<http://blog.sina.com.cn/s/blog_4b14a8c201019vxi.html>

今天社会的各行各业对信息系统的依赖与日俱增，特别是在金融等行业信息系统已经真正到须臾不可离异的地步。对于这样的大型企业，信息系统的重要性决定了对其可靠性、安全性的要求达到了前所未有的高度。作为提高可靠性、安全性的一个重要措施，投资巨大的灾备中心建设已经不再是满足某一企业的自身安全要求，而是成为行业的硬性规定。然而，影响信息系统可靠性、安全性的因素涉及的方面、因素非常多，并不是只要建立了灾备中心就可以一劳永逸地彻底解决问题。本文希望从多个角度探讨通过减少单点故障提高信息系统的安全性。

 今天信息系统的复杂性决定了完成一个看似简单的业务操作都需要一个长长的信息系统链条的各个环节提供保障。在这个链条中的任何一个环节出现问题，都将导致业务操作的失败。金融行业信息系统一般都是由数据中心、广域网、局域网、应用终端为基础，在其上建立的应用系统，以及维护基础平台和应用平台的组织构成。因此，无单点故障就在保证上述所有的环节都要实现无单点故障。

 本文讨论的无单点故障并不包括个人应用或几人以下的小团队的无单点故障问题。实现无单点故障需要巨大的成本投入，任何可靠性方面的提高都意味着投入的增加，因此无单点故障设计只是在考虑可能对全局或相对较大的区域造成影响的信息系统需要进行无单点故障设计。

**一、数据中心的无单点故障设计**

**1、  服务器的无单点故障设计**

 现今稍正规的数据中心服务器一般都会采用双机或集群设计，以保证当一台服务器出现故障时，重要的业务不会中断。但随着计算机应用深入到企业的各个方面，企业中都会有大量的系统在各个领域中运行，需要数量庞大的服务器支撑这些应用。相当一部分企业很难保证所有的服务器都能做到双机或者集群。而随着信息系统在企业中应用集成度的不断提高，各应用系统间的关系日益紧密，一个看似不重要的系统可能与核心系统密切相关，一般系统的故障可能直接导致关键系统无法正常运行。因此，在服务器的配置上，不但要考虑关键系统的无单点故障，对大量的非关键应用系统也同样需要考虑双机或集群，实现无单点故障设计，以全面保证企业的应用不会由于非核心系统的故障对核心系统造成影响。

 对于非核心业务的应用，并不一定都必须做到双机或集群，可以利用现已十分成熟的虚拟化技术，将一台服务器划分为多台，将大量的非关键应用系统交叉部署在不同的物理服务器上，彼此互备。根据各系统的重要性和相互的关联性，并考虑总体经济性，非核心服务器并不一定都必须是热备，有些服务器也可以是冷备，只要能在较短的时间内能及时启动，满足应用需求即可。

**2、  磁盘阵列的无单点故障设计**

 磁盘阵列本身就是一个相对高可靠性的设备，单个磁盘的故障并不会影响其上存储数据的安全性。先进的磁盘阵列可以通过配置双控制器实现控制器的无单点故障，但背板如果出现故障也将使整个磁盘阵列失效，尽管这个概率很低，风险也还是存在的。因此，如果条件允许，磁盘阵列也应该采用双机互备模式。

**3、  数据中心网络系统的无单点故障设计**

 一般的数据中心都已经采用双核心交换机模式实现无单点故障。但主交换机之外，防火墙、路由器是否存在双机互备，交换机与非核心服务器是否实现了双线接入都对整个系统的可靠性有重要影响。因此，在网络接入、防火墙、路由器、DMZ区设计等多个方面都需要考虑无单点故障设计。

**4、  灾备系统**

 灾备系统是确保系统可行性的最后一道屏障。但由于灾备系统投入使用的概率很低，相当一部分灾备系统并未达到理想的随时可以投入使用的状态。灾备中心除了服务器、网络平台要能承担得起主数据中心的关键任务外，不仅要实现与主数据中心各应用系统数据的一致性，应用程序更新版本的一致性，更重要的是灾备中心也需要建立与主数据中心同样能与各机构相连的网络，而不能只与主数据中心有顺畅的网络，因为一旦发生需要启用灾备中心的故障，与主数据中心的网络也会中断。

 为保证灾备系统能够在主数据中心出现灾难性故障时正常启用，一般的点对点方式的SDH专线很难做到各节点在灾备中心启动后，把应用自动切换到灾备中心。就是各节点都向两个数据中心铺设了专线，对于一个有大量节点的企业而言，切换也不是一个简单的问题。建立MPLS网络是解决快速切换的最佳方案，它可以在主数据中心出现故障时，自动切换到灾备中心，真正实现业务的不间断运行。

**二、网络系统的无单点故障设计**

**1、  广域网的无单点故障设计**

 今天建立广域网已经不存在任何技术障碍，可以通过SDH专线实现点对点互联，也可以建立MPLS VPN专网，还可以通过互连网VPN技术建立机构内部专网。尽管今天专线在技术上已经具备了相对较高的可靠性，但施工造成的断网是最常见的专线故障。因此，每个信息节点通过电信、联通两家公司分别建立专线是提高可靠性的有效方式。还可以通过SDH专线与互联网VPN互备实现无单点故障。

 为了防止两条专线被施工时同时挖断，条件允许时，应尽可能采用相隔较远的不同通道汇聚到机房。

**2、  节点内无单点故障设计**

 所谓节点就是一个与广域网相联的内部局域网系统。由于这些节点可能是几十人，也可能是由成百，甚至上千人的团队组成，还有些节点担负着承上启下的信息传输作用中，因此，为了将故障影响控制在最小范围内，节点内也应考虑无单点故障设计。

 节点实现无单点故障设计的要点一是要实现双线，或三线通过双路由器、双网关接入，配备两个三层交换机，即可实现节点的无单点故障设计，把单一设备或线路故障造成的影响降到最低。

**三、组织架构的无单点故障设计**

 无单点故障设计不但要考虑硬件和网络，在组织架构上也必须做充分的考虑。现今企业中的计算机平台日益复杂，应用系统五花八门，需要一个强大的技术团队做好维护工作。一旦维护出现问题，必将对业务经营产生重大影响。

 在组织架构上要做到无单点故障，就要求不管软件、硬件，每一个系统的维护都应有至少两个，或两组人员负责。许多企业通过服务外包的方式，将信息系统的维护交由专业的公司来做，但对于大型的企业自身也应有一批专业技术人员能够承担起各软硬件系统最基本的维护工作，只有这样才能保证一旦出现意外情况时，不会由于维护人员，或团队出现问题，造成系统的瘫痪。

 实现信息系统全部各关键环节的无单点故障需要巨大的资金投入，各企业必须根据自身的实力、信息系统在企业的重要性决定在哪些环节需要加强，哪些环节可以暂缓，在安全投入和获得的收益之间找到一个平衡点。