18. 支付宝打8折P0资损：再论防呆设计的重要性

大家好，我是隐墨星辰，专注境内/跨境支付架构设计十余年。今天聊聊支付宝昨天的P0资损故障，除了看热闹，也尝试聊聊资损防控中的“防呆设计”。

2025年1月16日下午14:40至14:45，支付宝平台出现重大故障。在这短短5分钟内，用户在进行个人转账、信用卡支付、缴费等操作时，订单支付页面均弹出“政府补贴”提示，直接享受到了20%的减免优惠。

关于支付宝是否补扣用户的钱，网友各种意见都有。我个人的观点：如果支付宝要扣，一定是在法律框架允许的情况下扣回，当然这不可避免带来网友们的口诛笔伐。如果不扣，也有很多先例，包括多多，企鹅等都曾出现过类似的事件，就直接送给用户。

关于可能的原因，比较多的猜测，是测试环境配置问题：技术团队在进行国补测试时，没有完全隔离测试环境和实际交易环境，导致测试数据误操作进入了真实交易环节，从而出现全平台的减免现象。同时也暴露出审核机制不完善，缺乏自动熔断机制等不足的地方。

凭心而论，支付宝处理的速度还是很快的，奈何交易量实在太大，才导致影响这么大。

除了吃瓜，做为一个支付人，我们当然还要想想自己：换成是我，我怎么做？大部分人想的大概就是环境隔离、流程规范、强化审核制度、加强培训等。

还有其它的吗？有的。

我以前写过一篇“在支付系统中实施防呆设计的实践”，也是类似在测试环境调用了外部渠道的生产环境，出现资损。

什么是防呆设计?

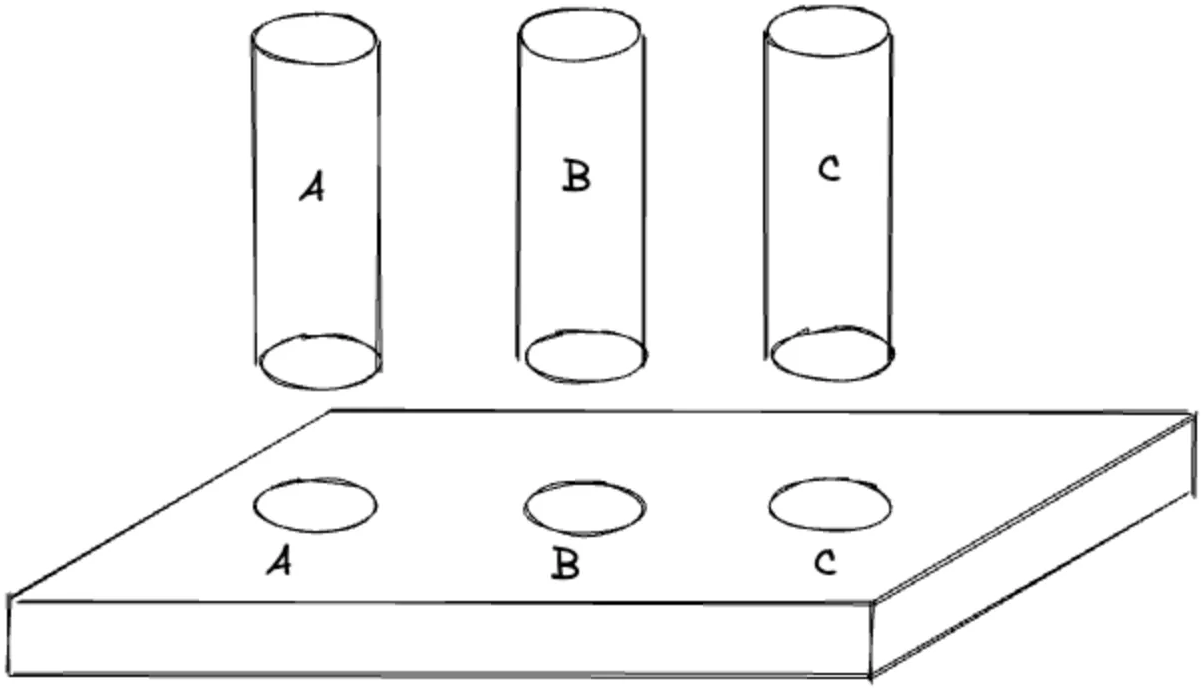
“防呆设计”（日语：ポカヨケ poka yoke）是一种预防性设计策略，目的是通过限制方法减少错误的发生。用户在无需额外注意力、经验或专业知识的情况下，也能准确无误地完成操作。

这个概念起源于日本，被广泛应用于丰田汽车的生产过程中，随着时间的推移，已成为全球范围内广泛采用的设计策略。

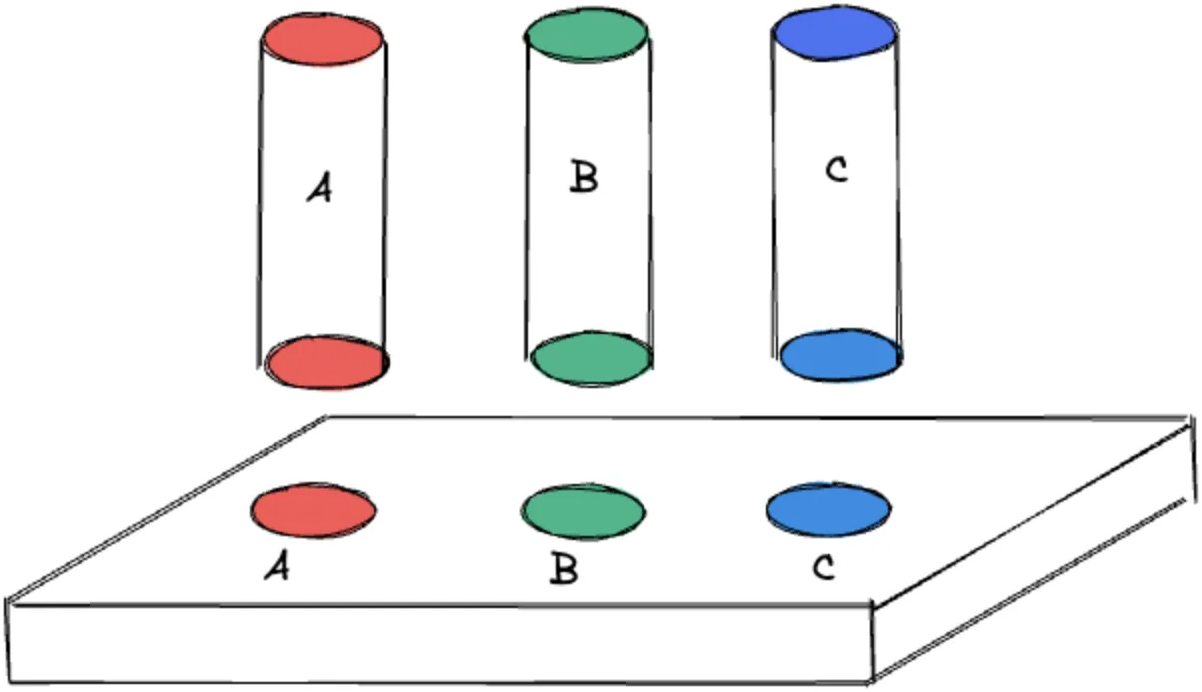
在工业设计中，防呆设计的例子比比皆是。例如，USB接口的设计确保了只有正确方向才能插入，而Type-C接口则进一步简化，支持双面插入。

下面是一个极简化的例子。

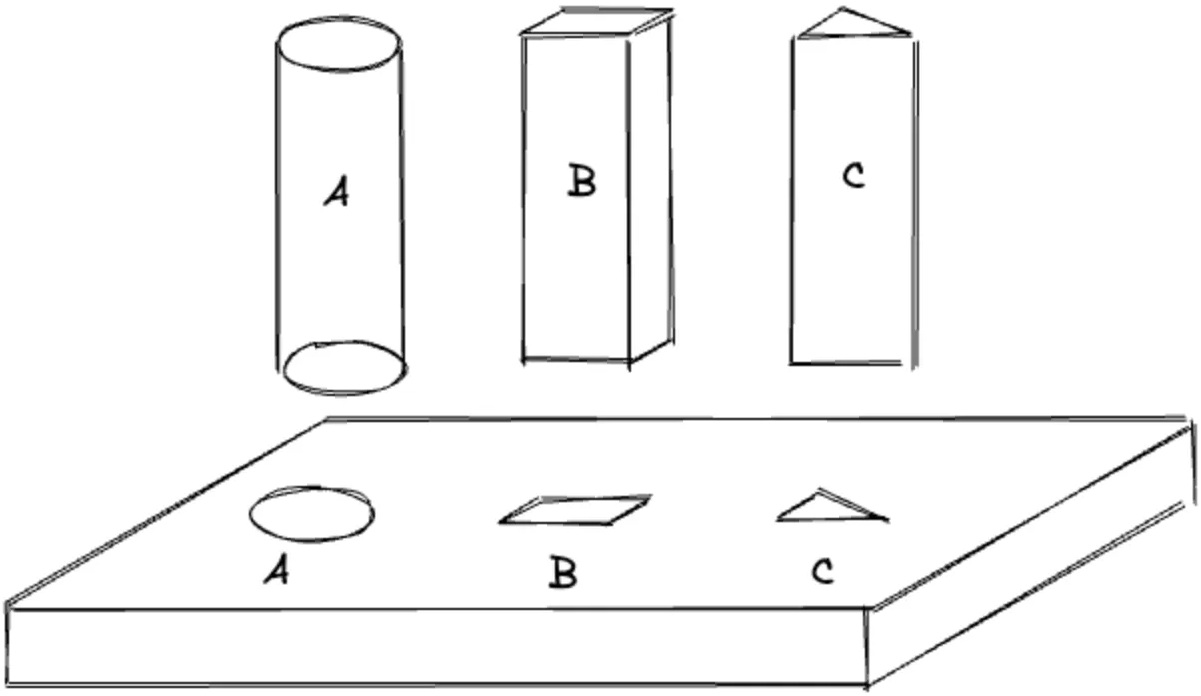
第一版：使用字母标识，容易出错。



第二版：使用颜色标识，减少出错。



第三版（防呆）：不同形状只能插到不同的位置，想错都错不了。



回到这个故障本身，具体怎么做呢？有下面几点供参考：

1. **环境隔离。**在测试环境和正式环境之间设置严格的隔离机制，像采用不同的网络配置、数据库连接等，就可以有效防止测试参数误传入正式环境，从而避免此类配置错误引发的故障。
2. **自动熔断机制。**所有的营销资金池强制设置最大金额，当补贴额度超出预设范围等情况时，自

动熔断机制能够及时切断错误的交易流程，防止问题进一步扩大，避免给用户和平台带来更大的损失。

3. **系统默认兜底检查不符合常理或明显高风险的操作或配置。**比如营销或补贴一定是有指定条件的，这次故障出现全类型可用。包括以前多多的故障，本来是拉新的，结果是全部用户可用。以前我们还出现过，客资手动重复上传两份一样的结算单，审核也通过，导致重复结算，而同一天同一个商户结算相同金额，明显也不符合常理。

从业多年，见过太多的线上故障，得到一个朴素的道理：“**人都是不可靠的，所以加再多的审批也是不可靠的，一定要想办法不要依赖人或流程来解决。**”多引入一些防呆设计，让再“呆笨”的人都没有出错的可能性，那么系统就是健壮的，也就没有那么多的线上应急和复盘。

阿里系最近几年时常在风口浪尖上，但抛开情绪，支付宝仍然人才济济，技术仍然领先，内部的流程体系也仍然是完备的，不能因为几次故障就完全否定。

每一次故障，背后都是一些鲜活生命高强度承压下的应急处理。还是希望大家少点故障，开心过个年。