

上海证券交易所的运行安全 保障与应急处理工作介绍

白硕

上海证券交易所

2005年3月

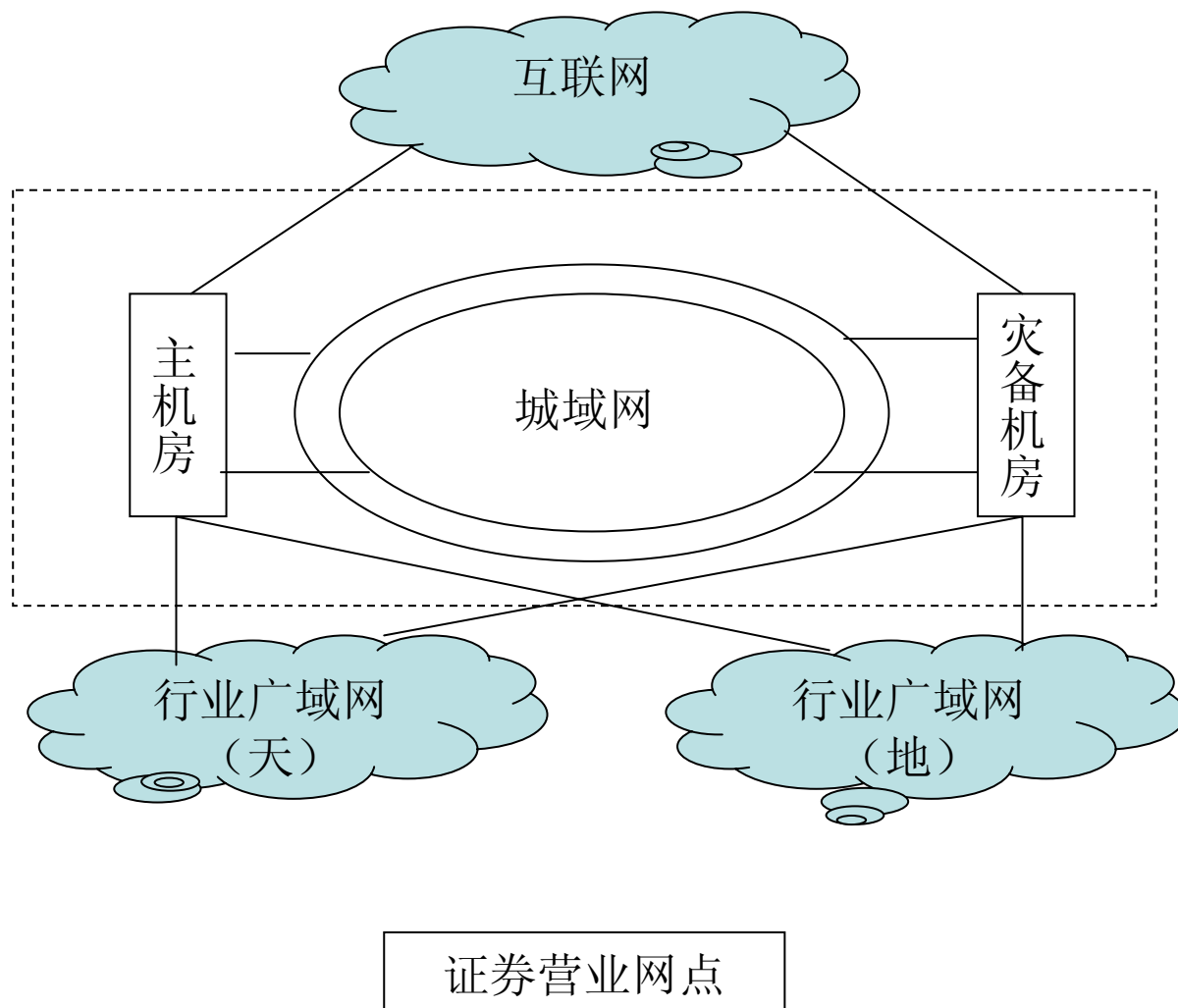
上海证券交易所简介

- 上海证券市场，简称“沪市”，中国证券行业主板市场
 - 800多只股票
 - 3000余万投资者账户
 - 通过天地双链路连接近3000个营业网点
- 从1990年恢复设立时起就实行了无纸化电子交易，核心交易系统采用集中式竞价撮合系统，各项业务信息化程度普遍很高，信息安全与运行安全保障几乎是同义词
- 交易日9:30-11:30, 13:00-15:00为交易时段，相应的系统具有非常高的运行安全保障要求，是Mission Critical

技术系统与技术基础设施

- 交易系统
- 监察系统
- 信息系统
 - 含数据仓库、业务管理、办公支持、周边辅助系统
- 通信系统
- 动力系统
 - 含多路不间断电源、恒温恒湿环境
- 机房
 - 主机房、灾难备份机房、远程数据备份机房

互联架构



周边系统

- 外部交易所（深交所）
- 登记结算系统
- 券商柜台系统
- 市场资讯系统（行情分析软件）

上海证券交易所的运行安全保障体系

- 组织
- 制度
- 基础设施
- 外部环境

组织

- 一把手负责
- 专职运行安全主管（总工程师）
- 专职运行安全队伍（技术中心）
- 全员参与

制度

- 问责与制衡
- 安全规章
- 应急预案与业务连续性预案
- 设备生命期管理
- 监督检查
- 论证
- 分级
- 培训与演练
- 良好的习惯

规章类别

- 方针类（目标、职责、奖惩等）
- 操作类（常规操作、应急操作、报告）
- 控制类（权限设置、口令更换、门禁等）
- 监视类（网络设备、应用系统、场地等）
- 分级类（重要性级别/可用性级别/密级等）
-

基础设施

- 隔离
- 加固
- 监控
- 加密与身份认证
- 权限控制
- 留痕与取证
- 备份
- 知识管理
- 物理安全
- 外来人员
- 介质
- 移动设备

隔离

- 几次较大的安全事件均与隔离不当有关
- 下决心解决隔离问题
- 正在实施的隔离方案：**8网分离**
 - 涉密网
 - 交易网、测试网、开发网
 - 业务内网、业务外网
 - 办公内网、办公外网

加固

- 迅速响应外界的病毒疫情通报
- 下载最新补丁
- 打补丁梯次进行，先外围，后核心

监控

- 已对核心交易网部署网络监控系统
- 监视对象包括
 - 网络设备
 - 主机
 - 应用
- 正在开发的新一代交易系统，在开发阶段就预留监控探针

加密与身份认证

- 证券“龙虎榜”及其覆灭
- 交易所网上业务
 - 会员公司业务
 - 上市公司业务
 - 大宗交易业务
 - 网上投票业务
 - 有偿信息服务业务
- **CnSCA**及其服务

权限控制

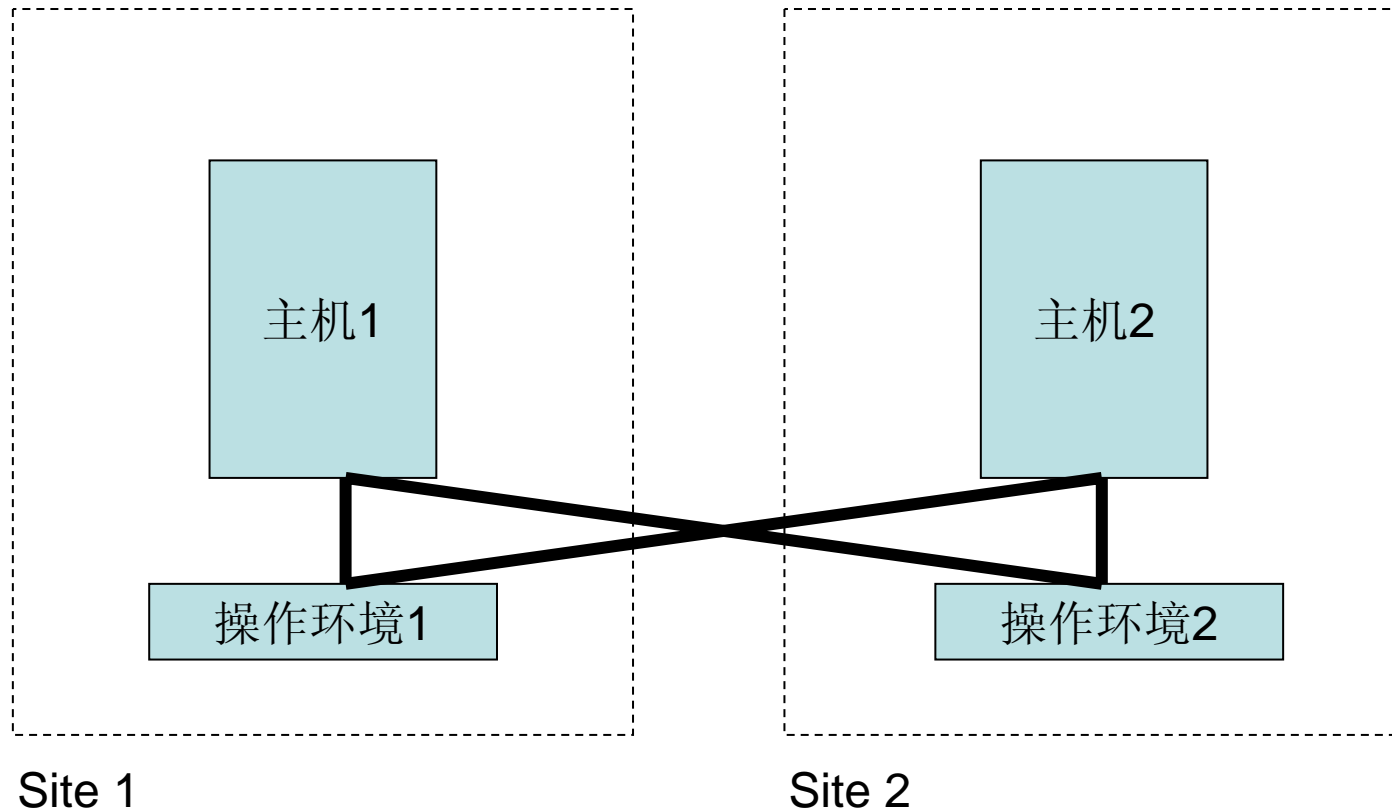
- 交易系统
- 业务管理系统//数据仓库
- 数据管理办法

留痕与取证

- 历史教训
- 留痕——硬拷贝（现有交易系统）
- 留痕——基于消息的网络存储（新一代交易系统）
- 留痕与系统安全的关系——松耦合

备份

- 数据：本地实时备份，远程在线/离线互备
- 交易系统：主机/操作环境全对称交叉互备



知识管理

- 建立并维护详尽的安全事件档案
- 建立并维护详尽的设备档案
- 建立市场**FAQ**，供专职的技术咨询电话接听人员查询解答
-

外部环境

- 法律法规（项目建设中的法律符合性）
- 标准（互操作、安全管理标准等）
- 认证认可体系（测评、资质）
- 信息通报与共享（证监会/上海市/**CERT**）
- 社会化网络信息安全服务（中科网威、启明星辰）
-

应急工作（1）

- 实行总工程师负责制
- 敏感时期启动特别保障制度
 - 巡视加倍，报警阈值降低，停止施工，设备供应商支持人员到场，信息报送等
- 实行二级响应机制
 - 一级：运行支持人员负责发现异常、进行日常响应维护（巡视、监控）
 - 二级：资深技术人员（软件、网络）负责响应较深层次的异常

应急工作（2）

- 处置原则
 - 预防为主
 - 勤于演练
 - 恢复优先
 - 保存证据
 - 一查到底
 - 适当避嫌

应急工作（3）

- 几个典型案例
 - 广播风暴——交换机故障及其处置
 - 错位的行情——通信网关故障及其处置
 - 小设备大麻烦——行情故障及其处置

谢谢各位的分享，请
发送邮件到

sbai@sse.com.cn

与我联系