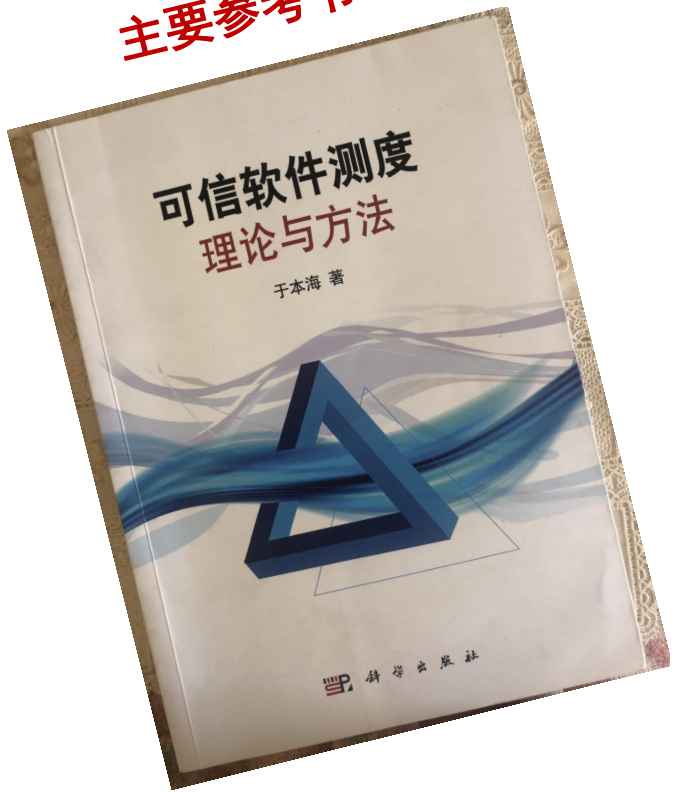
高可信软件工程

主要参考书：



主讲教师：李晓红

天津大学智算学部
2020年2月16日

第一讲 可信软件

高可信软件工程

1.1可信软件研究背景

- 软件系统的脆弱性是系统发生各种故障和影响实效的根源，直接或间接地对用户造成巨大损失。在一些可信度要求高的领域，软件系统实效会给人类生命， 财产造成重大甚至灾难性的损失。

  - 1996年6月欧洲 Ariane五型火箭，发射37s爆炸，**损失70亿$**
  - 2002年NIST发布：美国由软件缺陷引起的损失每年高达**595亿$**
  - 2003年俄亥俄州电力能源公司电力监测管理系统XA/21出错，造成美国和加拿大地区历史上最大停电事故，损失**250~300亿$**

  - 2006年中国银联跨行交易系统出现故障，**瘫痪8h，34万家商户**和**6万台ATM机**受影响
  - 2015年支付宝故障，转账无法进行，余额宝收益显示不了，造成人心惶惶
  - 携程官网及APP系统瘫痪，按照携程公布的数据，携程宕机一小时损失**100万$**

1.1可信软件研究背景

2019年最新发现的网络安全事件

- 澳大利亚维多利亚州政府3万名雇员个人信息外泄。3万名维多利亚州公务员工作详情数据遭窃。
- 万豪酒店5亿客户数据泄漏。万豪公司损失5.77亿美元。
- 德国IT安全机构回应数百名政客私人信息泄漏事件。多达1000名德国政界人士和名人遭信息泄露，内容包括私人地址、手机号码、聊天记录和信用卡号码。
- TLS 1.2 协议现漏洞，近3000网站受影响。
- 印度国有天然气公司再次泄漏了数百万客户的敏感信息（ Aadhaar 生物识别数据库信息）。预计受影响总人数或超过 670 万。
- 俄罗斯50多家大型企业遭到未知攻击者勒索。攻击使用物联网设备，尤其是路由器，伪装成欧尚、马格尼特、斯拉夫尼奥夫等50多家知名公司发送钓鱼电子邮件，对公司人员进行勒索攻击。
- 英特尔CPU再现高危漏洞 得到官方证实可泄漏私密数据。美国伍斯特理工学院研究人员在英特尔处理器中发现另外一个被称作Spoiler的高危漏洞，与之前被发现的Spectre相似，Spoiler会泄露用户的私密数据。Spoiler的根本原因是英特尔内存子系统实现中地址预测技术的一处缺陷。

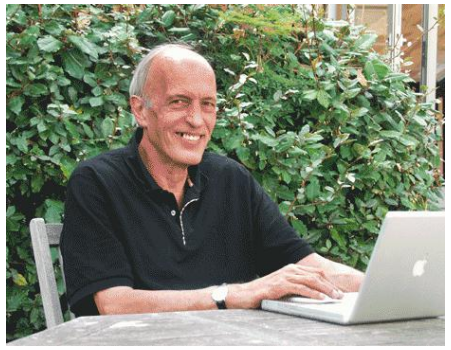
1.1可信软件研究背景

• 随着软件应用范围越来越广，需求复杂度越来越高，可用性需求越来越强。

软件开发存在的问题：

- 软件应用广度和深度加大，在互联网环境下，软件呈现网络化、服务化、虚拟化和集成化，对软件安全的要求越来越高，而软件可信程度不足。
- 软件项目的规模越来越大，开发环境越来越复杂，项目不能按期、按预算及预期质量完成的比例越来越高。著名的Chaos 报告对美国 8380 个软件项目的统计，仅有16%的项目按时按预算完成，有53 %的软件项目超时超预算，其余31%的项目被取消。
- 在项目开发前期，软件组织不能全面了解新开发项目的全部属性特征，对其复杂度、技术难题等因素分析不足，使得软件开发过程不可控，软件产品不可信。
- 软件项目开发是动态过程，会遇到很多不确定的困难和障碍：项目特征及外部环境变化；开发人员与用户沟通不到位；开发人员管理问题；缺乏有效软件过程管理方法和工具；软件设计存在缺陷等。
- 软件漏洞安全问题突出。

1.1 可信软件研究背景



1985年J.C.Laprie （**Jean-Claude Laprie**）提出了可信计算（dependable computing）的概念.

可信软件开发过程及软件有效运行是保证各类业务成功及人类安全关键因素.

软件产品可信在某种程度上取决于软件项目开发过程的可信性.

—软件可信性问题已经成为国际上一个重要问题

- ✓ 分析软件发开过程和软件产品的应用情况分析
- ✓ 研究可信软件评价指标体系
- ✓ 构建面向全生命周期的软件可信性测度模型

对提高软件可信度水平和软件成功率具有重要意义

1.2 可信软件的定义

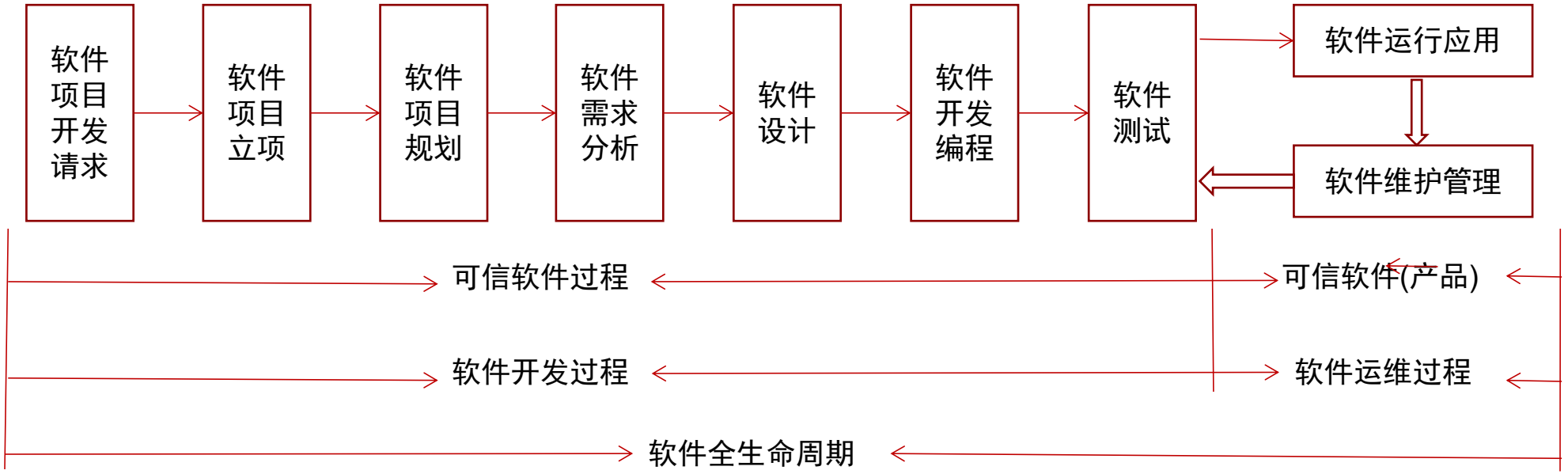
“**可信性**”是在“正确性”、“可靠性”、“安全性”、“时效性”、“完整性”、“可用性”、“可预测性”、“可控性”等众多概念的基础上发展起来的一个新概念，是客观对象诸多属性在人们心中的一个综合反应。

“**可信**”是指一个实体在实现一个既定目标的过程中，行为及结果可以预期，它强调目标与实现相符，强调行为和结果的可预测性和可控制性。

“**软件的可信**”是指软件系统的动态行为及其结果总是符合人们的预期，再受到干扰时仍能连续的提供服务。这里的干扰包括错误操作，环境影响、外部攻击等。

1.3 可信软件的内涵

- 将软件开发阶段作为一个整体来评估过程的可信性，不具体区分软件开发过程的细节，而将软件运维过程作为一个整体评价软件产品的可信性。



1.3 可信软件的内涵

管理视角

从软件可信方法学（STM）将软件可信性扩展为“软件满足既定需求的信息度”。

软件应用视角

软件的“可信”一个软件系统的行为总是与预期一致，软件的动态行为及其结果总是符合人们的预期，在受到干扰时仍能提供连续服务的能力，软件关注使用层面的综合化的质量属性及其保障，则可称之为可信。

理论层面

软件可信性是指计算机软件系统的服务经过证明，是值得信赖的。

软件工程视角

ISO/IEC 15408标准将可信定义为：一个可信的组件、操作或过程的行为在任意操作条件下都是可操作的，并能很好的抵抗应用软件、病毒以及一定的物理干扰造成的破坏。

1.4可信软件评价涉及的主要问题

- 可信软件评价涉及的主要领域

可信软件评价研究是管理学、软件工程以及信息科学等多学科的交叉领域，侧重软件项目管理研究

管理学科：包括组织层面、项目层面、工程层面和支持层面的管理；9大知识领域体系：软件范围管理、时间管理、进度管理、质量管理、成本管理、风险管理、人力资源管理、采购管理

研究对象：大型软件系统开发的工程化的理论和方法

研究内容：软件开发过程，以及软件开发的目的、任务、方法、技术、工具、文档和产品规格等

1.4可信软件评价涉及的主要问题

- 可信软件评价研究面临的主要问题
  - 软件可信评价的理论与方法研究

    将管理学科理论与软件工程理论有机结合，研究评价软件过程可信和软件产品可信的理论与方法。
  - 软件过程可信对于软件产品可信影响关系研究

    开发过程可信属性对软件产品可信属性的映射研究，研究软件产品可信属性与软件过程可信属性影响程度的定量关系。
  - 注重软件可信度度量模型研究忽略了软件过程可信性度量研究

    软件过程可信是影响软件产品可信的主要因素之一。软件的缺陷往往是在软件开发过程中植入的。因此，研究软件过程的可信性，是从根本上解决软件产品可信问题的主要途径之一。
  - 单一属性的软件可信评价方法不足以反应软件可信总体水平，缺乏软件产品综合可信度测度模型

    软件可信属性之间相互作用、相互影响，单一属性的评价不能反映整体可信水平， 需要构建多目标多属性的综合软件可信评价模型，全面反映可信水平。

1.4可信软件评价涉及的主要问题

- **软件过程可信度评价指标体系建立**

  从软件过程的客观属性（过程实体、过程行为、过程产品）和主观属性（软件成本、软件质量）等多个维度，构建软件过程可信度测度指标体系。

- **软件产品可信度评价指标体系建立**

  考虑软件应用环境复杂性和不确定性等特征，利用现有软件产品可信研究成果，在以往软件可信属性基础上，构建可信属性以及二级评价指标体系。

- **软件过程可信影响软件产品可信水平机理研究**

  从理论视角分析软件开发过程可信和软件产品可信相关性，建立软件过程属性和可信软件产品属性映射关系结构模型。发现影响软件过程可信和产品可信的关键属性。

- **建立可信软件过程评价模型**

  综合考虑各维度相互影响作用，用模糊层次分析理论，建立反映软件过程整体可信水平的综合评价模型。

- **建立可信软件评价模型**

  应用证据理论，结合单一属性度量模型，建立软件可信评价综合模型。

谢谢大家！