1、什么是可信软件

软件行为符合预期

自身行为

交互行为

特殊行为

可信指标

正确性

可靠性

安全性

可用性

2、可信软件的挑战

软件是复杂的

软件规模和应用领域不断扩大

需求不确定

项目管理的成本和风险

Bug 软件正确性和质量

3、软件的复杂性

规模大，组件多，关系复杂（访问序列，用户数量庞大）

交互频繁，行为动态（指数增长，动态算法）

运行环境的不确定性

功能与效率

软件安全

4、A garage door  open design

自动开车门，

5、complex from simple

cellular automata 元胞自动机　　（2^3=8）即2^8种规则

完美的分型结构:任何局部都与整体保持一致；

个体行为简单，规模庞大

swarm intelligence

鸟类飞行:抵御外敌，个体本身生存概率很高

swarm robotic

深度神经网络 很难做到如何修正问题

无序系统特定环境下有效（混沌理论）

脑极头盔

6、应用领域

7、软件工程第一定律

8、软件需求不确定

需求变动

软件本身软件环境

需求本身相容性

9、举例

例子一： the vasa sink

频繁改变需求 ： changing requirement frequently

没有具体标准 ： no specification

没有系统文档 ： design

没有测试过程 ： test

例子二： ariane 5disaster 火箭爆炸

10、软件工程的目标

用户信任

11、软件可信性

软件需求

12、形式化方法

判定程序是否符合期望

精确的数学语言

合理的抽象

严格的推理和证明

软件工程方面的应用

需求精确建模

模型转换，形式化开发设计

推理证明验证软件行为

13、 需求设计实现验证

14、形式化软件开发 : 之前满足的性质不会被破坏

用户需求到软件代码自动生成

程序代码符合需求

特点 : 需求一致、设计正确、模型到代码自动转换

（模型开发，不是写代码）模型迭代满足之前证明的条件

15、EVENT-B 正确有用（工具:Rodin）

http://wiki.event-b.org/index.php/Main_page 下载（首先安装jdk1.8）

核心概念:

informal requirement、modeling、refining精化、proving证明