# 概要：

……

为了满足物流管理系统各个环节对可靠性的要求，我带领团队对系统的运行环境和特点进行分析，找出可能影响系统可靠性的原因，根据分析出的结果制定了提高系统可靠性的措施：一是应用架构设计风格和设计模式，降低软件系统的复杂度；二是采用数据校验容错（冗余）机制，保证数据的完整性和正确性；此文以物流系统为例，讨论可靠性分析与设计在该项目中的应用。最后，讨论该系统的想法与教训。

……

软件可靠性是软件质量中最为重要的一项属性。软件可靠性设计技术是确保和提高软件质量的重要手段。系统可靠性是系统在规定的时间内及规定的环境条件下完成功能的能力，也就是系统无故障运行的概率。这里的故障是系统行为与需求不符，故障有等级之分。系统的可靠性可以通过历史数据和开发数据直接测量和估算出来。在产品的设计过程中，为消除产品的潜在缺陷和薄弱环节，防止故障发生，以确保满足特定的固有可靠性要求所采取的技术活动。可靠性设计是实现产品固有可靠性要求的最关键的环节，是在可靠性分析的基础上通过制定和贯彻可靠性设计准则来实现的，可靠性设计在总体的设计中占有十分重要的位置，必须把可靠性工程的重点放在设计阶段，并遵循预防为主，早期投入，从头抓起的方针。尽可靠把不可靠的因素消除在产品设计过程的早期。可靠性设计的目的是综合考虑产品的性能，可靠性，费用和设计等因素的基础上，通过采用相应可靠性设计技术，使产品的寿命周期内符合所规定的可靠性要求。

在Q系统中，物流的各个环节都要高要求的保证其可靠性，订单管理，物料需求，物流监控等等。经过我们的分析，从产品的性能，可靠性等同时出发，在以下几个方面对可靠性进行设计。

1. 物料审批中的防卫式设计。

当合作商提供物料后，公司需要物料进行校验审批。审批通过才可进行订购。审批模块是一个独立的构建，负责将请求来源模块提交的审批请求提交到后台的数据库系统。提供展示页面及页面给主管审批时参考，记录审批结果，并将审批结果反馈这个环节考虑到请求来源可能出现临时性故障。比如数据库锁，通信终端，模块代码更新异常等导致审批模块已经完成。而来源模块没有接收到审批结果的情况。所以针对此问题，我们做了一个防卫式设计。

2.公共池流程的防卫式设计

在公共池模块中，有一场景是运输部门朱门在查看下属公共池领养情况时，可以将一个运输团队已经领养的运输机会重新指派给另一个运输团队。我们的设计：先让运输团队自动执行弃养过程，再新新执行自动弃养，这里就有风险，就是在旧成员弃养成功后，新团队因为各种原因无法领养，导致领养不成功，所以我们在这也做了一个防卫式设计。

在这里，在新团队领养后，判断是否领养成功。如果不成功，则将该运输机会让原团队领养。避免……

3.数据处理模块中N版本程序设计。

DRS系统中有很多地方需要与外部系统做数据同步，比如，物料存储情况需要从MRPS系统传递到DRS系统做物料分销展示。N系统是我们公司独立分布在各地仓库的管理系统。各地的数据库属于异地数据库，不能用常规的事务处理方式保证数据一致性与完整性。我们需要统计到主服务并计量。

我们通过分析设计，首先借用透明网关从服务器建立一个DBLink到主数据库，然后在从数据库端建立一个定期执行的统计过程，在这个过程中，我们为保证计算过程正确性从而统计到主服务器，我们采用N版本程序设计，我们共同开发各个不同版本，各自从数据库统计计量后，各自验证正确，通过表决器比较3个版本执行结果，采用少数服从多数原则，这样可以将某个偶然出现的错误屏蔽掉，但这样的代价也很高，项目人员、开发资金等，但考虑到其统计计数巨为重要性，我们依然采用N版本程序设计开发。事实证明，采用N版本系统稳定性精确性更高。