

Fault Tree Analysis

故障树分析

2012-07-18

一. FTA 概述

1.FTA的发展---是安全系统工程中常用的一种分析方法。

1961年，美国贝尔电话研究所的Watson首创了FTA，并且将其应用于研究民兵式导弹发射控制系统的安全性评价中，用它来预测导弹发射的随机故障概率。接着美国波音公司的Hassle对这个方法做了重大的改进，并采用了计算机进行辅助分析和计算。

1974年，美国原子能委员会应用FTA对商用核电站进行了风险评价，发表了Rasmussen report引起世界各国关注。

目前FTA的分析方法已经从宇航，核工业进入一般电子，电力，化工，机械和交通等领域。

一. FTA 概述

2.FTA的发展基本概念和原理

故障树（FTA）是一种演绎推理法，即从结果分析原因的分析方法。这种方法是从一个可能的事件开始一层一层逐步寻找引起事故的触发事件，直接原因与间接原因。并且分析这些事故原因之间的逻辑关系，用一种成为故障树的树形图表示这些原因以及以及他们的逻辑关系。最后通过故障树的定性和定量分析，找出故障树的主要原因，未确定安全对策提供可靠依据，以达到预测和预防事故发生的主要目的。

一. FTA 概述

3.FTA的特点

- 1) 故障树（FTA）是一种图形演绎推理法，是事故事件在一定条件下的逻辑推理方法。它可以围绕某特定的事故做层层深入的分析，因而在清晰的故障树图形下，表达系统内各事件的内在联系，并指出单元故障和系统故障之间的逻辑关系，便于找出系统的薄弱环节。
- 2) FTA具有很大的灵活性，不仅可以分析某些单元故障对系统的影响，还可以对导致系统故障的特殊原因，如人为原因和环境影响进行分析。
- 3) 进行FTA的过程，是一个对系统更深入认识的过程，它要求分析人员把握系统内各要素间的内在联系，弄清各种潜在的因素对故障发生的影响的途径和程度，因而许多问题在分析的过程中就被发现和解决了，从而提高了系统的安全性。
- 4) 利用故障树模型可以定量计算复杂系统发生事故的概率，为改善和评价系统安全性提供了定量依据。

二. 故障树的构建

1.故障树分析程序

准备阶段

- 1) 确定所要分析的系统，在分析过程中，合理地处理好所要分析系统与外界环境与其边界条件，确定所要分析系统的范围，明确影响系统安全的主要因素。
- 2) 熟悉系统。这是故障树分析的基础和依据。对于已经确定的系统进行深入的调查研究。收集系统有关资料和数据，包括系统的结构，性能，工艺流程，运行条件，故障类型，维修情况，环境因素等。
- 3) 调查系统发生的故障。收集，调查所分析系统曾经发生过的故障和将来有可能发生的故障，同时还要收集，调查本公司，相关公司，以及国内外曾发生的故障。

二. 故障树的构建

1.故障树分析程序

故障树的编制

- 1) 确定故障树的顶事件。确定顶事件是指确定所要分析的对象事件。根据故障调查报告分析其损失大小和故障频率，选择易于发生且后果严重的故障作为故障树的顶事件。
- 2) 调查与顶事件有关的所有原因事件。从人，机，环境和信息等方面调查与故障树顶事件有关的所有故障原因，确定故障原因并进行影响分析。
- 3) 编制故障树。采用一些规定的符号，按照一定的逻辑关系，把故障树的顶事件与引起顶事件的原因事件，绘制成反映因果关系的树形图。

二. 故障树的构建

4) 故障树的定性分析

故障树的定性分析主要是按照故障树的结构，求取故障树的最小割集或最小径集，以及基本事件的结构重要度，根据定性分析的结果，确定预防故障的安全保障措施。

5) 故障树的定量分析

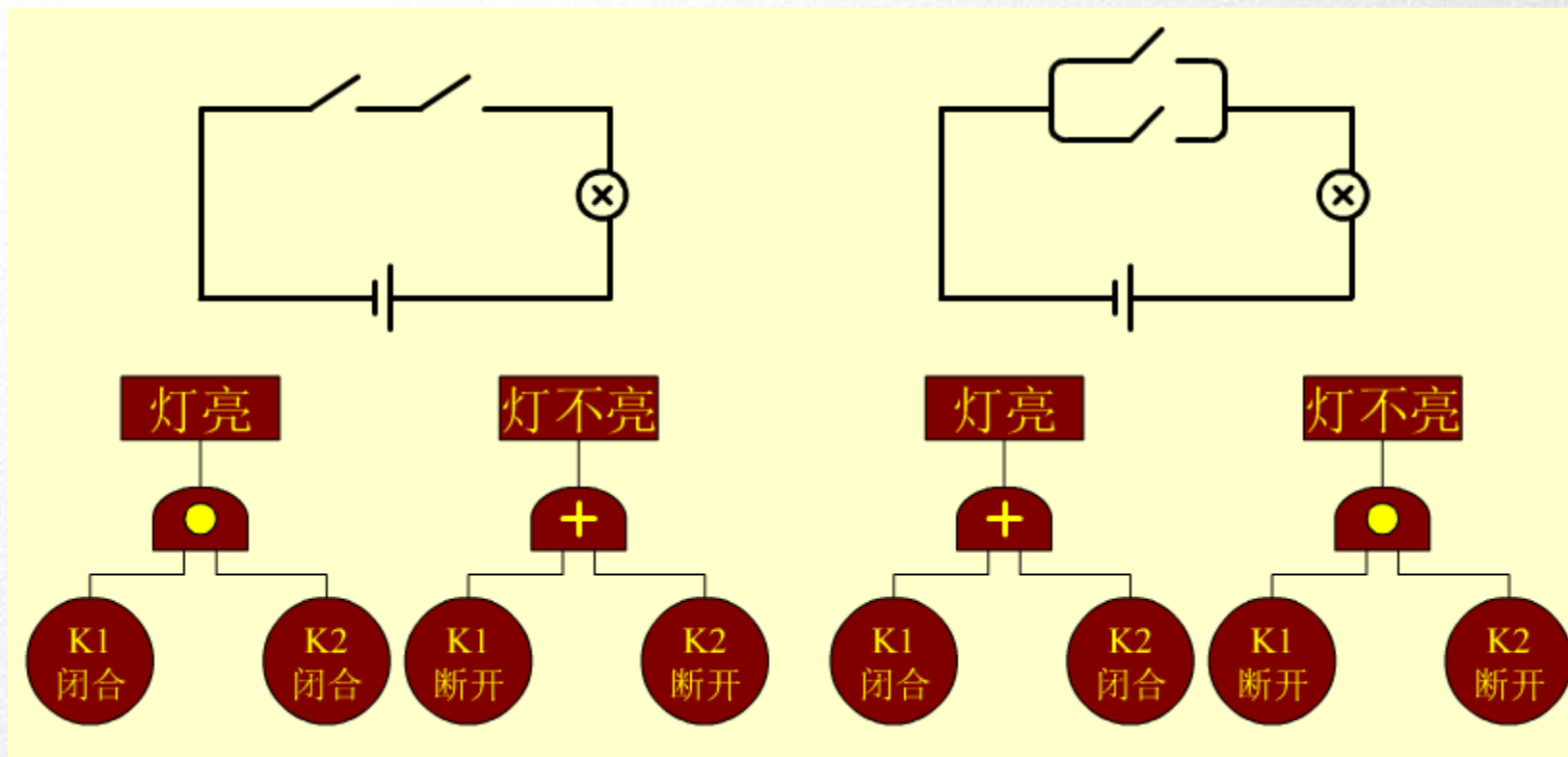
故障树定量分析主要是根据引起故障发生的个基本事件的发生概率，计算故障树顶事件发生的概率，计算各基本事件的概率重要度和关键重要度。根据定量分析的结果以及故障发生以后可能造成的危害，对系统进行风险分析，以确定安全投资方向。

6) 故障树分析的结果总结和应用

必须及时对故障树分析的结果进行评价，总结，提出改进建议，整理储存故障树定性和定量分析的全部资料和数据，并注重综合利用各种安全分析的资料，为系统安全性评价与安全性设计提供依据。

二. 故障树的构建

逻辑门符号举例（一）



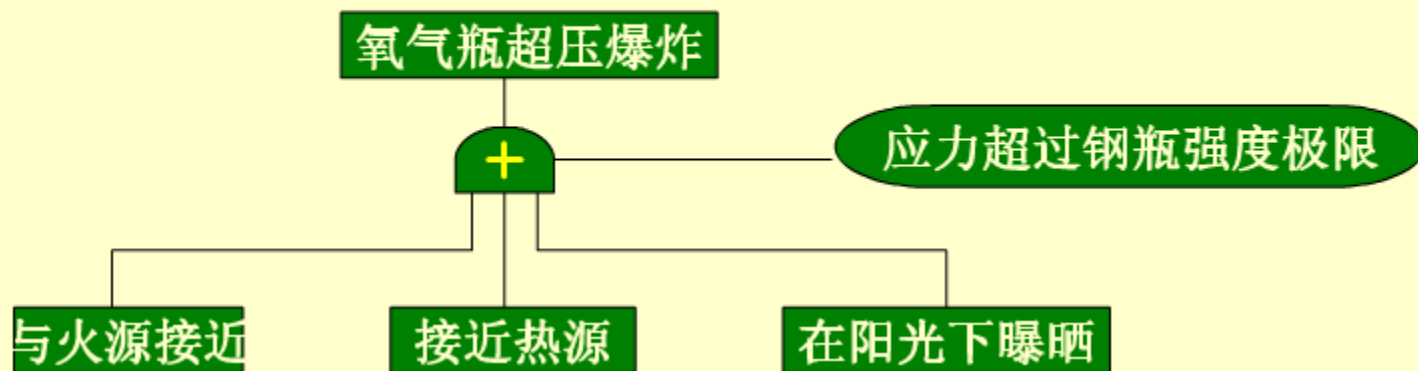
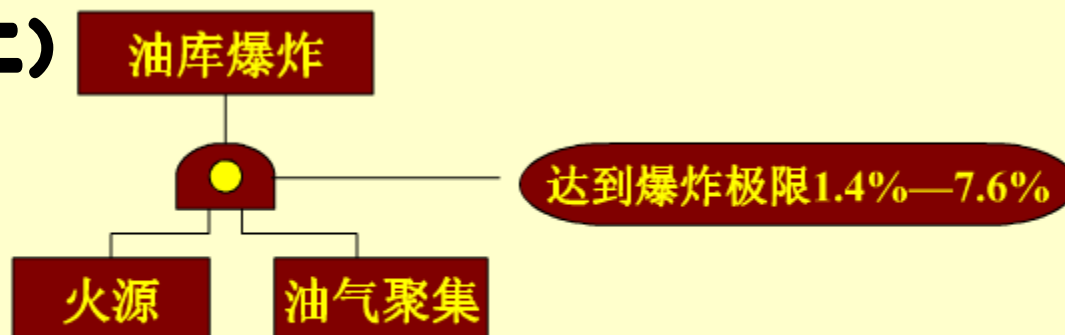
二. 故障树的构建

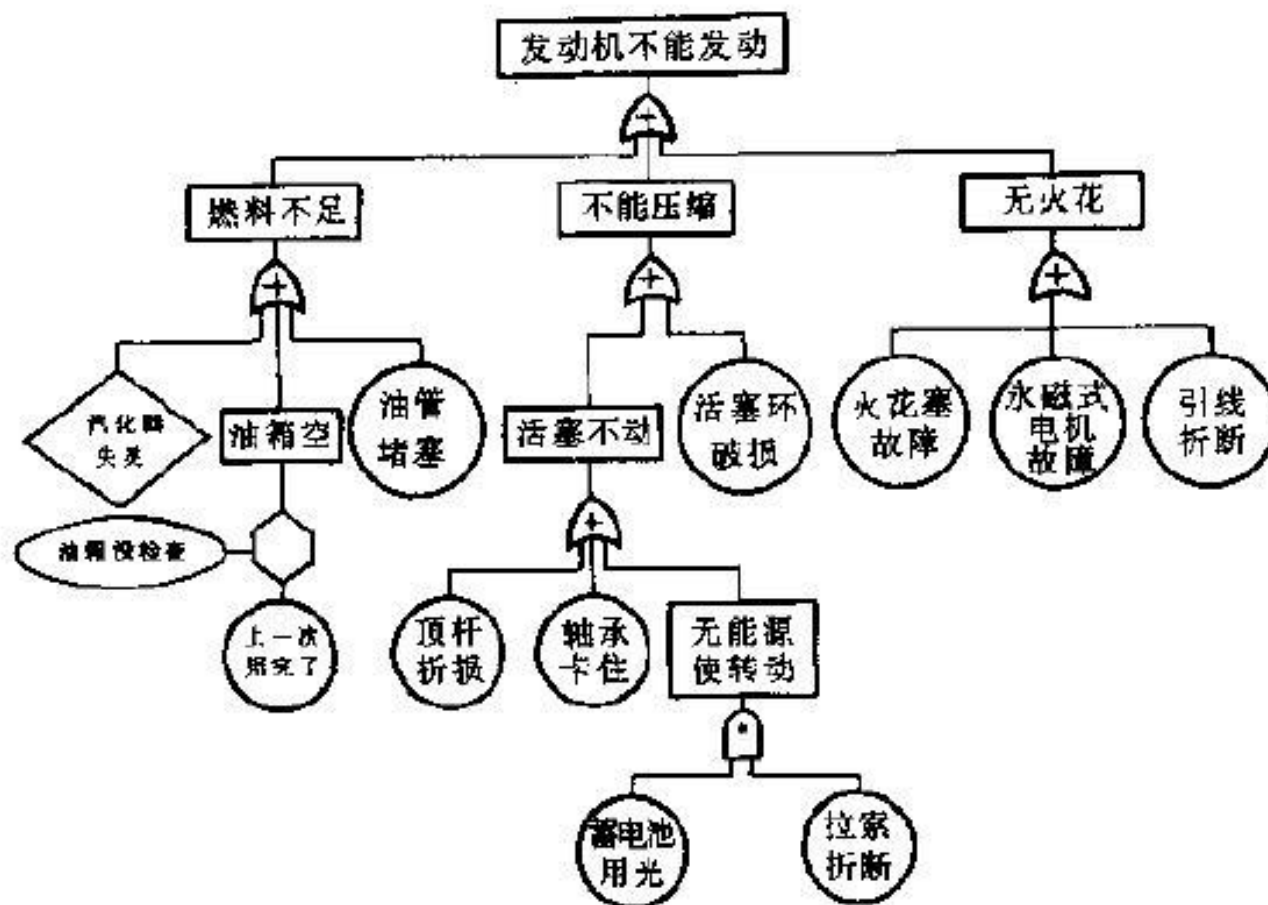
逻辑门符号介绍

名称		符号	符号的意义
逻辑门符号	与门		表示只有所有输入事件 B_1 、 B_2 都发生时，输出事件 A 才发生。换句话说，只要有一个输入事件不发生，则输出事件就不发生。有若干个输入事件也是如此。
	或门		表示输入事件 B_1 、 B_2 中任一个事件发生时，输出事件 A 发生。换句话说，只有全部输入事件都不发生，输出事件才不发生。有若干个输入事件也是如此。
	条件与门		条件与门表示输入事件 B_1 、 B_2 不仅同时发生，而且还必须满足条件 a ，才会有输出事件 A 发生，否则就不发生。 a 是指输出事件 A 发生的条件，而不是事件。
	条件或门		条件或门表示输入事件 B_1 、 B_2 至少有一个发生，在满足条件 a 的情况下，输出事件 A 才发生。
	限制门		限制门表示当输入事件满足某种给定条件时，直接引起输出事件，否则输出事件不发生，给定的条件写在椭圆形内。
	转出符号		表示这个部分树由此转出，并在三角形内标出对应的数字，以表示向何处转移。

二. 故障树的构建

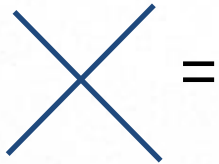
逻辑门符号举例（二）





5 Why 分析基础

看一眼就能知道的情况，要好好的去把握



=

事实的来龙去脉含糊不清



=

事实的来龙去脉很清楚

~~炉内的温度不上升~~

炉内的温度达不到规定值

炉内完全不上升
(和常温一样)

~~A生产线的制品有不良发生~~

A生产线的第3工程，制品的○○部+尺寸不良在冬季有大约5,000ppm発生量

~~屏幕上显示出的OHP表看不清~~

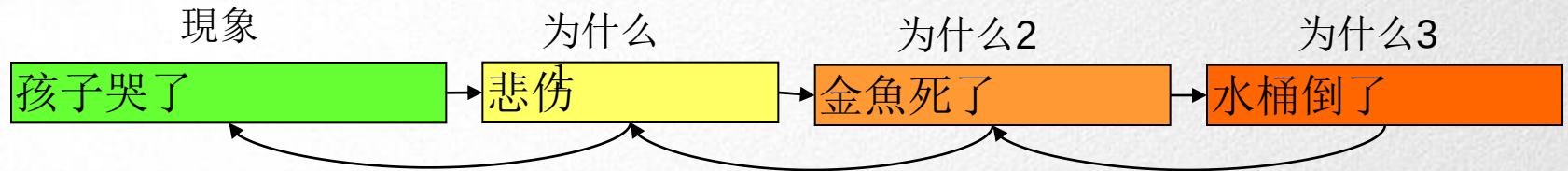
屏幕上的文字模糊不清

显示出来的部分很暗

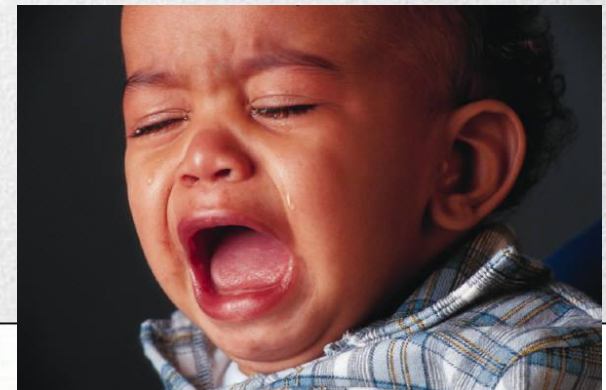
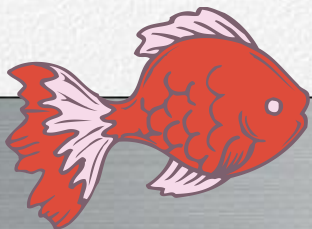
~~军用手套被随处乱扔~~

在油罐旁边经常在中午会有很脏的军用手套被仍在一边

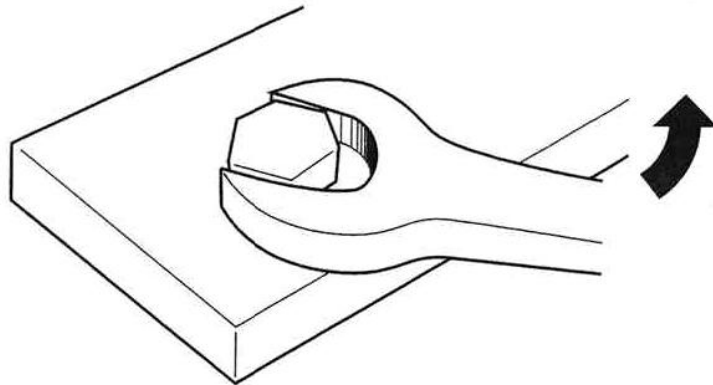
从「为什么」到「现象」的追溯



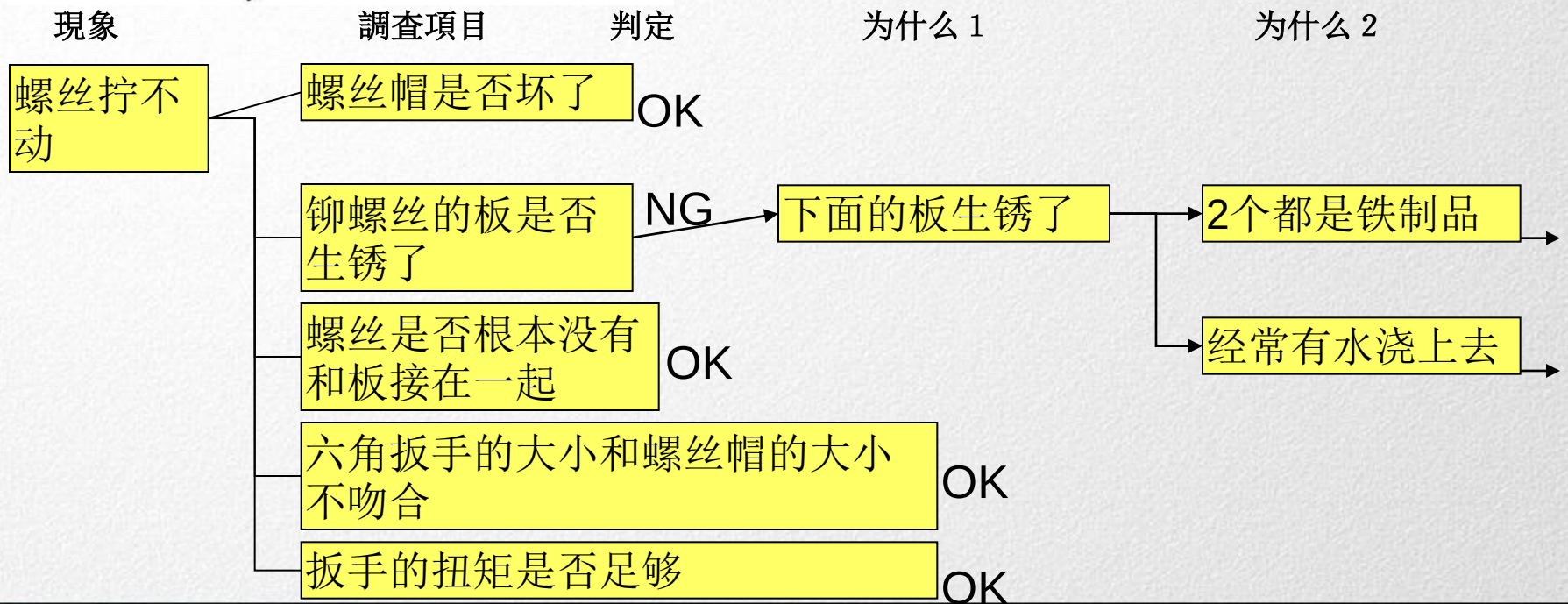
(为啥3)	水桶倒了	从	(为啥2)	金魚死了
(为啥2)	金魚死了	从	(为啥1)	很伤悲
(为啥1)	很悲伤	从	(现象)	在哭泣



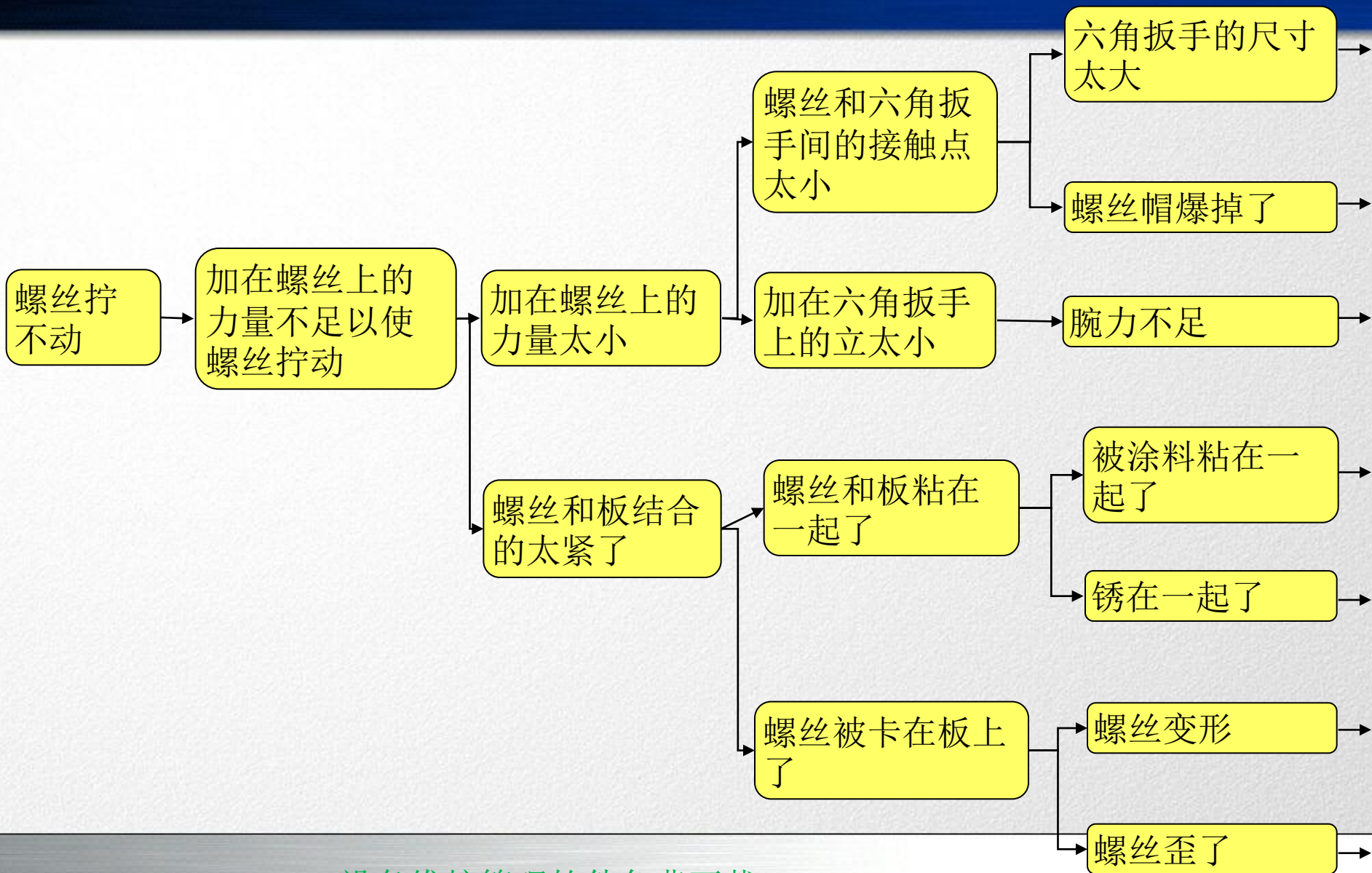
螺丝为什么转不动？



探究原因

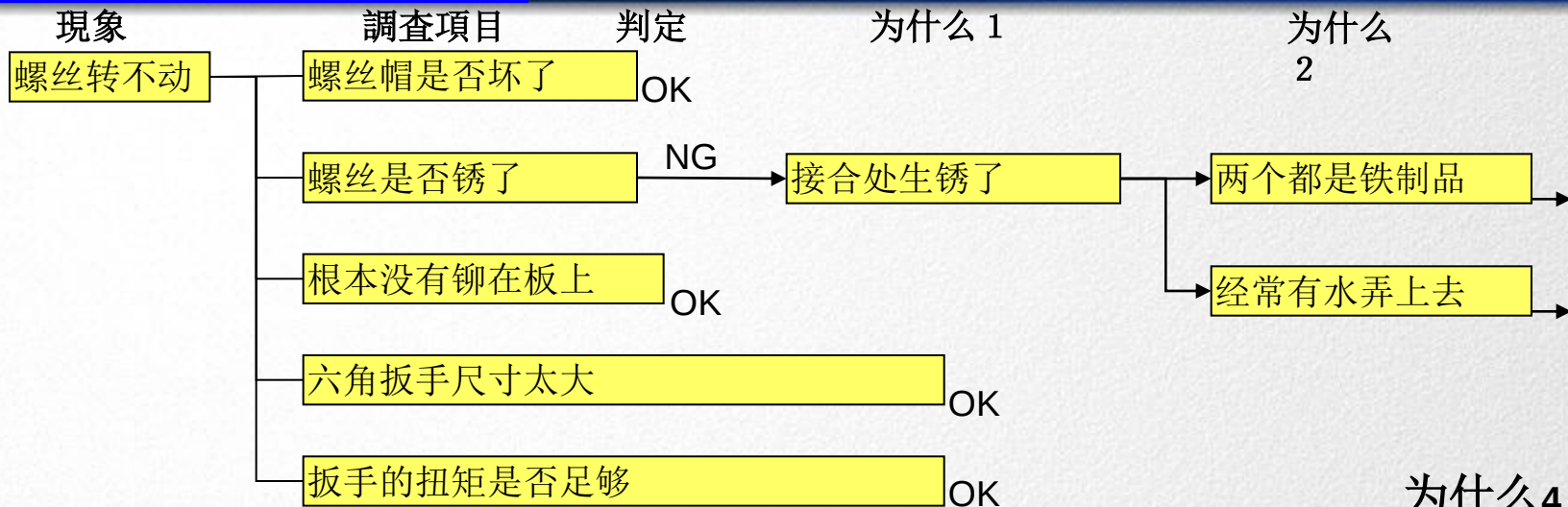


从原理・原则出发探究问题本质

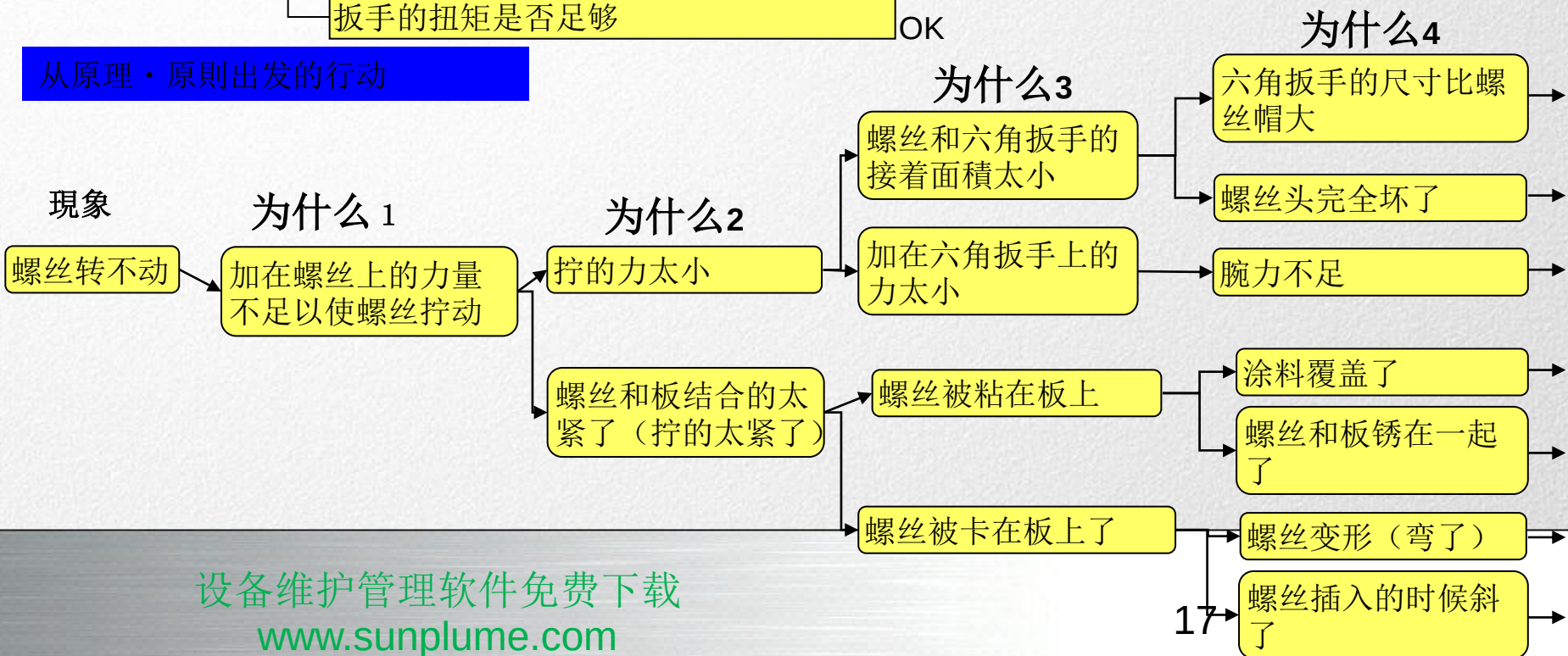


各种方法的比較

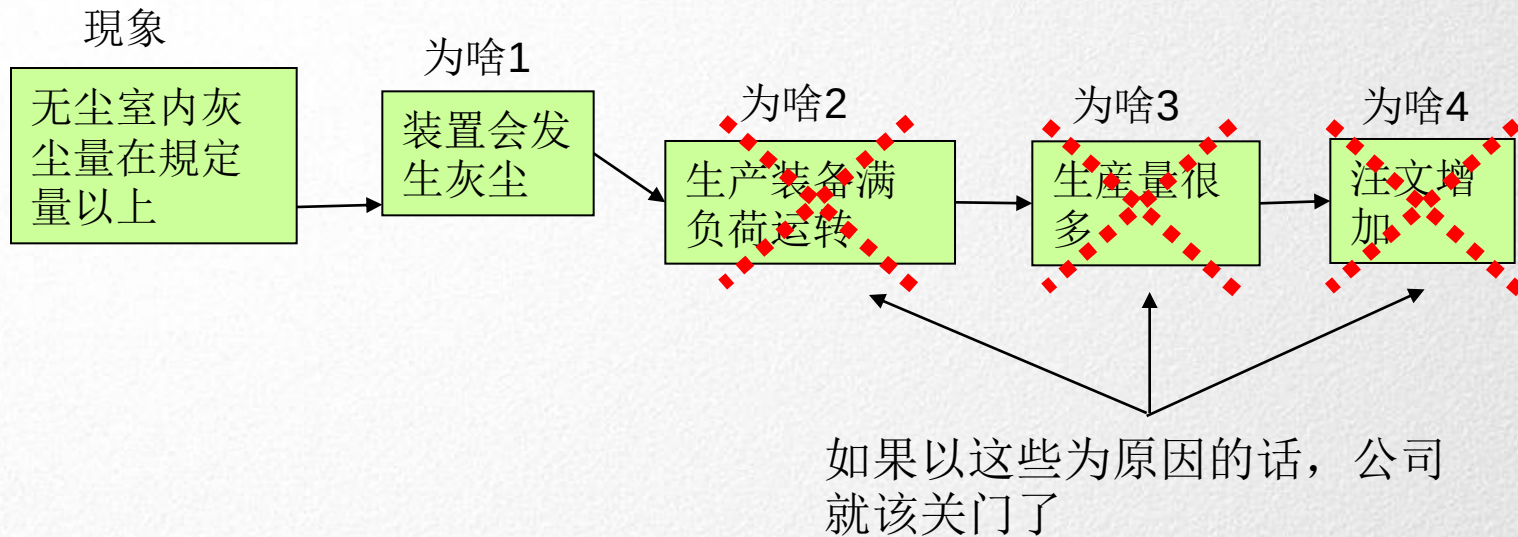
从应有的状态开始的行动



从原理・原则出发的行动



奇怪的「为什么」的例 1



分析的方向不要感情用事

