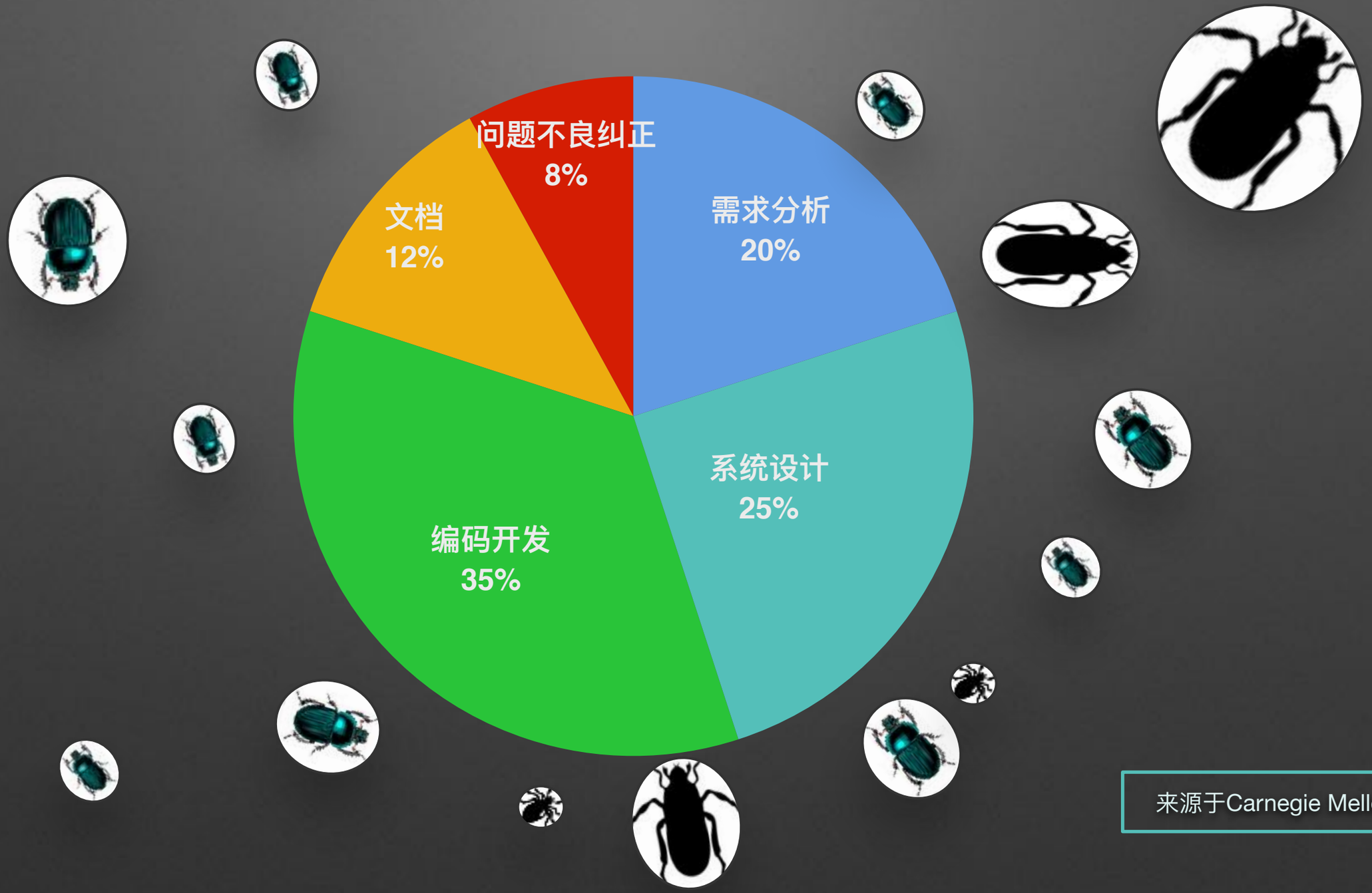
项目管理 之于 安全开发

— 范亚铃（安全牛）

议题主旨

随着信息安全的重要性不断被认可和提高，安全开发也日益受到软件研发管理者的重视。但是安全开发不仅仅是流程、意识和技能的问题，它也是一个工程性问题，安全开发是需要成本的。如何避免安全开发成为压死骆驼的最后一根稻草，如何顺利的将安全开发有机的融入到现有研发流程体系之中，这是我们即将要探讨的议题。

安全漏洞的源



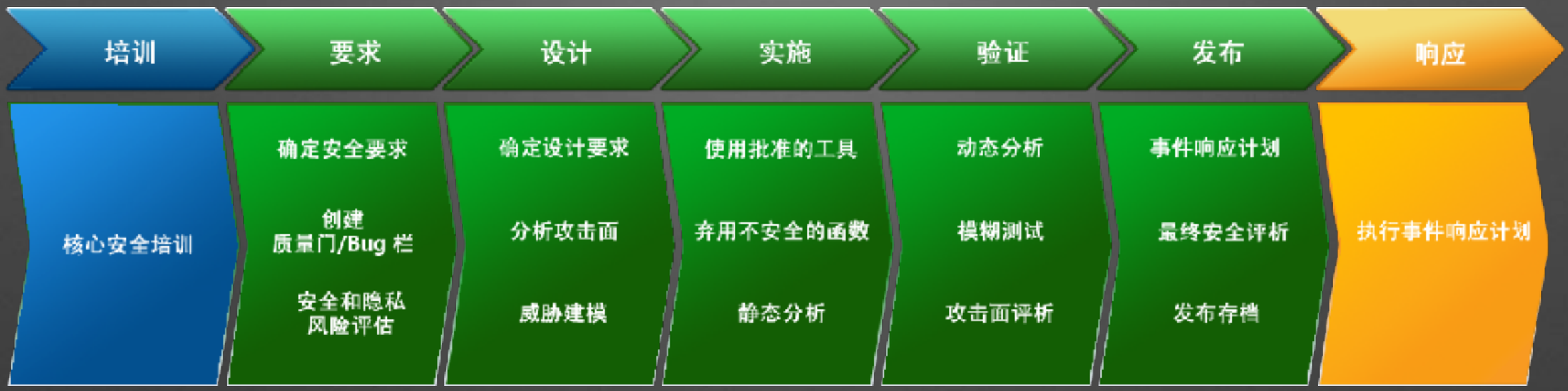
来源于Carnegie Mellon

漏洞解决的轨迹

漏洞根除之路沿着软件系统生命周期不断向前延伸。

安全开发方法不断形成

微软安全开发方法



16项必须的安全活动，3项可选的安全活动。

安全开发方法不断形成

思科安全开发方法

安全开发方法不断形成

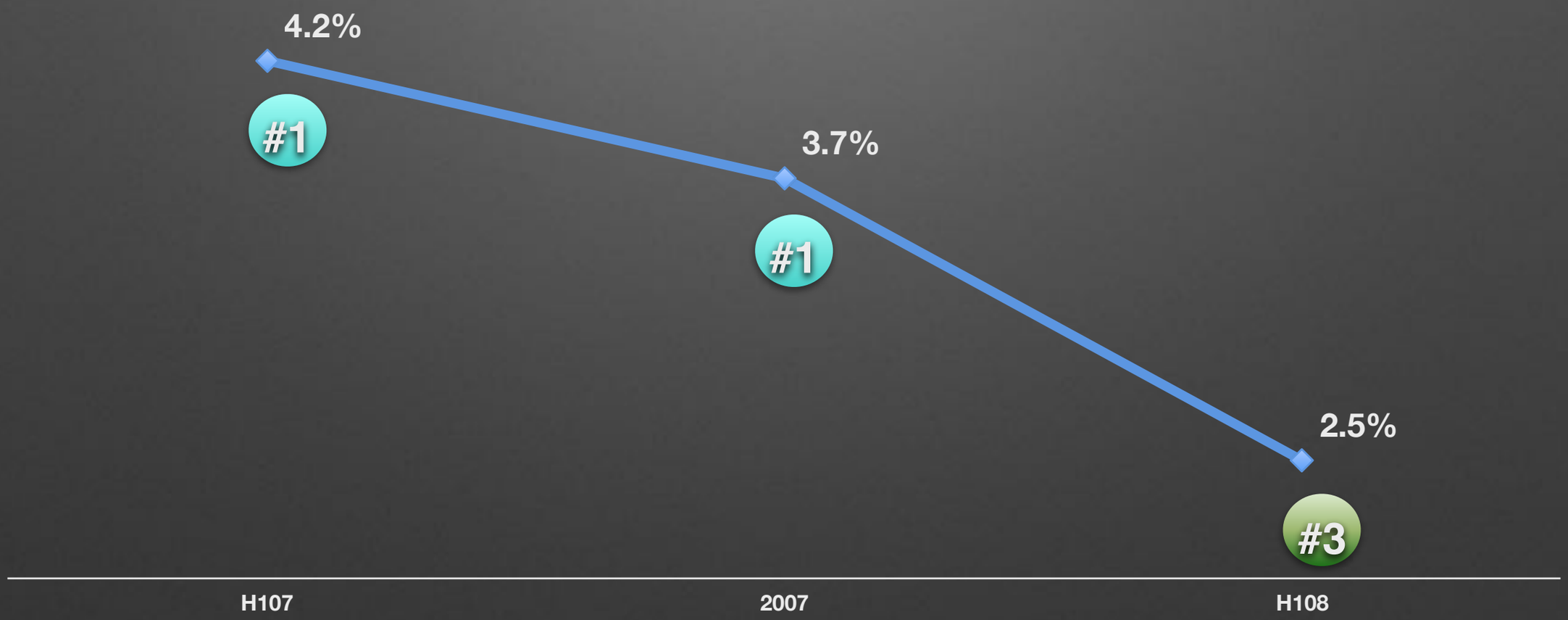
GooAnn安全开发框架

•业务安全分析	•威胁建模	•安全编码培训	•单元测试	•用户安全意识培训
•隐私安全分析	•攻击面分析	•安全编码规范	•集成测试	•系统安全管理与操作培训
•合规性分析	•系统安全建模	•原代码审核	•系统功能测试	•临时账户管理
•业务安全建模	•设计评审	•静态代码分析	•可接受性测试	•系统安全交付
•需求评审		•单元测试	•模糊测试	•数据安全迁移
		•代码评审	•渗透测试	•上线评审
			•代码动态分析	
			•错误注入测试	

安全开发管理（配置安全管理 漏洞管理 安全培训管理，……）

微软漏洞的比重逐步降低

在全部已披露的漏洞中，微软产品所占的比重



Sources: IBM X-Force 2007, 2008 Security Report

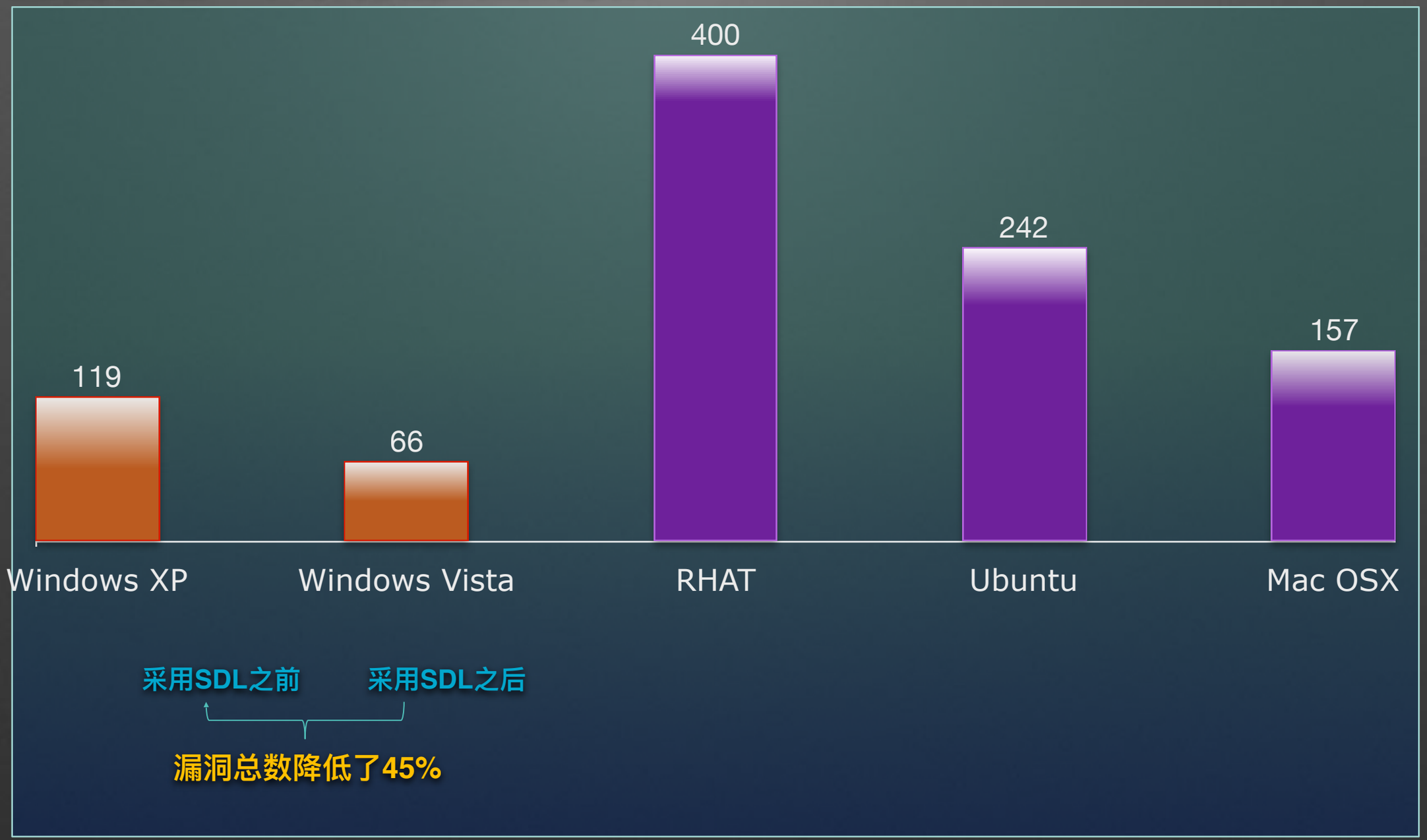
SQL Server采用SDL的效果

正式发布后36个月内披露的漏洞总数

Sources: Analysis by Jeff Jones (Microsoft technet security blog)

Vista采用SDL的效果

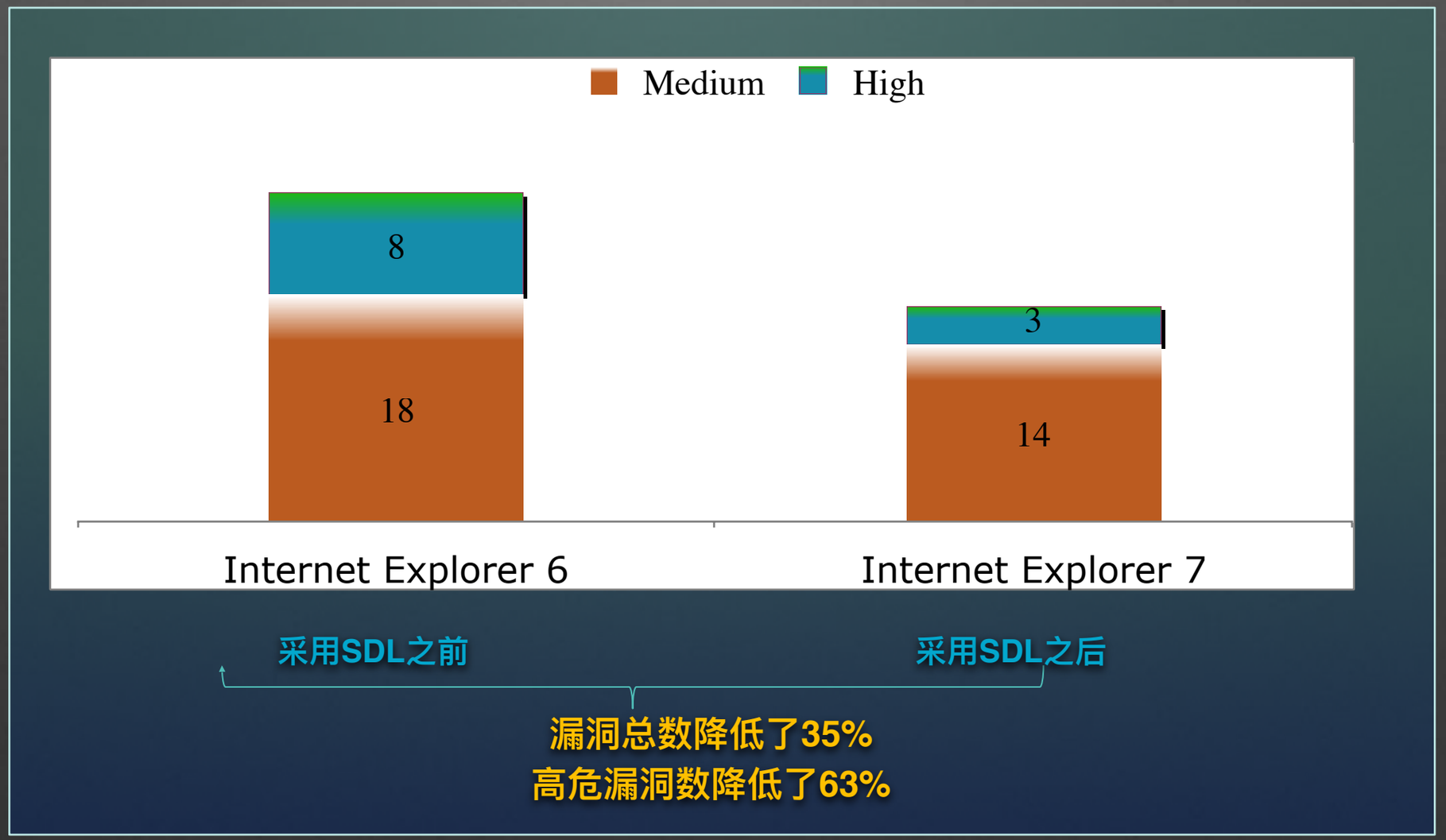
正式发布后12个月内披露的漏洞总数



Source: Windows Vista One Year Vulnerability Report, Microsoft Security Blog 23 Jan 2008

IE采用SDL后的效果

正式发布后12个月内修复的漏洞总数



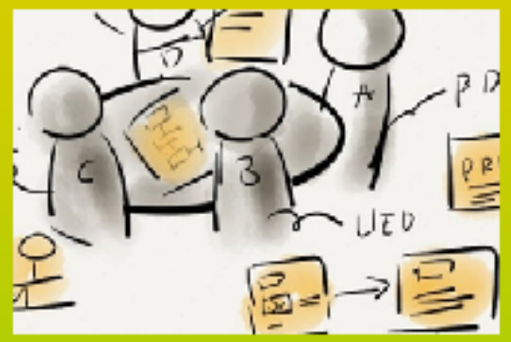
Source: Browser Vulnerability Analysis, Microsoft Security Blog 27-NOV-2007

从国内的很多实例来看，

效果不全都是积极的...

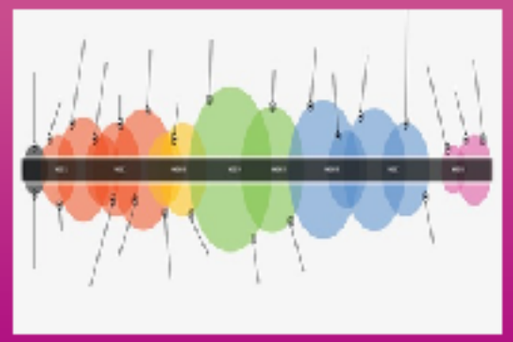
知易行难

人员技能



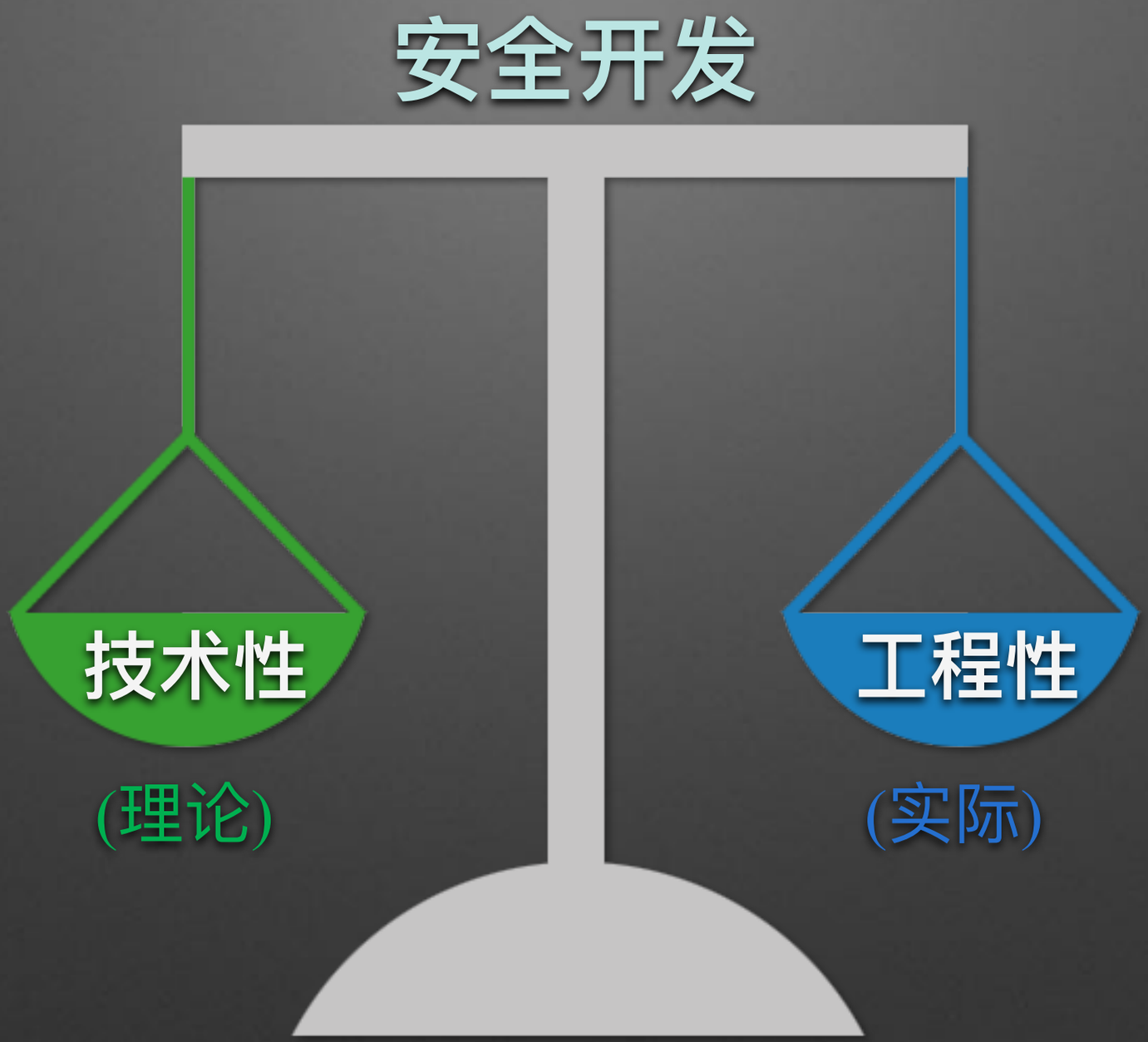
开发流程

项目成本



项目周期

安全开发的两个属性



安全开发面临的课题

系统使用者

成本关心者

关系人

开发管理者

开发执行者

课题解锁

取舍

可舍	不可舍
时间空耗	持续改善
低效能活动	问题深挖

独立的QA

PM

- 进度
- 推进
- 油门

平 衡

QA

- 质量
- 控制
- 刹车

进退有度

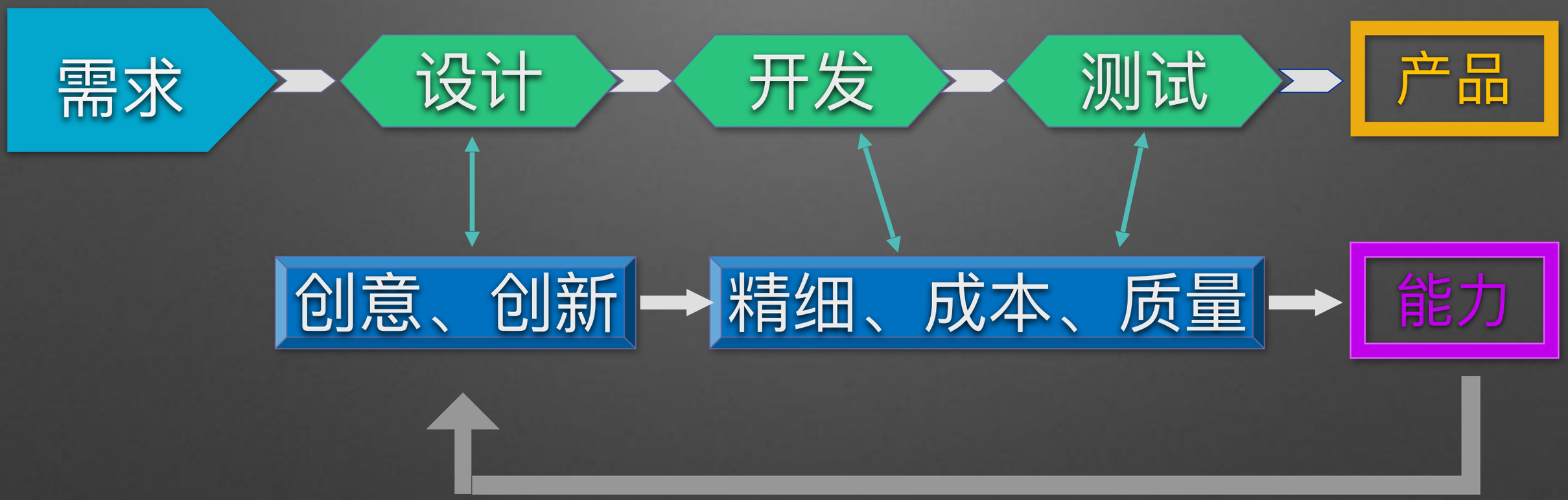
给管理者减负

取舍之外

安全开发
组件化、
工具化、
自动化

项目管理
精细化、
定量化、
自动化

软件开发

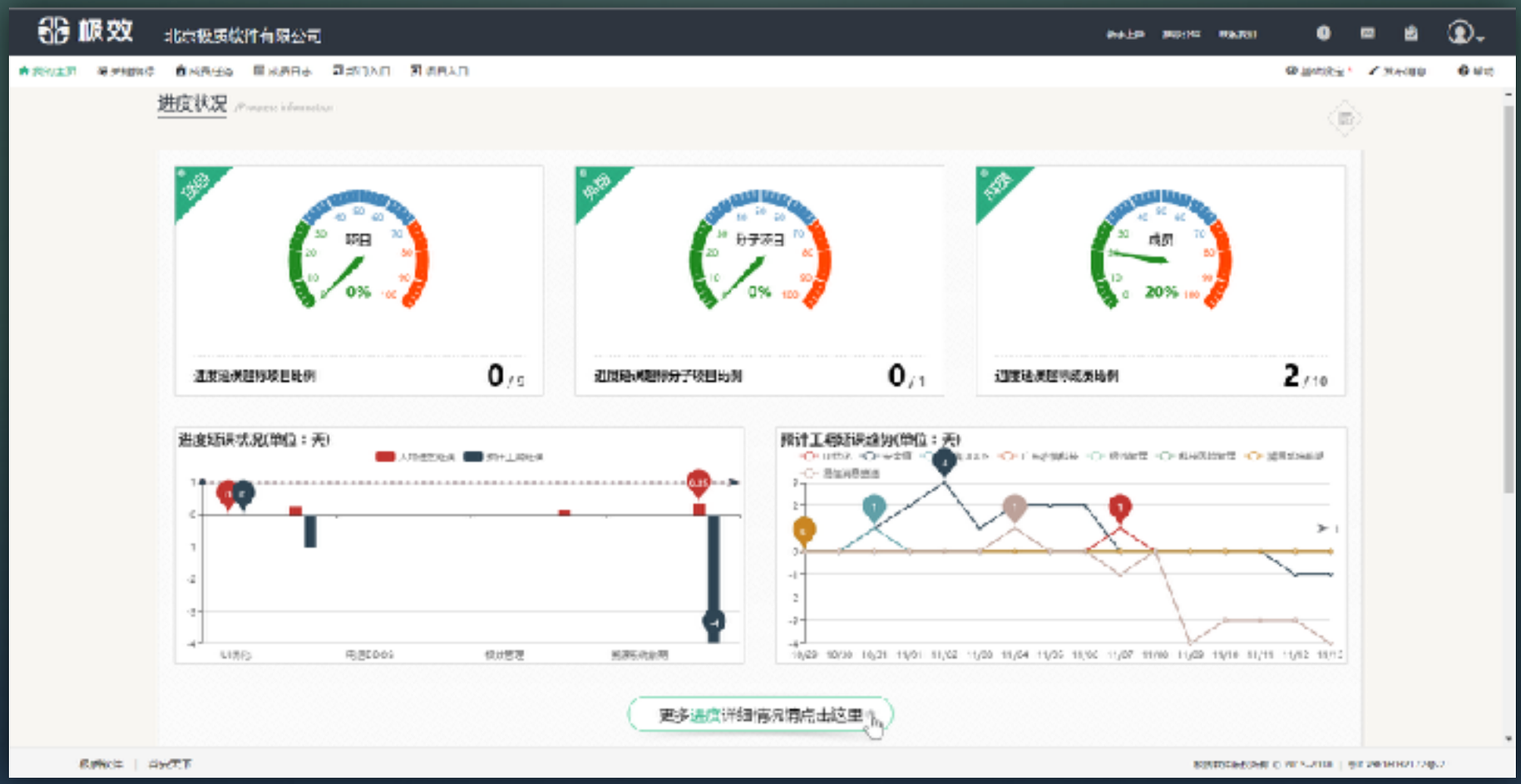


探索之路

在我们的实践中，实施精细化项目管理后：

- 团队生产效率提升超过15%；
- 项目进度延误率大幅下降，延期项目少于20%；
- Bug率大幅下降，软件质量和安全性显著提升；
- 项目经理用于进度安排和项目数据收集分析的时间减少70%以上；
- 团队成员工作态度明显好转，积极性和主动性大幅提升。

“极效”管理



jxguanli.com

谢谢您的倾听！