极客时间 训练营

架构实战营模块7

第2课：如何用 FMEA 方法排除架构隐患？

李运华

前阿里资深技术专家（P9）

教学目标

极客时间 训练营

1. 掌握 FMEA 方法的基本概念
2. 掌握 FMEA 的技巧和应用

凡事预则立不预则废！

目录

1. FMEA 介绍

FMEA 介绍

极客时间 训练营

定义

FMEA（Failure mode and effects analysis，故障模式与影响分析）又称为失效模式与后果分析、失效模式与效应分析、故障模式与后果分析等，专栏采用“故障模式与影响分析”。

历史

FMEA 最早是在美国军方开始应用的，20世纪40年代后期，美国空军正式采用了 FMEA。

二十世纪60年代，在开发出将宇航员送上月球并安全返回地球的手段的同时，FMEA 得到了初步的推动和发展。

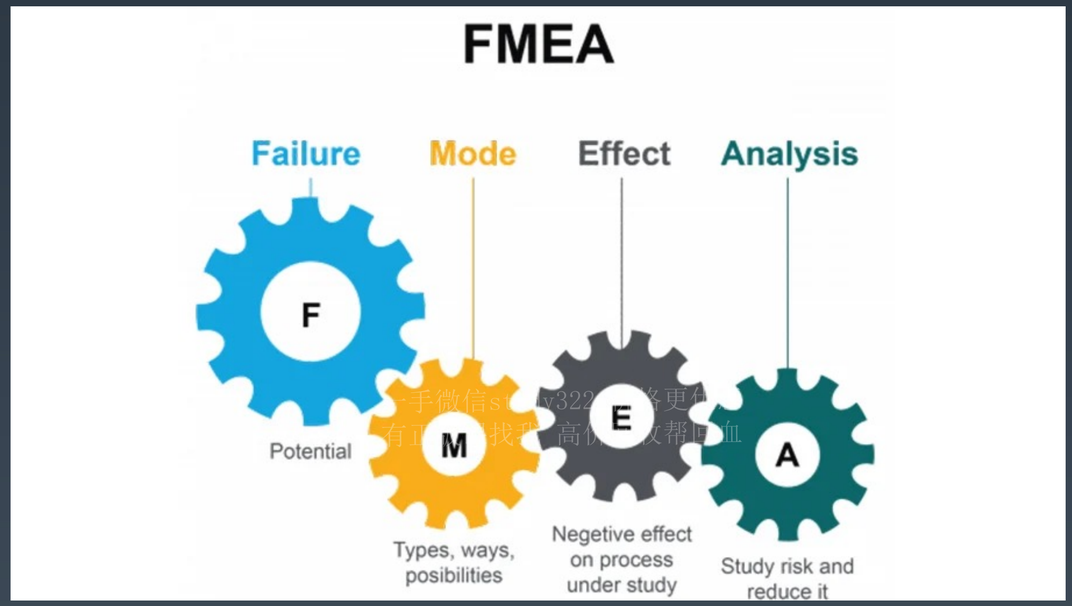
二十世纪70年代后期，福特汽车公司在平托事件之后，出于安全和法规方面的考虑，在汽车行业采用了 FMEA。

作用

FMEA 之所以能够在这些差异很大的领域都得到应用，根本原因在于 FMEA 是一套分析和思考的方法，而不是某个领域的技能或者工具。

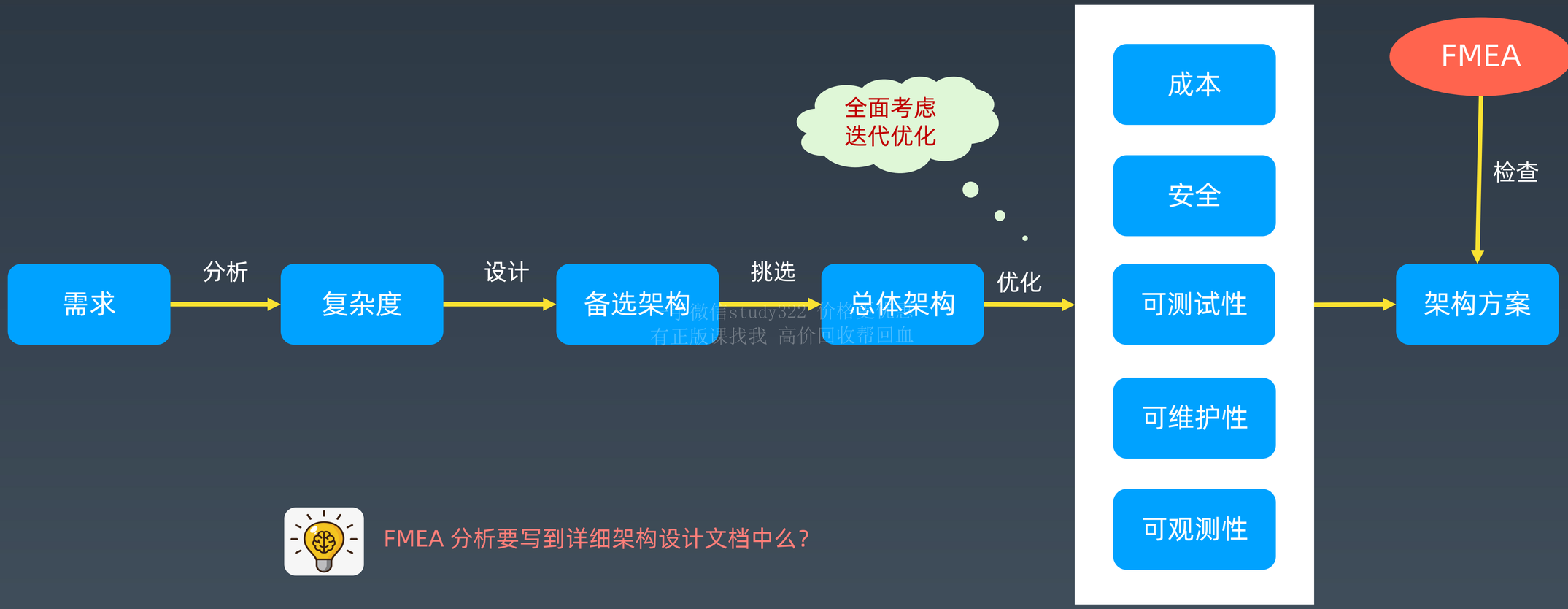
FMEA 并不能指导我们如何做架构设计，而是当我们设计出一个架构后，再使用 FMEA 对这个架构进行分析，看看架构是否还存在某些可用性的隐患。

FMEA 详解



Failure：假设系统某些组件或者模块出现故障。
Mode： 故障发生的方式、可能性。
Effect ： 故障的影响。
Analysis：分析系统的可能反应，以及如何改进。

FMEA 什么阶段应用？



FMEA 分析要写到详细架构设计文档中么？

案例 - 电子门锁 FMEA 分析

极客时间 训练营

【Failure】
电子门锁的控制器坏了。

【Mode】
软件故障，可能性不确定。

【Effect】
打不开门，进不了家。

【Analysis】
1. 控制器坏了，系统没有任何方法进行处理；
2. 可以使用钥匙开门，然后复位控制器。

【Failure】
电子门锁的控制器没电了。

【Mode】
电池耗尽，可能每三个月一次。

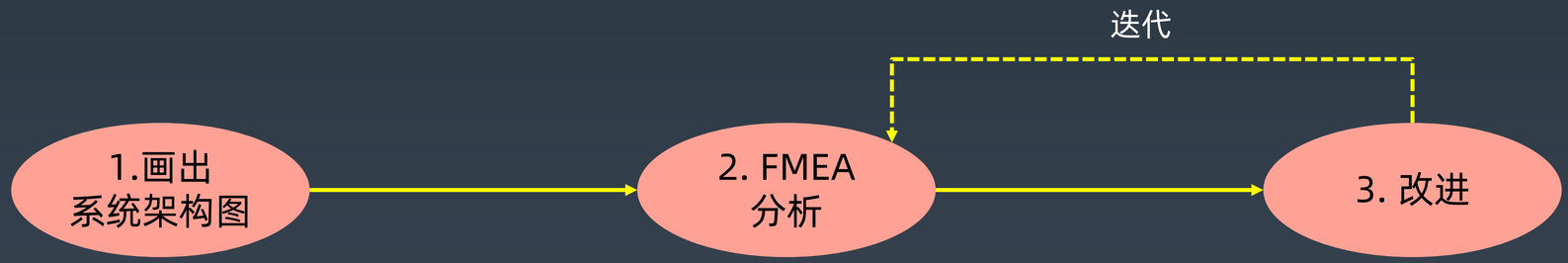
【Effect】
打不开门，进不了家。

【Analysis】
1. 没电了，系统没有任何方法进行处理；
2. 可以使用钥匙开门，然后更换电池。

都用电子锁了，为何还要求用户带钥匙？

2. FMEA 技巧

FMEA 应用步骤



1. 给出初始的架构设计图，一般是系统架构图和部署架构图；
2. 假设架构中某个 Role 发生故障，然后分析此故障对系统功能造成的影响；
3. 根据分析结果，判断架构是否需要进行优化。

客户端和前端需要用应用 FMEA 来优化架构么？

FMEA 分析维度

极客时间 训练营

业务功能	故障模式	故障影响	严重程度	故障原因	故障概率	风险程度	已有措施	规避措施	解决措施	后续规划
FMEA 分析涉及的功能点。	系统可能会出现什么样的故障。	当发生故障模式中描述的故障时，业务功能具体会受到什么影响。	故障对业务的影响程度。	导致故障现象发生的原因，不同原因可能导致相同现象。	某个具体故障原因发生的概率。	综合严重程度和故障概率来一起判断某个故障的最终等级。	针对具体的故障原因，系统现在是否提供了某些措施应对。	为了降低故障发生概率或者故障影响采取的一些措施。	解决措施是指为了解决问题而做的一些事情。	系统的后续改进规划。

不需要死记硬背这11个维度，需要的时候对照模板就可以了！

FMEA 技巧详解1

极客时间 训练营

业务功能

用户角度划分的业务相关的功能点。

从用户角度而不是系统角度。

例如：对于一个用户管理系统，使用 FMEA 分析时 “登录” “注册”才是功能点，而用户管理系统中的数据库存储功能、Redis缓存功能不能作为FMEA分析的功能点。

故障模式

系统会出现什么样的故障，包括故障点和故障形式。

故障模式并不需要给出真正的故障原因，只需要假设出现某种故障现象即可。

故障模式的描述要尽量精确，多使用量化描述，避免使用泛化的描述。例如，推荐使用“MySQL响应时间达到3秒”，而不是“MySQL响应慢”。

故障影响

故障发生后业务功能具体会受到什么影响。

常见的影响有：功能点偶尔不可用、功能点完全不可用、部分用户功能点不可用、功能点响应缓慢、功能点出错等。

故障影响也需要尽量准确描述。例如，推荐使用“20%的用户无法登录”，而不是“大部分用户无法登录”。

20%的用户无法登录还是21.25%的用户无法登录更好？

FMEA 技巧详解2 - 严重程度

极客时间 训练营

严重程度

从业务的角度看故障的影响程度。

1. 一般分为“致命/高/中/低/无”五个档次。

2. 严重程度按照这个公式进行评估：严重程度 = 功能点重要程度×故障影响范围×功能点受损程度。
例如：登录功能比修改用户资料要重要得多，80%的用户比20%的用户范围更大，完全无法登录比登录缓慢要更严重。

3. 团队讨论确定，包括业务、开发、运维等一起讨论，但是要避免业务方有意无意夸大严重程度。

4. 如果争执不下，架构师拍板。

如果架构师瞎拍怎么办？

FMEA 技巧详解3

极客时间 训练营

故障原因

导致故障现象出现的原因。

故障现象相同，对业务影响相同；故障原因不同，发生概率、检测手段、处理措施不同。

例如：
1. 发生概率：“MySQL bug”的概率要远远低于“没有索引”导致查询慢。
2. 检测手段：磁盘坏道导致 MySQL 响应慢和慢查询的检测手段不同。
3. 处理措施：磁盘坏道要换机器，慢查询要优化索引。

故障概率

某个具体故障原因发生的概率。

一般分为“高/中/低”三档即可，几个特别注意的现象：

1. 硬件

硬件随着使用时间推移，故障概率会越来越高。例如，新的硬盘和3年的硬盘。

2. 开源系统

成熟的开源系统 bug 率低，版本3.0比版本0.3要成熟；已经有使用经验和第一次使用。

3. 自研系统

和开源系统类似，成熟的自研系统故障概率会低，而新开发的系统故障概率会高。

风险程度

综合严重程度和故障概率来一起判断某个故障的最终等级。

风险程度 = 严重程度×故障概率。

某个故障影响非常严重，但其概率很低，最终来看风险程度就低。

例如：“某个机房业务瘫痪”对业务影响是致命的，但如果故障原因是“地震”，如果机房在广州概率就很低，如果机房在东京，概率就高很多。

如果业务方随意抬高故障影响的严重程度，会出现什么情况？

FMEA 技巧详解4

极客时间 训练营

已有措施

针对具体的故障原因，系统现在是否提供了某些措施来应对。

常见措施有：

1. 检测告警

检测故障并告警，系统自己不针对故障进行处理，需要人工干预。

2. 容错

检测到故障后，系统能够自行应对。例如，Hadoop 集群。

3. 自恢复

检测到故障后，系统能够自己恢复。例如，踢出故障的容器节点，创建新的容器。

规避措施

为了降低故障发生概率或者故障影响而采取的一些措施。

可以是技术手段，也可以是管理手段。

例如：

1. 技术手段：为了避免新引入的 MongoDB 丢失数据，在 MySQL 中冗余一份。
2. 管理手段：为了降低磁盘坏道的概率，强制统一更换服务时间超过2年的磁盘。

解决措施

为了能够解决问题而采取的一些措施。

一般都是技术手段。例如：

1. 为了解决密码暴力破解，增加密码重试次数限制。
2. 为了解决拖库导致数据泄露，将数据库中的敏感数据加密保存。
3. 为了解决非法访问，增加白名单控制。

如果某个故障既可以采取规避措施，又可以采取解决措施，优先选择解决措施

是否可以全部采取解决措施？

FMEA 技巧详解5 - 后续规划

极客时间 训练营

后续规划

针对 FMEA 分析表格，查漏补缺，优化系统架构。

具体步骤：
第一步：排序，按照风险程度的评估结果排序；
第二步：制定改进方案；
第三步：对改进后的方案重新应用 FMEA 评估。

技巧：
1. 技术手段、管理手段都可以；
2. 检测、规避、解决手段都可以；
3. 需要考虑成本。

例如：地震、敏感数据泄露、MongoDB 断电丢失数据，分别如何处理。

如果业务方或者老板瞎提要求，三个字：得加钱！

FMEA 落地技巧

极客时间 训练营

抓住核心

优先针对核心场景进行分析。

分工合作

可以安排给初级架构师或者高级开发人员，锻炼架构思维。

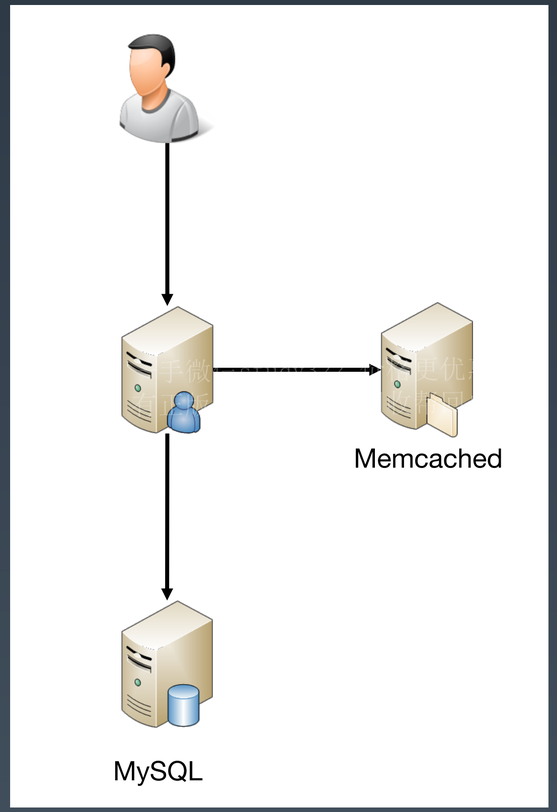
适可而止

严重程度为高的必须解决，严重程度为中的做好检测和告警。

如果遗漏评估某个点，导致线上严重事故怎么办？

3. FMEA 详细案例

FMEA 案例



FMEA 分析 - 登录

极客时间 训练营

功能点	故障模式	故障影响	严重程度	故障原因	故障概率	风险程度	已有措施	规避措施	解决措施	后续规划
登录	MySQL 无法访问	当 MC 中无缓存时，用户无法登录	高	MySQL 服务器断电	中	中	无	MC 缓存数据，登录时可以不访问 MySQL	无	增加 MySQL从机，从机支持读数据
登录	MySQL 无法访问	同上	高	Server 到 MySQL 网络中断	中	中	无	同上	无	MySQL 双网卡
登录	MySQL 响应时间超过 5s	当 MC 中无缓存时，用户登录很慢	中	MySQL 慢查询	中	低	无	同上	无	增加慢查询告警

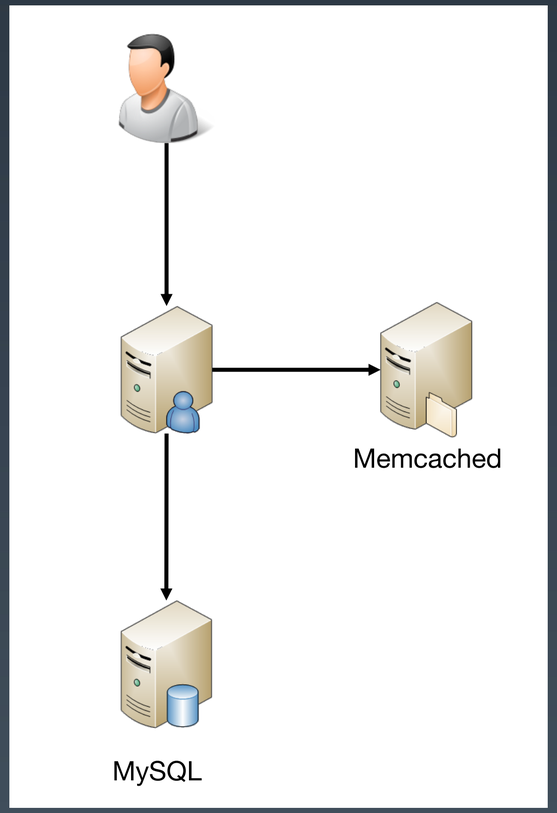
FMEA 分析 - 注册

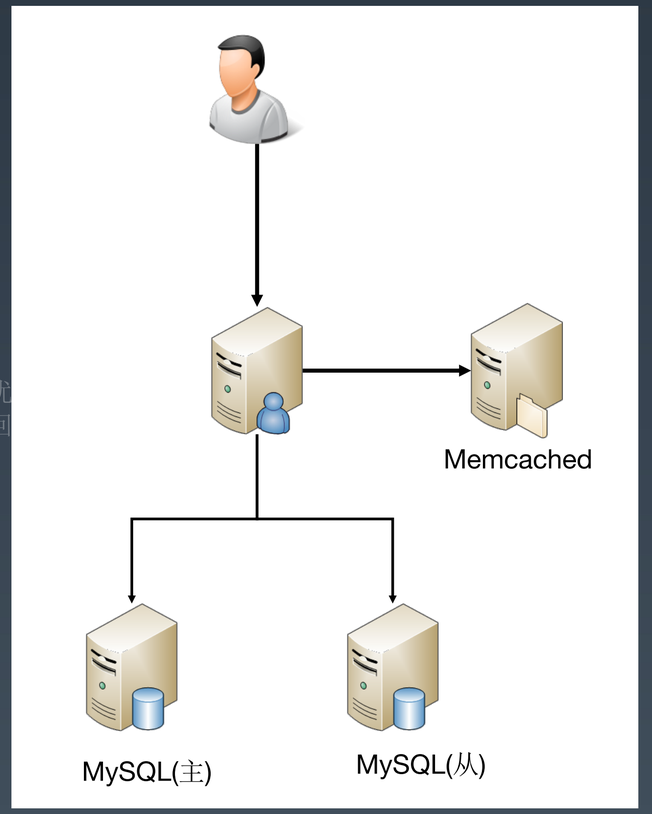
极客时间 训练营

功能点	故障模式	故障影响	严重程度	故障原因	故障概率	风险程度	已有措施	规避措施	解决措施	后续规划
注册	MySQL 无法访问	用户无法注册	中，每天注册人数并不多	MySQL 服务器断电	中	低	无	无	无	增加告警
注册	MySQL 无法访问	用户无法注册	同上	Server 到 MySQL 网络中断	中	低	无	无	无	增加告警
注册	MySQL 响应时间超过 5s	用户注册很慢	中	MySQL 慢查询	中	低	无	无	无	增加告警

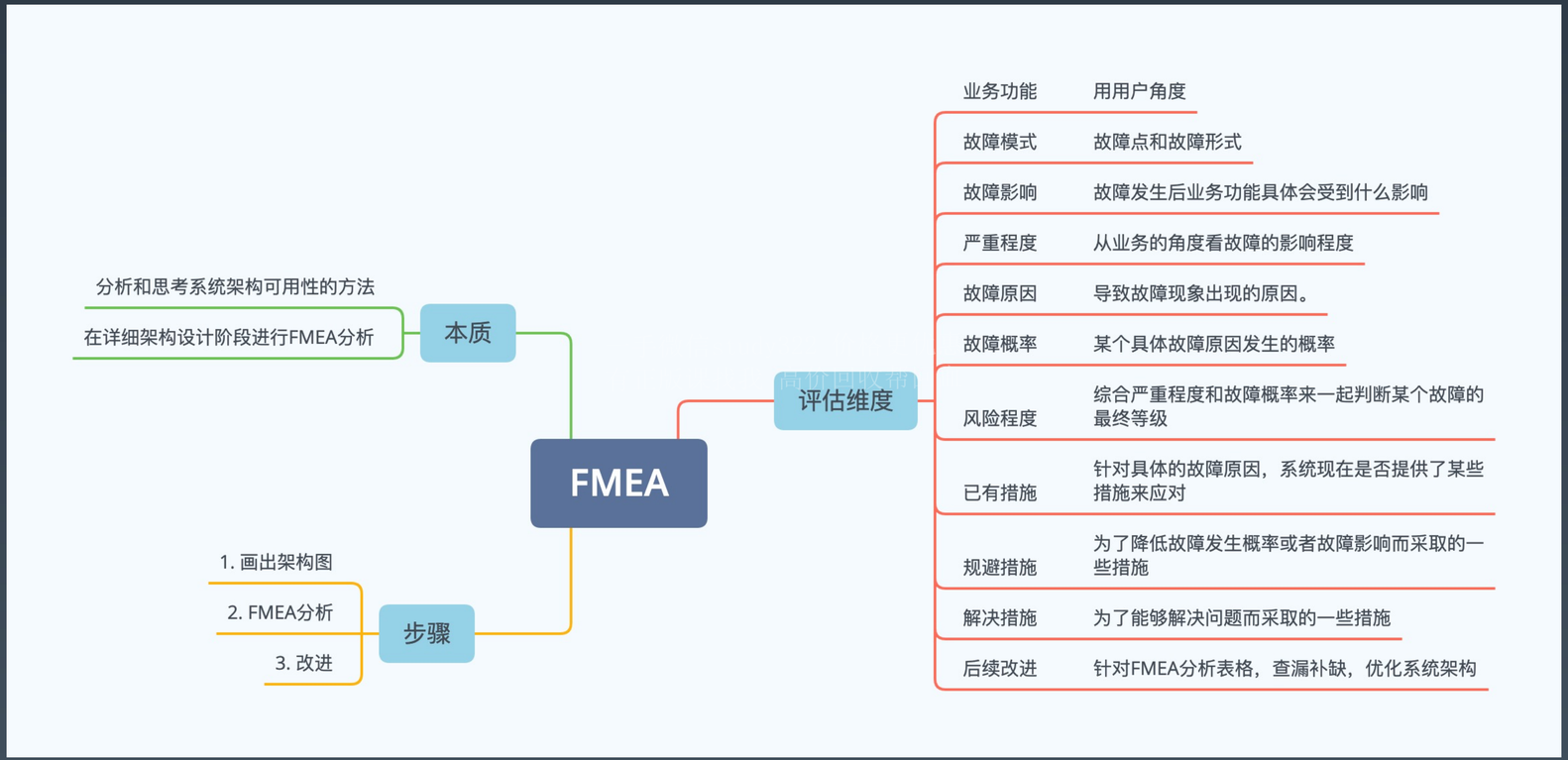
为什么同样的故障原因，不同场景下规避措施、改进计划都不一样了？

FMEA 优化后的架构





本节思维导图


FMEA
本质
分析和思考系统架构可用性的方法
在详细架构设计阶段进行FMEA分析
步骤
1. 画出架构图
2. FMEA分析
3. 改进
评估维度
业务功能
用用户角度
故障模式
故障点和故障形式
故障影响
故障发生后业务功能具体会受到什么影响
严重程度
从业务的角度看故障的影响程度
故障原因
导致故障现象出现的原因。
故障概率
某个具体故障原因发生的概率
风险程度
综合严重程度和故障概率来一起判断某个故障的最终等级
已有措施
针对具体的故障原因，系统现在是否提供了某些措施来应对
规避措施
为了降低故障发生概率或者故障影响而采取的一些措施
解决措施
为了能够解决问题而采取的一些措施
后续改进
针对FMEA分析表格，查漏补缺，优化系统架构

随堂测验

极客时间 训练营

【判断题】

1. FMEA 主要用于指导设计高可用架构。
2. 备选架构设计的时候就需要针对每个备选架构方案进行详细的 FMEA 评估。
3. FMEA 评估的时候，故障影响相关的数据越精确越好。
4. FMEA 评估的时候不能刻意太高故障的严重等级。
5. FMEA 改进措施中，并不一定需要都是解决方案。

【思考题】

FMEA 评估会带来一定的工作量，那么是否会降低架构设计的效率？

Q&A

茶歇时间

极客时间 训练营

八卦，趣闻，内幕.....

THANKS