金品业务应急系统

技术白皮书

北京金品高端科技有限公司

Beijing Jinpin Highpoint Technology Co.,Ltd

1 概述

随着计算机使用的迅速普及和互联网的广泛应用，各类信息系统安全持续运营问题日益突出，诸如病毒感染破坏、黑客攻击、误操作破坏、硬盘故障、人为破坏等安全问题，往往造成系统失常、文件损坏、文件丢失事故，更有甚者会引起数十台至数百台主 机系统崩溃，乃至所有系统信息和用户数据丢失等严重后果！一旦发生数十台甚至数百台主机系统和环境的重装，则短时间内难以恢复运营，而停止运营会造成比较重大的、有时是不可挽回和难以估量的损失。

根据调查，信息系统可能遭遇的各类灾难中，有 9%是硬件级别的故障，例如：主板、RAID 控制器、网卡、电源、内置/外置存储等设施出现问题，还有高达 91%的灾难成因是“软”错误，例如：数据误删除、黑客/病毒攻击、系统崩溃、打补丁造成不稳定等等。磁带备份、基于磁盘的备份、Cluster/HA 等传统的数据保护机制对于上述灾难都只能提供有限的保护。

信息系统是日常业务工作正常运行的关键要素，具有十分重要的作用，因此有必要针对信息系统目前的运行模式加以调整，增加相应的保护措施，以防止上述问题的出现。

为保证业务连续正常运行，很多安全手段被采用。传统的安全保障体系，大多基于防火墙、IDS、防病毒等技术构建单纯的防御体系，存在着较大的缺陷，如：对未知的攻击难于防范；对已知病毒采用对比法进除病毒导致系统不可预见风险，对未知病毒无法及时应对。传统的保护模式成本高、恢复时间长，难以满足业务连续性的要求，因此，必须采用新的保护手段弥补上述缺陷。

综上，我们开发出“业务应急系统”。采用数据存储、数据复制、iSCSI 及网络启动等多项技术，为业务系统提供从系统到数据的全方位保护和快速恢复。

保护系统和数据，瞬间恢复业务系统运行

2 业务应急系统

2.1 系统主要功能和特性

同时对多台服务器业务应急

一套业务应急系统可以同时对多个服务器进行保护。如果多个服务器上的业务同时出现故障，一套业务应急系统可同时应急顶替多个业务系统工作，并由系统管理员选择在网络相对空闲时将故障业务系统恢复到正常状态。对多个业务系统应急恢复时，仍然可以通过快照版本回滚功能选择最合适的版本做应急和恢复使用。

支持对操作系统及数据在线复制，支持定时多版本

业务应急系统可以在业务系统正常运行时，对操作系统、应用软件以及数据进行全方位的复制，并形成多时间点、多版本的历史快照。

- 支持全量和差异量复制；
- 灵活的快照时间策略；
- 可对任何指定的目录或文件进行复制。

对多台服务器自动恢复

自动恢复，是业务应急系统内置的一整套快照版本选择和恢复流程功能。一旦遇到应用系统出现故障时，由业务应急系统顶替业务系统运行，同时在业务应急系统的后台，设定恢复策略，包括恢复的目标卷、快照版本以及开始时间，设置完成后启用策略，自动执行恢复操作。

全方位的保护

区别于传统保护手段仅能对数据进行保护，业务应急系统可实现对操作系统、应用软件、数据库和数据文件的全方位保护。

安全和高可用

- 可抗拒任何病毒和攻击；
- 可有效保护系统、环境和数据；
- 通过 iSCSI、sBoot、sPXE 协议，由网络对多台服务器进行启动，几分钟 内恢复多台服务器的业务执行功能；
- 轻松使系统达到较高的可用性；

- 大幅度提高系统和数据的安全性和可用性。

管理便捷

- 系统和数据恢复后的烦琐的环境恢复全自动快速完成；
- 管理工作量减少至 5%以下，成本大幅度降低；
- 支持远程管理功能。

IP SAN 存储

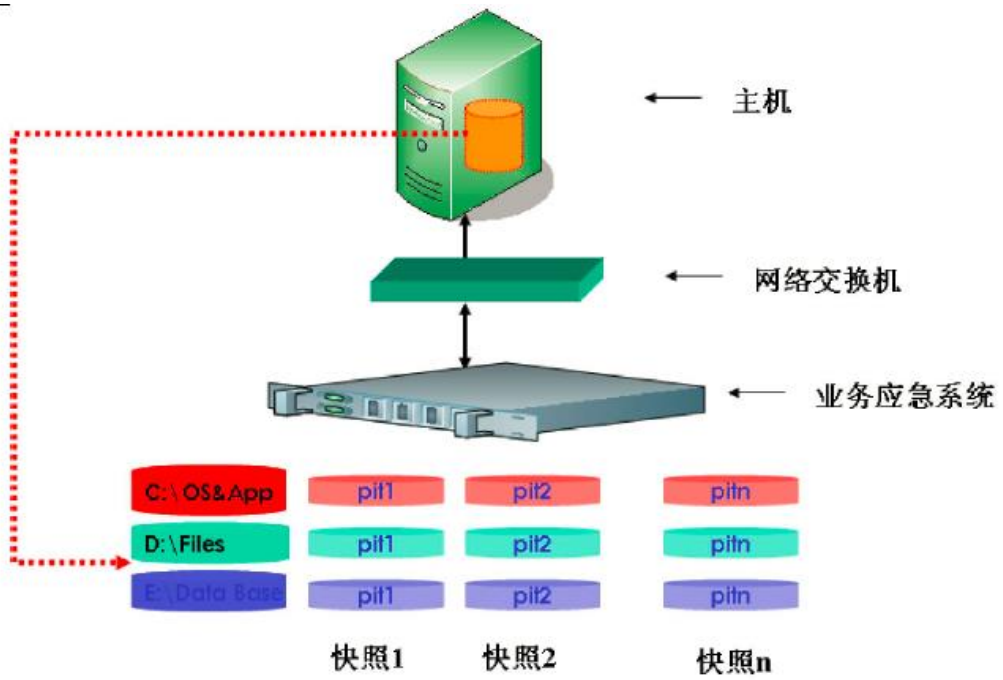
- 由网络 iSCSI 存储启动多台服务器，可支持系统运营所需的带宽和可靠性；
- 基于 IP SAN 的、对保护对象数据的集中存储；
- 成本低、容量大，扩展容易；
- 支持 RAID-5，RAID-6，RAID-1 方式的数据保护，可靠性高，成本低。

2.2 实现过程

业务应急系统对业务系统的保护分为两个阶段：业务系统正常运行阶段和业务系统应急阶段。

业务系统正常运行阶段

业务系统正常运行时，对业务系统进行在线复制，工作过程如下图所示：



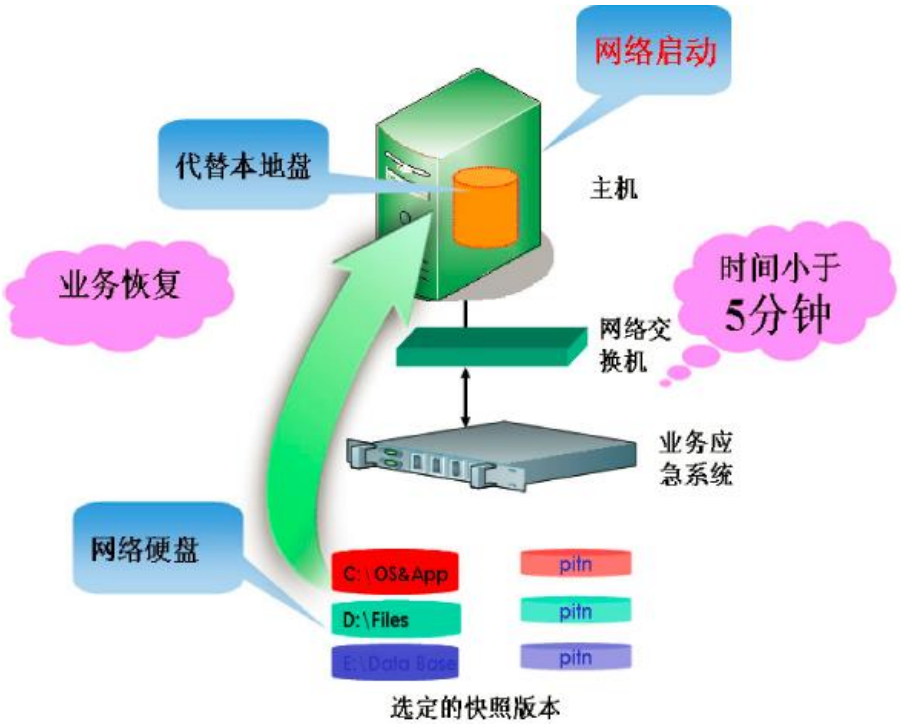
“业务应急系统”的软件自动扫描各服务器的本地磁盘信息（如 C、D、E 等及其各盘大小），然后对应每台服务器的磁盘在网络存储上为其分配相应的空

间。

根据预先设定的规则，“业务应急系统”自动对各服务器的操作系统、应用软件、数据及数据库实施动态差异量复制，并形成多版本镜像数据，供恢复时选用。

业务系统应急阶段

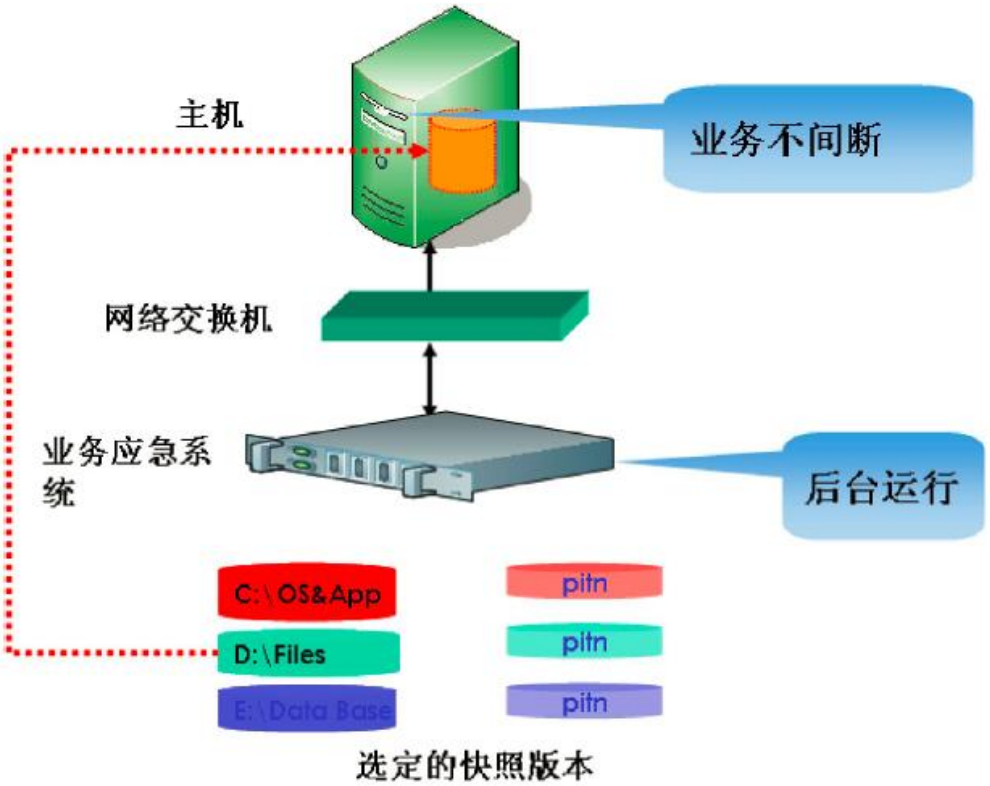
业务系统中断时，由业务应急系统接替业务主机的硬盘并启动，恢复业务系统的运行。工作过程如下图所示：



当业务系统出现中断时，将业务主机网络启动操作系统、应用软件，并使用原有的复制的数据，数据库数据；由于在网络存储里保存着可用的操作系统、应用软件、数据及数据库等多版本镜像，因此可在数分钟内由网络启动来恢复 多台服务器的运营，屏蔽各服务器本地盘的故障与问题。

若所选择的某时刻的文件、备份数据有问题，则可通过回滚到其他不同时 刻的版本而快速恢复到可用数据状态。

原业务系统的后台恢复过程，如下图所示：



当实施网络启动操作系统、应用软件并恢复业务运营后，可在系统 I/O 比较少的时间（如深夜），使用“业务应急系统”的恢复功能，对各服务器原有 的磁盘进行恢复操作；将存放在网络存储里的可用的操作系统、应用软件、数据及数据库恢复（回写）到本地盘，该操作支持对数十台服务器的自动恢复，非常便于运营管理。

当完成对本地盘的全部系统和数据的恢复后，根据需要，只需重启系统，并选择本地启动即可将运营切换到本地盘上。

2.3 规格型号

业务应急系统为软硬件一体化产品，主要规格：

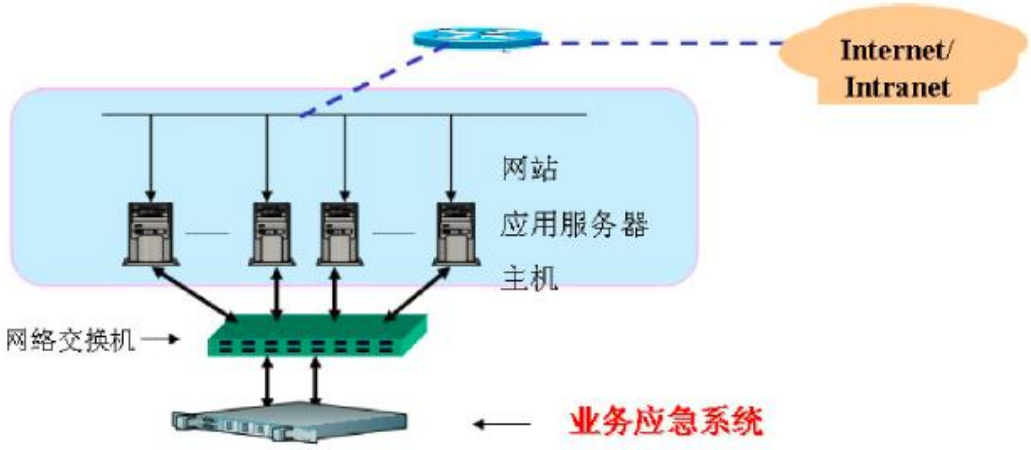
- 标准 19 英寸机架式设备；
- 高度：2U；
- 电源：AC220V，550W；
- 网卡：2 个 1000Base-T；
- 内置存储：4TB～16TB（可选）；
- 存储支持：Raid 0、1、5、6；

- 存储扩展：可选配 SCSI 或 FC 外置存储系统，需选配相应扩展卡；
- 支持的协议： iSCSI、 iSCSI Boot、sBoot、 sPXE；
- 支持的系统： Microsoft Windows 全系列、Red Hat Enterprise Linux 4.5 以上；
- 管理： Web UI；
- 应急启动方式：PXE、iSCSI HBA；
- RTO：约 5 分钟（主机启动时间）；
- RPO：最小 10 分钟（视数据量而定）；
- 跨网段部署：可选配启动器。

2.4 部署方式

业务应急系统可不改变用户现有网络结构，直接接入现有的网络，如被保护的主机不在同一个冲突域，每增加一个网段需另配一台启动器，或使用 iSCSI HBA 方式部署。

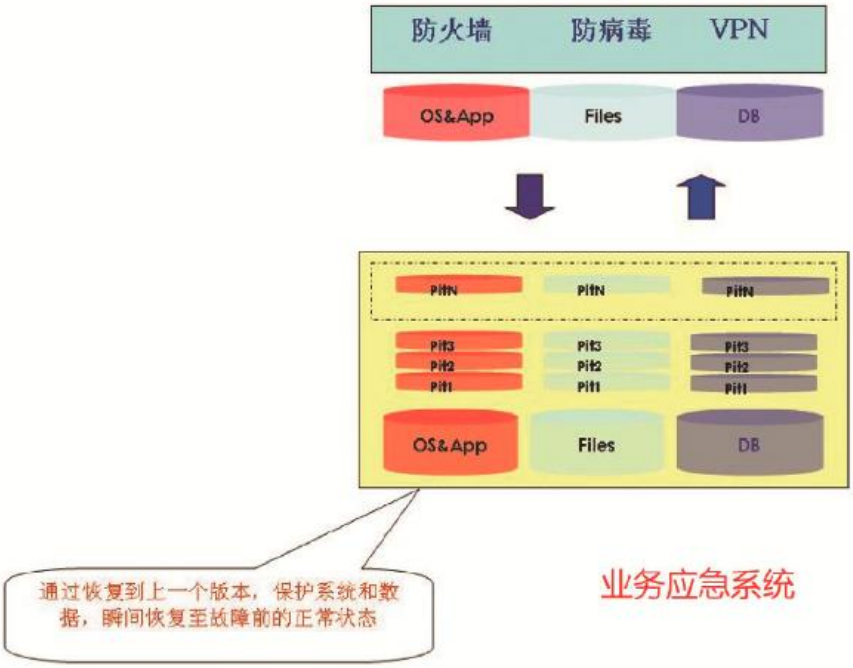
为降低对业务网络的影响，推荐组建业务应急专网。部署方式如下图所示：



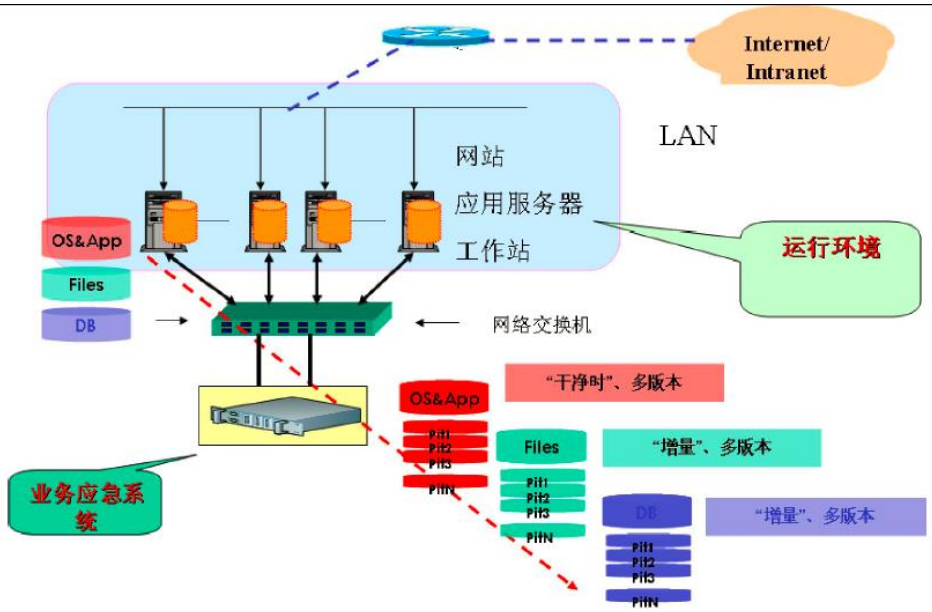
2.5 自身安全

业务应急系统本身系业务连续性保护产品，突破了传统数据保护仅仅对文件及数据库的保护，通过对操作系统、应用软件、数据库、数据文件进行复制，实现了对系统的 全方位的保护，使得信息系统能够在遭到破坏时，利用其“多版本回滚”技术，使系统 迅速恢复到故障前的正常运行状态。

“业务应急系统”并非传统意义上的安全产品(如:防火墙、防病毒、VPN 等),其实质是利用数据保护技术,丰富和完善了现有的安全防护体系,提高了系统的可用性。“业务应急系统”不是传统安全产品的替代品,而是作为数据安全体系的补充和扩展。



“业务应急系统”可抗拒任何病毒和攻击,可有效保护系统、环境和数据 。基于 IP SAN 的集中存储;成本低、容量大,扩展容易。支持 RAID 方式的数据保护,轻松 地使系统实现高可用;大幅度提高系统和数据的安全性和可用性。



“业务应急系统”中保存的“可用的操作系统及环境”为只读的，因此无病毒感染的可能，能保持该系统处于“可用”的状态。

“业务应急系统”中定时周期性地做数据增量复制而保存的部分，虽可能染上难以查杀的未知病毒，但是任何病毒必须运行在相应的“操作系统和环境”下，才能起作用，“业务应急系统”自身为“非 Windows”环境，任何隐藏的病毒均无法发作；其次，利用“业务应急系统”保存多版本快照的特点，实施“回滚”到干净的、无污染的版本，亦避开了病毒。

3 技术特点

3.1 全中文管理界面

业务应急系统的管理，采用中文 Web 操作模式，非常方便与简单，易手管理与操作。

业务应急系统客户端系统采用纯软件形式，易于安装，对客户端运行无明显影响。

3.2 在线系统和数据的多时间点/多版本复制

在线复制：在设定的时间，以变化量的方式式、对指定文件目录进行在线复制， 复制时不影响主机业务的运行。

- 在业务应急系统对应分配的卷空间上，对复制的数据产生快照（Snapshot）：
- 设定快照的时间间隔；
- 按时间片进行快照；
- 形成多版本；
- 可对任何制定的目录实施上述处理（如：D：SQLServer）。

3.3 对多台服务器实施网络启动

- 通过网络启动，可在几分钟内使多台主机恢复至故障前的正常运行状态。
- 当主机系统受病毒或其他因素影响出现问题时；
- 进行网络启动，引导运行保存在业务应急系统内的操作系统、应用软件，并使用原有复制的文件数据、数据库数据；
- 多版本回滚：若所选择的某时刻的数据有问题，则可通过回滚到其他不同时刻的版本，快速恢复到可用状态。

3.4 系统及数据即时迁移

当被保护的主机发生硬件损毁，如主板、CPU、电源、内存、网卡等，业务应急系统支持被保护主机系统及数据的即时迁移，即使用一台架构相同新的机器，通过网络启 动模式，快速恢复运营，并进行系统及数据恢复。

3.5 多版本及多系统保护支持

支持 Windows XP、Windows 2003、Windows 2000、Windows 2008、Windows Vista、Windows 7 等全系列 Microsoft Windows 系统及 Red Hat Enterprise Linux 4.5 以上版本平台的主机保护。

3.6 完善的病毒防护体系

业务应急系统可抗拒任何病毒和攻击，可有效保护系统、环境和数据。

- 业务应急系统中保存的“可用的操作系统和环境”是只读的，因此无病毒感染的可能，能保持该系统处于“无污染”的干净状态，因此利用业务应急系统重 新启动运行时，系统处于“无污染”的干净状态。
- 业务应急系统中定时周期性地做数据增量复制而保存的部分，虽可能染上难以 查杀的未知病毒，但第一，任何病毒必须运行在相应的“操作系统和环境”下， 才能起作用，业务应急系统自身为“非 Windows”环境，任何隐藏的病毒均无 法发作；其次，利用业务应急系统保存多版本数据的特点，实施“回滚”到干 净的、无污染的版本，亦避开了病毒。

3.7 防网络攻击能力

业务应急系统采用专用的操作系统，只提供了与客户机通信、业务应急有关的端口和服务，对于网络中其它机器而言就是一个黑盒子，网络抗攻击能力很强。

3.8 RAID 功能支持

业务应急系统的内置支持 RAID0、1、5，存储系统具有较高的可用性；大幅度提高系统和数据的安全性和可用性。

4 产品定位

4.1 业务连续性保障工具

通过部署业务应急系统，可在业务系统发生中断时，通过应急启动的方式快速恢复业务的运行，缩短停机时间，提高业务系统的可用性。

4.2 灾难恢复演练工具

灾难恢复演练作为业务连续性管理的一个重要环节，通常具有操作复杂、资源占用较大的问题，成功进行一次演练的难度很高。

使用业务应急系统，可以大大降低演练的技术难度，只需要部署一个简单的演练环境，就可以使用业务应急系统中备用机授权的功能，很少的时间就可以将所有的业务系统运行起来，从而实现检验容灾备份的可用性、灾难恢复应急预案

的可执行性等演练目的。

4.3 运维工具

业务应急系统具备的自动多主机在线复制、镜像的功能，可以降低系统运维人员在备份、备份介质管理等相关的维护难度，降低工作强度。

4.4 系统升级保障工具

在进行业务系统升级、补丁修补等操作时，可以利用业务应急系统的多版本回滚功能，当升级出现问题时，快速地将业务系统恢复到升级前的版本，避免因升级而造成的长时间业务停顿，有效降低业务系统升级的风险。

Copyright @ 2015 金品高端版权所有。

如果您想进一步了解金品业务应急系统，请来电或者发邮件咨询北京金品高端科技有限公司， 我们将协助您构建最适合贵公司的应用系统。

北京高端科技有限公司确认本出版物中信息其发行到目前为止是准确的。本出版物可能包含技术错误或印刷错误，这些信息无需告知即可进行修改。相关更改将定期增加到文中另行发表。金品公司可能在任何时候对本出版物中提及的产品和程序进行改进或变化。 未经金品公司的许可，禁止任何企业及个人复制本出版物。本出版物中的信息按其原样提供，金品公司对于文中的信息不提供任何保证，并明确拒绝特殊目的的暗示性商业性保证。

“JINPIN”是北京金品高端科技有限公司的注册商标。 关于金品公司更多的信息，请访问 www.scsi.cn

地址：北京市海淀区海淀大街 38 号银科大厦 812 室

联系人：肖海文

电话：010-82603525

传真：010—82603525-225

手机：18911787979　13910781139

E-mail：　xhw@scsi.cn