,主研领域:系统架构,容灾,网络与存储技术,项目管理。

表 1 RTO/RPO 与灾难恢复能力等级的关系

灾难恢复能力等级	RTO	RPO
1	2 天以上	1 天至 7 天
2	24 小时以上	1 天至 7 天
3	12 小时以上	数小时至 1 天
4	数小时至 2 天	数小时至 1 天
5	数分钟至 2 天	0 至 30 分钟
6	数分钟	0

项目定位为数据级灾难备份[5]，参照国标第 3 级的标准，采用了多种容灾技术[6,7]实现了数据级灾备。根据责任界面，灾备中心负责数据的复制和存放，提供恢复演练环境；各接入单位负责系统和数据的恢复。灾备中心的服务承诺以 RPO 为主，所以对各接入单位的 RPO 承诺为第 3 级——数小时至 1 天，即 $T_{RPO} \leqslant 24$ 小时。

为了达到服务承诺，灾备中心必须保证用户存放的灾备数据满足 RPO 的要求。

本文主要针对采用异步方式将数据复制、备份到灾备中心，这里主要研究恢复能力第 1 级至第 5 级的灾备系统，即 $T_{RPO} \neq 0$ 的系统。对于恢复能力第 6 级的灾备中心，T_{RPO} 必须等于 0，采用同步方式，不存在业务调度的情况，不再论述。

2 RPO 风险模型

本项目建设的灾备中心利用广域网将各家单位的数据传送、储存到灾备中心。由于带宽小、数据量大，每次作业时间会很长，作业时间成为影响 RPO 的主要因素。按照当时的一般认识，每次作业时间 $T \leqslant T_{\text{RPO}}$，则能保证恢复点目标，实现服务承诺。但是经过深入研究发现这样的认识存在问题。

由于 T_{RPO} 是一个时间指标，而时间是一个恒定向前的因素，我们可以将灾备作业放置于时间轴上，灾备工作是一个由一次灾备作业、作业之间的等待时间、下一次灾备作业组成的过程，如图 1 所示。

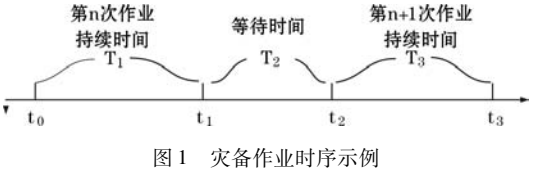

图 1 灾备作业时序示例

第 n 次灾备作业自 t_0 开始，灾备系统将用户在时间点 t_0 产生的灾备数据传输至灾备中心，经过 T_1 持续时间，于时间点 t_1 完成作业；经过 T_2 的等待时间，下一次作业即 $n+1$ 次作业于时间点 t_2 开始，将用户在时间点 t_2 产生的灾备数据传输至灾备中心，经过 T_3 持续时间于时间点 t_3 完成作业。这一过程会不断重复。

2.1 灾难发生时间与灾备作业的关系

结合灾备工作，讨论灾难发生时间对数据恢复点的影响：

第一种情况——灾难在第 n 次作业过程中发生，如图 2 所示。

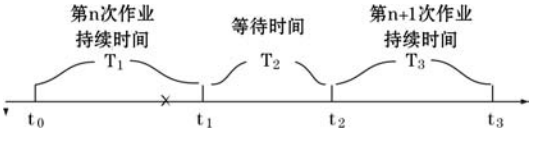

图 2 灾难在第 n 次作业过程中发生

1）第 n 次作业失败；

2）时间点 t_0 的数据无法恢复；

3）能够恢复的时间点是第 $n-1$ 次灾备作业的起始点。

这种情况也可以视同灾难在第 $n+1$ 次作业过程中间发生，如图 3 所示。

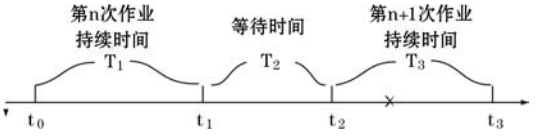

图 3 灾难在第 $n+1$ 次作业过程中发生

1）第 $n+1$ 次作业失败；

2）时间点 t_2 的数据无法恢复；

3）能够恢复的时间点是第 n 次灾备作业的起始点，即：t_0。

第二种情况——灾难在等待时间发生，如图 4 所示。

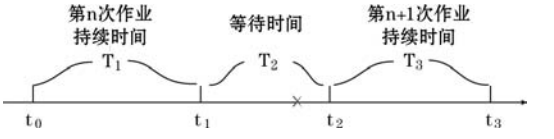

图 4 灾难在等待时间发生

1）第 n 次作业成功；

2）时间点 t_0 的数据可以恢复；

3）能够恢复的时间点第 n 次作业的起始点，即：t_0。

经过分析，可以看出：在完成下一次作业之前，都只能恢复本次作业起始点的数据。得出结论：在 $n+1$ 次作业完成之前，数据恢复点位于第 n 次作业的起始点 t_0。

2.2 灾难发生时间与 RPO 的关系

灾难发生时间与 RPO 的关系是：当灾难发生时，向前 RPO 规定的时间内可以恢复数据的时间点目标。

第一种情况——RPO 时间小于一次作业时间，即第 n 次作业时间 $T_1 > T_{RPO}$ 时，如图 5 所示。

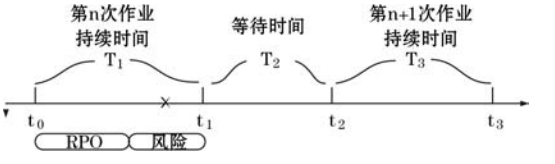

图 5 RPO 时间小于作业时间

当 $T_1 > T_{RPO}$，表示一次作业时间大于 T_{RPO}，很显然，灾备中心无法完成服务承诺。若灾难在图中“风险”区段发生时，第 n 次作业的数据无法恢复，灾难恢复失败。为了保证灾备业务正常开展，每次作业时间必须不大于 T_{RPO}，即：$T_n \leqslant T_{RPO}$。

第二种情况——RPO 时间大于第 n 次作业时间，但小于第 $n+1$ 次作业的完成时间，即 $T_1 \leqslant T_{RPO} < (T_1 + T_2 + T_3)$ 时，如图 6 所示。

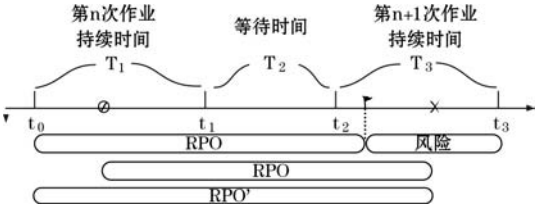

图 6 RPO 时间大于第 n 次作业时间且小于第 $n+1$ 次作业的完成时间

$T_1 \leqslant T_{RPO} < (T_1 + T_2 + T_3)$，当灾难发生在区间（$T_{RPO} - t_1$）里时，可以恢复时间点 t_0 的数据；当灾难发生在区间（$t_3 - RPO$）里时，灾难发生时间点向前 RPO 规定的时间段内并没有

找到可用的数据恢复点,根据之前的结论"在 $n+1$ 次作业完成之前,数据恢复点位于第 n 次作业的起始点 t_0。",向前 T'_{RPO} 到达 t_0 才能找到第 1 个可用的数据恢复点,由于 $T'_{RPO} > T_{RPO}$,作业恢复不能达到服务承诺,虽然第 n 次作业的数据完成传输,但是灾难恢复存在风险。

第三种情况——RPO 时间大于第 $n+1$ 次作业的完成时间,即($T_1 + T_2 + T_3$) $\leqslant T_{RPO}$ 时,如图 7 所示。

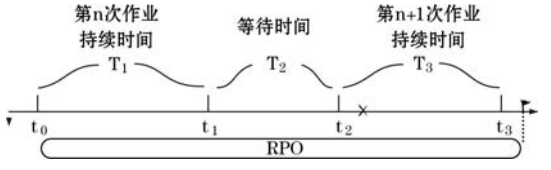

图 7　RPO 时间大于第 $n+1$ 次作业的完成时间

($T_1 + T_2 + T_3$) $\leqslant T_{RPO}$,当灾难在区间($t_3 - t_1$)里发生时,可恢复第 n 次作业的数据,可以恢复时间点 t_0 的数据;当灾难发生在($T_{RPO} - t_3$)区间时,可恢复第 $n+1$ 次作业的数据,可以恢复时间点 t_2 的数据。

根据以上分析,可以得出结论:

(1) 当($T_1 + T_2 + T_3$) $\leqslant T_{RPO}$ 时,灾备系统在没有风险条件下达到 RPO 要求

在以下两个条件同时有效的情况下,可以保证数据恢复点目标达到 RPO 的要求:

1) $T_n \leqslant T_{RPO}$

2) ($T_1 + T_2 + T_3$) $\leqslant T_{RPO}$

由于($T_1 + T_2 + T_3$) $\leqslant T_{RPO}$,则必然 $T_n \leqslant T_{RPO}$,以上结论可以简化为:

($T_1 + T_2 + T_3$) $\leqslant T_{RPO}$

公式可以表示为:

$$\frac{(T_1 + T_2 + T_3)}{T_{RPO}} - 1 \leqslant 0 \qquad (1)$$

(2) 当 $T_{RPO} <$ ($T_1 + T_2 + T_3$) $\leqslant 2T_{RPO}$ 时,灾备系统能达到 RPO 要求,但存在风险

当 $T_n \leqslant T_{RPO}$ 且 $T_1 \leqslant T_{RPO} <$ ($T_1 + T_2 + T_3$) 时,第 n 次作业的数据完成了传输,如果灾难发生在区间($T_{RPO} - t_1$)里时,可以恢复时间点 t_0 的数据,如果灾难发生在区间($t_3 - T_{RPO}$)里时,恢复失败。说明要达到 T_{RPO} 要求,存在一定的风险。

因为: $T_n \leqslant T_{RPO}$,所以: $T_1 \leqslant T_{RPO}$, $T_3 \leqslant T_{RPO}$;

因为: T_2 是等待时间可以用于调剂,所以: $T_2 \to 0$。

所以: $T_1 + T_2 + T_3 \leqslant 2T_{RPO}$

同时: $T_1 + T_2 + T_3 > T_{RPO}$。

则: $T_{RPO} <$ ($T_1 + T_2 + T_3$) $\leqslant 2\ T_{RPO}$

公式可以表示为:

$$0 < \frac{(T_1 + T_2 + T_3)}{T_{RPO}} - 1 \leqslant 1 \qquad (2)$$

(3) 当任何一次作业大于 T_{RPO} 时,灾备系统不能达到 T_{RPO} 要求

当 $T_n > T_{RPO}$ 时,灾备中心无法完成服务承诺。

因为: $T_n > T_{RPO}$,所以: $T_1 > T_{RPO}$, $T_3 > T_{RPO}$;

因为 T_2 是等待时间可以用于调剂,所以: $T_2 \to 0$。

所以: $T_1 + T_2 + T_3 > 2T_{RPO}$。

公式可以表示为:

$$\frac{(T_1 + T_2 + T_3)}{T_{RPO}} - 1 > 1 \qquad (3)$$

(4) RPO 风险值公式汇总

归纳以上公式计算,可以得出 RPO 风险值公式为:

$$\alpha = \frac{T_1 + T_2 + T_3}{T_{RPO}} - 1 \qquad (4)$$

当时 $\alpha \leqslant 0$,表示没有任何风险的情况下可以达到 RPO 要求;

当时 $0 < \alpha \leqslant 1$,表示在一定风险情况下可以达到 RPO 要求,α 越大且越接近 1 表示风险越大,反之风险越小;

当时 $\alpha > 1$,表示不可能达到 RPO 要求;

(5) 推论

1) 每次作业时间最多控制在多长时间可以保证达到 RPO 要求,且没有风险:

当 $\alpha \leqslant 0$ 时,即: ($T_1 + T_2 + T_3$) $\leqslant T_{RPO}$,可以在没有风险情况下达成 RPO 要求。

假设: 每次作业时间相近,即 $T_1 \approx T_3$;

为了计算最长时间, T_2 作为等待时间可以调剂,即 $T_2 \to 0$;

因为: ($T_1 + T_2 + T_3$) $\leqslant T_{RPO}$

所以: ($T_1 + 0 + T_1$) $\leqslant T_{RPO}$

即: $T_1 \leqslant \frac{T_{RPO}}{2}$

推论一　每次作业时间控制在 $\frac{T_{RPO}}{2}$ 的范围内,灾备业务是安全的。

2) 当作业存在风险,如何进行调度:

当 $0 < \alpha \leqslant 1$ 时,作业存在超时的风险。为了避免风险,要么灾难发生在 $n+1$ 次作业之后,要么让第 $n+1$ 次作业在区间($T_{RPO} - t_1$)时间范围内完成。由于灾难不可控,所以较为可行的做法是"让第 $n+1$ 次作业在区间 ($T_{RPO} - T_1$)时间范围内完成",以此来降低不能完成服务承诺的风险。即: $T_3 \leqslant T_{RPO} - T_1$。

由于: $T_1 > \frac{T_{RPO}}{2}$,所以: $T_3 < \frac{T_{RPO}}{2}$。

推论二　当作业产生风险时,应该尽量缩短 T_3 的时间, T_3 必须小于 $\frac{T_{PRO}}{2}$。

3) 传统灾备作业方法对实现 RPO 的风险:

传统灾备作业方法是每间隔一段时间开始一次作业,而间隔时间往往等于 RPO 规定的时间。如图 8 所示。

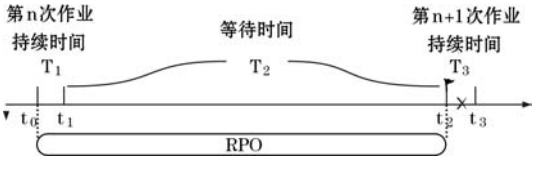

图 8　传统灾备作业方法

由于两次作业起始点的间隔时间为 T_{RPO},当灾难在下一次作业过程中发生时,即灾难在 T_3 发生时,则系统无法达到 RPO 目标。

设: $T_3 = n$,

则发生不能达到 RPO 的概率为:

$$P = \frac{n}{n + T_{RPO}} \qquad (5)$$

因为 T_{RPO} 为常量,当 n 越小,则 P 越小;当 n 越大,则 P 越大。

由于 $n \leqslant T_{RPO}$,根据以上公式可以得出: $P \leqslant 50\%$。

推论三　传统灾备作业方法会对实现 RPO 产生风险,风险一般不高于 50%。

对于采用独享的高带宽备用网络系统[8]，数据传输速度不再成为瓶颈，每次作业的持续时间都很短。根据风险概率公式 $P=\frac{n}{n+T_{RPO}}$，风险发生的概率往往很低。

3 灾备业务调度模型

在实际应用中，RPO 风险值 α 主要用于通过历史数据测算各家单位的平均风险值：

$$\alpha\text{平均}=\frac{(T_1+T_2+T_3+\cdots+T_n)}{n\times T_{RPO}}-1 \tag{6}$$

实际工作中，测算本次作业或者下一次作业的 RPO 风险值，需要对公式的取值进行调整，如图 9 所示。

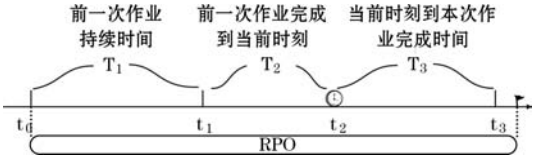

图 9 实际业务 RPO 风险值

将 RPO 风险模型中的下一次作业开始时间 t_2 替换为当前时刻，即前一次作业完成时间点 t_1 到当前时刻 t_2 之间的时间段为 T_2，代表前一次作业完成到当前时刻的时间，当前时刻 t_2 到本次作业完成时间 t_3 之间的时间段为 T_3，代表本次作业将要完成的时间。

由于 T_1 和 T_2 发生在当前时刻之前，都是已知的数值。

而 T_3 是预测数值，是用于预测 RPO 风险的关键值。对于定位数据级灾备的项目来说，由于广域网的网络带宽（用户出口带宽和灾备中心入口带宽）是灾备业务的主要瓶颈，所以影响作业完成时间的主要因素是数据量大小 g（Mb）和带宽 m（Mb/s）的大小。

g 代表：从当前开始，完成作业还需要传输多少数据量；

m 代表：当前网络带宽速率：

$$T_3=\frac{g}{m} \tag{7}$$

业务调度模型的 RPO 风险值公式是：

$$\alpha=\frac{T_1+T_2+T_3}{T_{RPO}}-1 \tag{8}$$

当 $\alpha\leqslant 0$ 时，无需预警；

当 $0<\alpha\leqslant 1$ 时，提示预警，说明本次作业能够在 RPO 内完成，但不能保证下一次作业能够在 RPO 内完成，需要关注当前和下一次作业的资源利用情况，当 α 越来越大时，风险越大，必要时进行干预；

当 $\alpha>1$ 时，说明本次作业不能在 RPO 内完成，系统可能存在问题，需要结合故障检测[9]进行排错，排除故障后，必须通过干预进行灾备业务的调度。

在实际应用“RPO 风险模型”转化为“灾备业务调度模型”时，必须考虑其他因素。由于灾备中心要面对多个用户单位，每个用户单位又有多个灾备作业同时发起，在调度时需要考虑客户作业优先顺序；对于正在执行的作业还要考虑它的剩余完成时间。

1）对正在执行的灾备事物进行干预，调度模型：

$$\beta=\alpha(\text{RPO 风险值})\times i_1+\text{客户作业优先级}\times i_2+\text{剩余完成时间}\times i_3 \tag{9}$$

其中：i 为加权系数，$i_1+i_2+i_3=1$，加权系数可以按实际情况调整。

2）对将要执行的灾备事务进行干预，调度模型：

$$\beta=\alpha\text{平均}(\text{RPO 风险值历史情况})\times i_1+\text{客户作业优先级}\times i_2 \tag{10}$$

其中：i 为加权系数，$i_1+i_2=1$，加权系数可以按实际情况调整。

当 β 越来越大时，风险值随之增大，调度优先级也越高。当风险值超过设定的阈值，需要对作业进行干预。

主要调度的方法：通过干预其他作业，将资源让给 RPO 风险值较高的作业，使其完成任务。当 RPO 风险值得到控制后，重新恢复被干预的作业。干预方式如表 2 所示。

表 2 灾备业务调度干预方式表

名称	说明
暂停	将当前正在执行的灾备事务进行暂停，让出计算和网络资源
延迟	将某一将要执行的灾备事务进行延迟操作，让出计算和网络资源
终止	终止某一正在进行中的灾备事务，让出计算和网络资源
限速	对某一正在进行或将要进行的灾备事务进行限速，让出网络资源

4 业务调度模型应用在容灾业务管理系统

由于业务调度模型明确，业务调度方法清晰，基于业务调度模型开发的业务管理系统很快得到应用。在政务外网带宽限制等现实约束条件下，通过业务调度，在保证用户正常生产业务开展的同时实现了多用户、多系统、多任务的灾备恢复点目标。如图 10 所示。

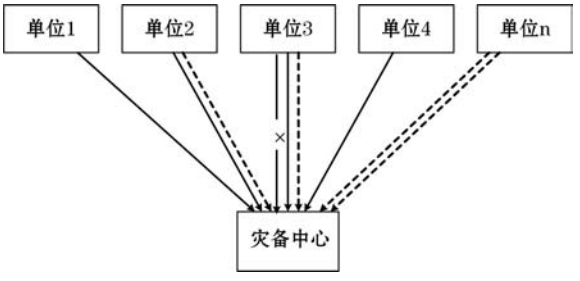

图 10 灾难业务管理系统

管理系统以列表、图示的模式，对各单位各项作业进行标注。对每个用户每个作业根据业务调度模型计算的风险值进行风险测算，分别通过实线、虚线、带有叉号标记的线进行标注：实线表示正常，虚线表示预警，带有叉号表示干预。对于灾备作业的业务调度工作根据业务调度模型开展。

灾备系统从项目验收运行至今，8 家接入单位共完成作业 30 491 次，根据业务调度模型，共提示 4 113 次预警，其中进行干预 48 次。灾备业务统计表如表 3 所示。

表 3 灾备业务统计表

序号	单位	完成作业次数	预警次数	干预次数
1	单位 1	1 464	573	19
2	单位 2	3 425	758	0
3	单位 3	4 023	1 459	0
4	单位 4	542	292	9
5	单位 5	440	82	0
6	单位 6	3 223	43	7
7	单位 7	15 816	712	13
8	单位 8	1 558	194	0
合计		30 491	4 113	48

通过业务调度模型的监控和干预,保障了灾备作业在预定时间内完成复制,使系统运行正常。系统运行至今,客户关于RPO 不达标的投诉为 0。

业务调度模型同时也提高了灾备系统的总体性能,通过对多个用户的多个任务的合理调度,有效利用了不太宽裕的系统资源。系统运行至今,灾备中心累计保护的数据量为 438015 GB。

2011 年,某单位核心生产存储设备发生严重故障,导致主要业务应用无法正常服务。灾备中心立即响应并开展了系统数据恢复工作,生产系统于当天基本恢复正常,未对该单位业务开展产生较大影响。经过核实,生产数据实际丢失量达到了灾备中心的服务承诺,业务调度模型有效保障了生产系统安全运行,为生产系统的有效灾难恢复发挥了决定性的作用。

5　结　语

根据研究得出的 RPO 风险模型、灾备业务调度模型为基础,开发了一个灾备业务管理系统,实现了面向多用户多任务的灾备业务管理,按照承诺的 RPO 要求,为各接入用户提供了有效的服务,保证了灾备业务调度任务。目前上海市电子政务灾难备份中心信息系统运行正常,获得了各方的高度评价,上海市电子政务灾难备份中心项目获得了“2012 年度上海市优秀工程咨询成果一等奖”。

参　考　文　献

[1] 杨义先,姚文斌,陈 钊. 信息系统灾备技术综论[J]. 北京邮电大学学报,2010,33(2):1-6.

[2] 汤建忠,潘民,沈瑾,等. 烟草异地数据灾备系统的研究与实现[J]. 计算机系统应用,2010,19(2):16-19.

[3] 施跃跃,徐景良. 金融行业灾备架构高指标 RTO 的实现方式[J]. 计算机应用与软件,2012,29(8):206-209.

[4] 中华人民共和国国家监督检验疫总局,中国国家标准化管理委员会. GB/T 20988-2007 信息安全技术信息系统灾难恢复规范[S]. 北京:中国标准出版社,2007.

[5] 何熹. 数据级灾难恢复的数据复制技术研究与分析[J]. 计算机安全,2010(3):40-42.

[6] 刘伟. 信息系统容灾建设的研究与探讨[J]. 数字通信,2011(6):59-61.

[7] 康潇文,杨英杰,杜鑫. 虚拟存储技术在容灾系统中的应用[J]. 计算机工程,2009,35(21):36-38,4.

[8] 王渝次,王秀,杨淑琴,等. 信息系统灾难恢复的规划及实施[TP·292][M]. 北京:北京交通大学出版社,2006.

[9] 毛秀青,陈性元,杨英杰,等. 面向容灾的自适应故障检测框架研究[J]. 计算机工程,2012,38(7):4-6.

(上接第 310 页)

5　结　语

本文结合三维集成原则来设计微波三维集成电路,并应用 Visual C++ 6.0、Visual Basic 6.0 等工具开发了一款用于微波电路三维集成设计的辅助软件:对于基础元件,实现编辑、综合和分析的功能;对于功能组件,实现编辑、设计功能。分别以微带线和微带线-微带线过渡结构为例,对上述功能进行阐述和验证。

参　考　文　献

[1] Connolly P. CAD software industry trends and directions[J]. Engineering Design Graphics Journal,1999,63:26-33.

[2] Pantoli L. Conversion matrix extraction by commercial CAD software for the stability design of autonomous circuits[J]. International Journal of RF and Microwave Computer-Aided Engineering,2010,20:313-320.

[3] Liu S. Integrated CAD Software with ERP Interface for Steel Portal Frames[J]. Advanced Materials Research,2010,139-141:2136-2139.

[4] Jansen R. A novel CAD tool and concept compatible with the requirements of multilayer GaAs MMIC technology[J]. Microwave Symposium Digest,IEEE MTT-S International,1985,1:711-714.

[5] 高葆新. 微波 CAD 软件智能化与专家系统[J]. 国际电子快讯,1991(4):27-31.

[6] 傅佳辉,吴群. 微波 EDA 电磁场仿真软件评述[J]. 微波学报,2004,20(2):91-95.

[7] Gupta K C,Ramesh Garg,Bahl I J. Microstrip Lines and slotlines[M]. Dedham:Artech House,1979.

[8] 廖承恩. 微波技术基础[M]. 西安:西安电子科技大学出版社,1994.

(上接第 324 页)

行研究,以邻界区的聚类生成为方式将训练样本和测试样本采用基于均值和标准差的 K 均值聚类算法进行聚类分析,然后对邻界区中远离分类超平面的样本数据点和噪声或过拟合进行样本筛选,提取可能的支持向量,最终以增量学习模式实现最优超平面的构造。最后通过与算法 Bayes、BP 算法、单个 SVM、多 SVM 融合检测算法等进行实验仿真对比,证明了该算法的优越性。

参　考　文　献

[1] Cortes C,Vapnik V. Support Vector Networks[J]. Machine Learning,1995,20(3):273-297.

[2] 刘晔,王泽兵,冯雁,等. 基于增量支持向量机的 DoS 入侵检测[J]. 计算机工程,2006,32(4):179-186.

[3] Syed N,Liu H,Sung K. Incremental Learning with Support Vector Machines[C]//Proc. of International Joint Conference on Artificial Intelligence. Stockholm,Sweden:[s. n.],1999:272-276.

[4] 牟琦,陈艺坤. 一种基于快速增量 SVM 的入侵检测方法[J]. 计算机工程,2012,12:92-94.

[5] 丁文军,薛安荣. 基于 SVM 的 Web 文本快速增量分类算法[J]. 计算机应用研究,2012(4):1275-1278.

[6] 李汉彪,刘渊. 一种 SVM 入侵检测的融合新策略[J]. 计算机工程与应用,2012,48(4):87-90.

[7] 徐永华,李广水. 基于距离加权模板约简和属性信息熵的增量 SVM 入侵检测算法[J]. 计算机科学,2012,39(12):76-78.

[8] 张永俊,牟琦,毕孝儒. 基于云模型的增量 SVM 入侵检测方法[J]. 计算机应用与软件,2013,30(3):311-314.

[9] 井小沛,汪厚祥,聂凯. 基于修正核函数 SVM 的网络入侵检测[J]. 系统工程与电子技术,2012,34(5):1036-1040.