系统架构设计师

安全和可靠性案例

姜美荣

目录

直播内容：安全和可靠性设计

1. 安全和区块链相关案例☆☆☆☆

- 关于区块链
- 相关案例

2. 可靠性设计☆☆☆☆☆

- 可靠性定义
- 可靠性设计
- 可靠性模型
- 可靠性管理
- 相关案例

区块链技术

- 用共识机制、点对点网络、智能合约等技术结合而成的一种分布式存储数据库技术。

- 区块链分为公有链、联盟链、私有链和混合链四大类。

- 区块链的典型特征：多中心化、多方维护、时序数据、智能合约、不可篡改、开放共识、安全可信。

区块链技术

区块链的特点「区块链」是一串以密码学方式关联起来的数据块，块内记录了一段时间内网络中发生的所有事件(交易).块链条（账本）分布存储在网络中多个节点。

去中心化:由于使用分布式核算和存储，不存在中心化的硬件或管理机构，任意节点的权利和义务都是均等的，系统中的数据块由整个系统中具有维护功能的节点来共同维护。

开放性:系统是开放的，如:区块链上的**交易信息是公开**的，不过**账户身份信息是高度加密**的。

自治性:区块链采用基于协商一致的规范和协议(比如一套公开透明的算法)，使得整个系统中的所有节点能够在信任的环境自由安全的交换数据，使得对“人”的信任改成了对机器的信任，任何人为的干预不起作用。

安全性(信息不可篡改):数据在多个结点存储了多份，**篡改数据得改掉51%结点的数据**，这太难。同时，还有其它安全机制，如:比特币的每笔交易，都由付款人用**私钥签名**，证明确实是他同意向某人付款，其它人无法伪造。

匿名性(去信任):由于节点之间的交换遵循固定的算法，其数据交互是无需信任的(区块链中的程序规则会自行判断活动是否有效)，因此交易对手无须通过公开身份的方式让对方对自己产生信任，对信用的累积非常有帮助。

区块链技术

区块链分层架构

面向具体场景开发DApp，涵盖金融支付（跨境结算）、供应链管理（农产品溯源）、数字身份等垂直领域。该层直接承载用户交互与业务逻辑实现。

部署智能合约实现自动化执行，通过预编程脚本在满足条件时触发资产转移、合约清算等操作。以太坊等平台在该层扩展了图灵完备的编程能力。

设计经济模型驱动节点参与验证，如比特币的挖矿奖励和交易手续费机制。通过代币发行与分配规则维护网络生态的可持续性。

集成PoW、PoS、DPoS等算法解决分布式网络记账权分配问题，通过超过51%节点验证机制确保全网账本一致性。共识机制直接影响系统的吞吐量与安全性。

采用P2P组网技术构建分布式自治系统，节点通过传播机制同步新区块数据，依靠验证机制确认交易合法性。公有链、联盟链和私有链在该层实现不同级别的中心化控制。

封装底层数据结构与安全技术，包含区块的链式结构、哈希函数、Merkle树、时间戳及非对称加密技术，确保数据不可篡改性和完整性。区块通过保存前序哈希值形成链式存储，交易数据采用双重加密保障隐私。

区块链技术

1、POW 工作量证明机制

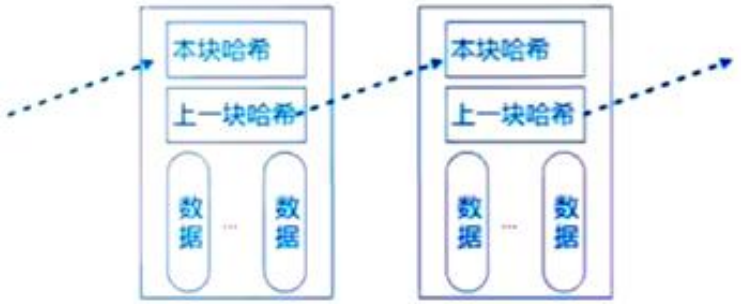
2、 pos 权益证明机制

3、 DPoS股份授权证明机制

4、区块链双花问题

5、挖矿

6、矿工



区块链技术

区块链的优缺点

区块链的优点

1.不可篡改的时间戳：可解决数据追踪与信息防伪问题
2.去中心化的分布式结构：现实中可节省大量的中介成本
3.安全的信任机制：可解决现今物联网技术的核心缺陷
4.灵活的可编程特性：可帮助规范现有市场秩序

区块链的缺点

1.高耗能问题
2.数据库存储空间问题
3.处理大规模交易的抗压能力问题
4.安全性问题

需求广泛：

区块链1.0：可编程货币：去中心化的数字支付系统，无障碍的价值转换；

区块链2.0：可编程金融：股票、清算、私募股权等众多金融领域；

区块链3.0：可编程社会：公证、仲裁、审计、物流、医疗、邮件等领域。

202505真题

第1问、区块链的6层是什么，各自功能（数据层、网络层、共识层、激励层、合约层、应用层）。

202505真题

【参考答案】：

数据层

封装底层数据结构与安全技术，包含区块的链式结构、哈希函数、Merkle树、时间戳及非对称加密技术，确保数据不可篡改性和完整性。区块通过保存前序哈希值形成链式存储，交易数据采用双重加密保障隐私。

网络层

采用P2P组网技术构建分布式自治系统，节点通过传播机制同步新区块数据，依靠验证机制确认交易合法性。公有链、联盟链和私有链在该层实现不同级别的中心化控制。

共识层

集成PoW、PoS、DPoS等算法解决分布式网络记账权分配问题，通过超过51%节点验证机制确保全网络账本一致性。共识机制直接影响系统的吞吐量与安全性。

激励层

设计经济模型驱动节点参与验证，如比特币的挖矿奖励和交易手续费机制。通过代币发行与分配规则维护网络生态的可持续性。

合约层

部署智能合约实现自动化执行，通过预编程脚本在满足条件时触发资产转移、合约清算等操作。以太坊等平台在该层扩展了图灵完备的编程能力。

应用层

面向具体场景开发DApp，涵盖金融支付（跨境结算）、供应链管理（农产品溯源）、数字身份等垂直领域。该层直接承载用户交互与业务逻辑实现。

202505真题

第2问：区块链应用在农产品的检验流程中，有三个角色，数据录入人，核对人和审核人，请说明三个角色在上链过程基本工作流程（可能是要说怎么上链确认方修改防抵赖？）

202505真题

参考答案：
1.信息填写人员
①登录区块链系统录入农产品基础数据（批次、产地、检测报告等）；
②上传原始凭证（如检测机构盖章文件）至IPFS分布式存储；
③调用智能合约生成初始哈希值将关键信息上链；
④系统自动生成带时间戳的区块链存证编号。

2.核对人员
验的数据包进行二级加密签名，触发智能合约进入审核队列。

3.审核人员
①调取前两级操作的全流程区块链日志；
②复核数据修改记录（需超过2/3节点共识)；
③最终确认时激活时间锁功能，使该批次数据进入只读状态；
④颁发可验证数字凭证（VC），同步至农业监管链节点。所有操作痕迹均通过非对称加密永久上链。

202505真题

第3问：智能合约在区块链中的主要作用主要体现在哪三个方面?

202505真题

【参考答案】：
智能合约是一种以代码形式编写的程序，存储在区块链上，用于自动执行合约条款，无需第三方介入。其核心作用包括自动化履约、确保交易透明性和不可算改性。

智能合约包含以下三方面：
1.目动化履约：智能合约可以在满足预设条件时自动执行交易或协议，减少人工十预和信任成本。例如，在预付式消费场景中，消费者预付的资金可以通过智能合约锁定，按照服务进度分阶段释放给商家，确保资金安全。

2.透明性和不可篡改性：智能合约的代码是公开的，任何人都可以验证其内容和执行结果。此外，由于区块链的分布式账本和共识机制，一旦合约被记录在区块上，其内容就无法被算改，保证了交易的不可算改性。

3.去中心化和安全性：智能合约依赖于区块链的去中心化架构和加密技术，确保交易的安全性和可信度。合约代码部署在链上节点，满足条件时由网络节点通过共识机制验证并执行，将结果记录至区块。

安全相关（作业）

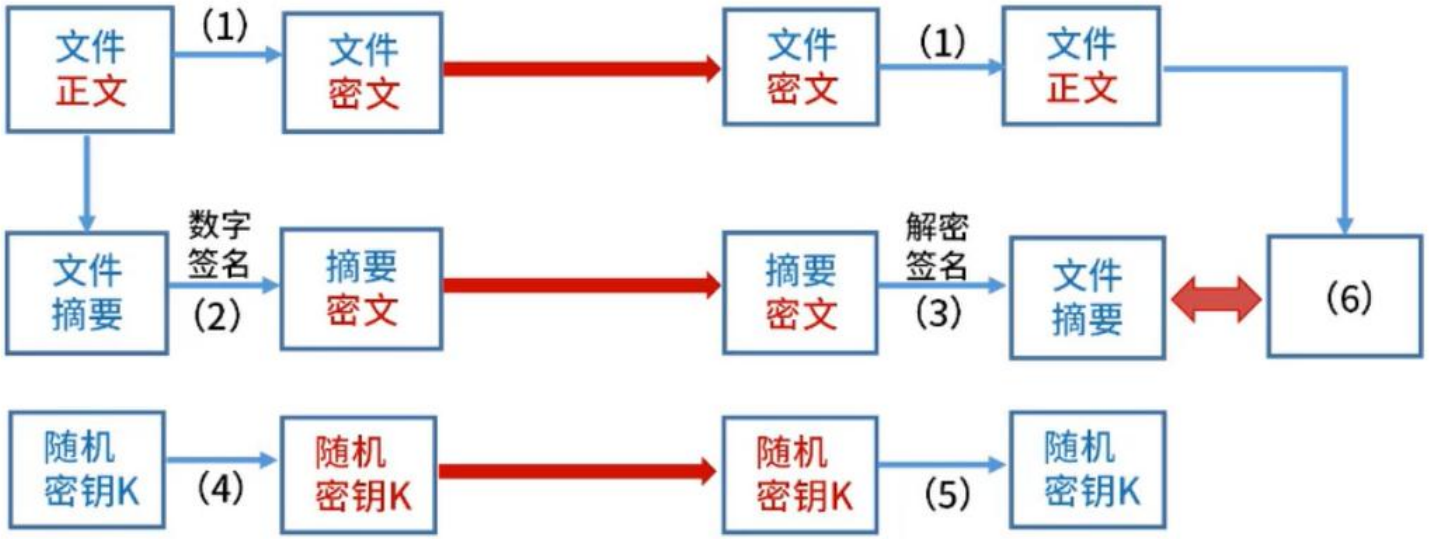
[问题1](13分)

某军区要架设一套内部文件安全传输系统，该文件以加密方式传输，支持最大2G的单个文件传输，为保障安全可靠性，发送者不可抵赖发送过的文件，若文件被第三方截获，第三方无法解密也无法篡改其内容。根据此需求，架构设计师王工设计了如下的安全架构:

请用以下选项补充图中缺失部分:

(a)发送方公钥Pa　(b) 发送方私钥Sa　(c) 接收方公钥Pb　(d) 接收方私钥Sb　(e)随机密钥K

(f)文件密文 (g)文件摘要



安全相关（作业）

[问题2](12分)

ISO安全体系结构包含的安全服务有:①鉴别服务;②访问控制服务;③数据保密性服务;④数据完整性服务;⑤抗否认性服务。请问:

(1)针对跨站伪造请求攻击可以采用哪种安全服务来解决或者缓解?

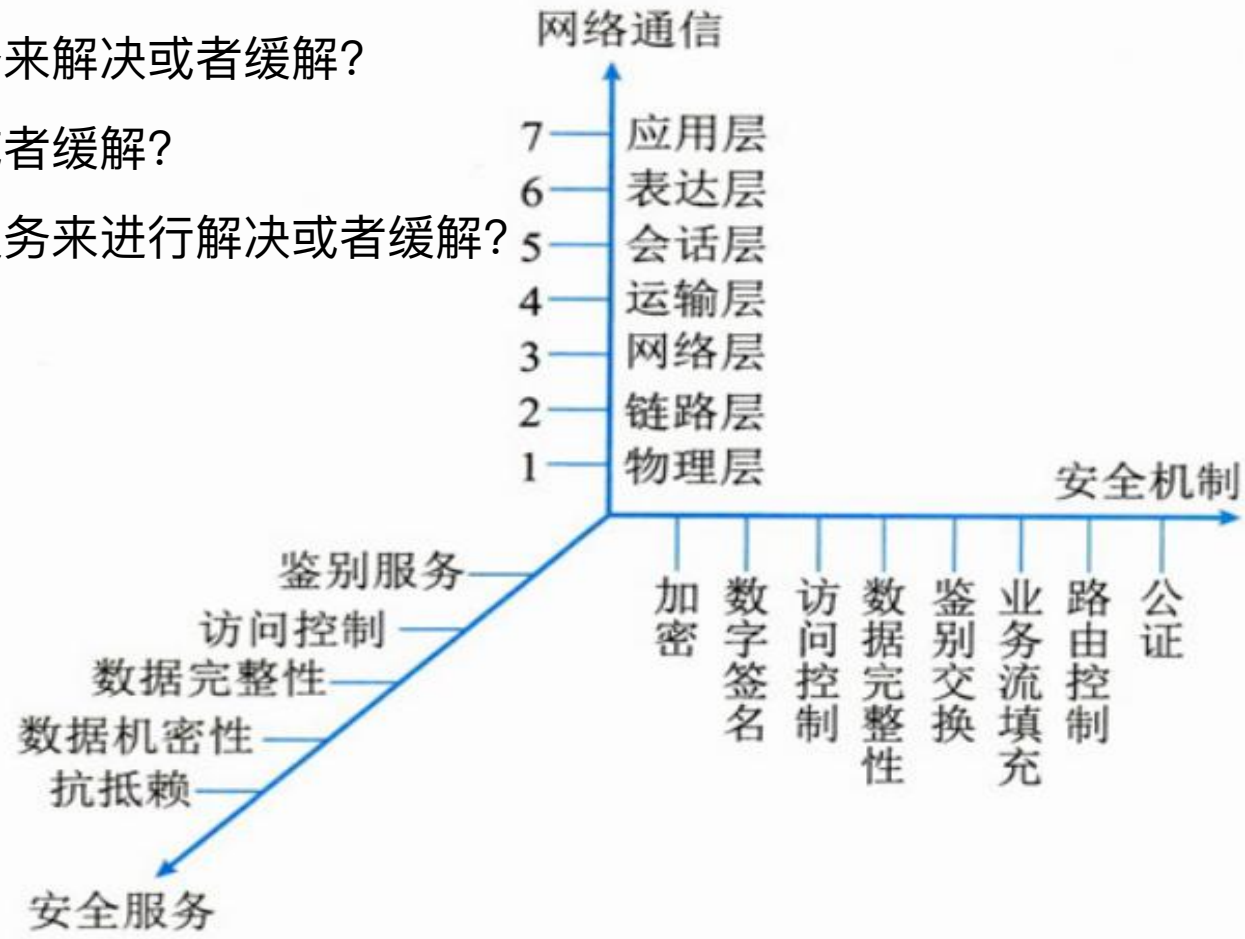
(2)针对口令明文传输漏洞攻击可以采用哪种安全服务来解决或者缓解?

(3)针对签名伪造攻击可以采用哪种安全服务来解决或者缓解?

(4)如果下载的软件被植入木马，可以采用哪种安全服务来进行解决或者缓解?

[参考答案][问题1]

(1)① (2)③ (3)⑤ (4)④



安全相关（作业）

试题二

阅读以下关于 web 系统设计的叙述，在答题纸上回答问题1至问题3。

【说明】

某公司拟开发一个食品供应链溯源系统，该系统需要提供从原材料供应商、加工商、物流、分销商、零售商、消费者的食品供应链全流程溯源。该公司组建了项目组，并召开了项目开发讨论会。会上，张工提出通过二维码扫描获取食品信息，采用中心化数据库作为数据存储媒介；李工提出使用中心化数据库容易产生数据信任、溯源追责困难等问题，建议建立区块链和数据库的映射存储，提供存储和查询操作功能，并提出采用数据接入层、数据核心层、应用表示层三层体系架构实现该食品溯源系统。

【问题1】（6分）

去中心化和开放性是区块链的重要特征，请用200字以内的文字简要说明什么是区块链的去中心化和开放性。

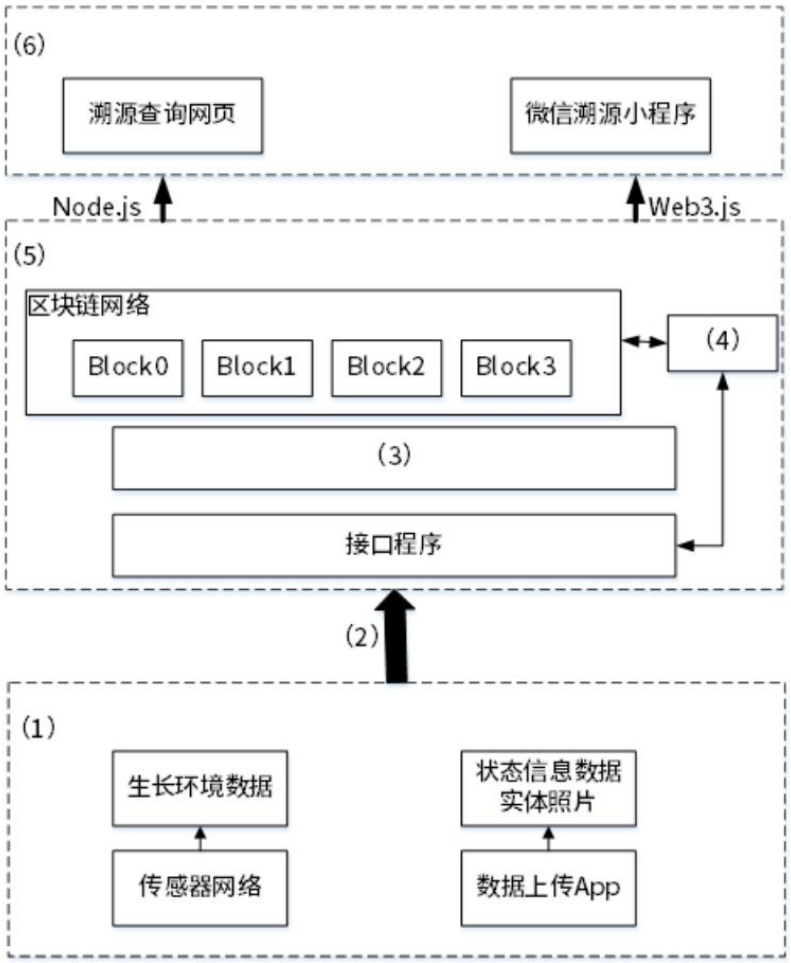
【问题2】（7分）

分布式交易账本、哈希散列函数、公私钥签名、时间戳就是区块链的核心技术，请从上述技术中选择两种最适合解决数据信任问题的技术，并用300字以内的文字说明原因。

【问题3】（12分）

根据李工的建议，该系统将采用三层架构。请从下面给出的（a）～（m）候选项中进行选择，补充完善图5-1中（1）～（6）处空白的内容，完成该系统的架构设计方案。

安全相关（作业）



(a) 数据接入层
(b) 智能合约
(c) Socket
(d) 4G/Wifi
(e) 应用表示层
(f) 数据库
(g) MVC
(h) 数据核心层
(i) 传感器网络
(j) 区块链网络
(k) 4G/Wifi
(l) JDBC
(m) 业务逻辑层

安全相关（作业）

答案：

【问题1】

1、去中心化

区块链采用了分布式计算和存储，不存在中心化的硬件或管理机构，因此使得任意节点的权利和义务都是均等的。

2、开放性

区块链的系统的一个开放性质的，除了交易各方的私有信息被加密外，区块链的数据对所有人公开的。

【问题2】

分布式交易账本、公私钥签名

- 分布式交易账本使交易账本在全网不止一份，而是有多份，当有人想篡改账本时，非常难以实现，所以能解决数据可信度问题。
- 公私钥签名是使用非对称加密机制，做签名，以验证持有人以及防止伪造的效果，这种技术也极难被破解，能验证持有人自然能一定程度解决数据可信度的问题。

【问题3】

(1) (a) 数据接入层 (2) (k) 4G/Wifi

(3) (b) 智能合约 (4) (f) 数据库

(5) (h) 数据核心层 (6) (e) 应用表示层

软件可靠性性定义

可靠性(Reliability)是指产品在规定的条件下和规定的时间内完成规定功能的能力。子特性：成熟性，容错性，易恢复性，可靠性的依从性。

影响软件可靠性的主要因素：软件的开发方法和开发环境、软件运行环境、软件系统（规模）、软件的内部结构、软件可靠性投入。

软件可靠性指标

可靠度是软件系统在规定的条件下、规定的时间内不发生失效的概率。

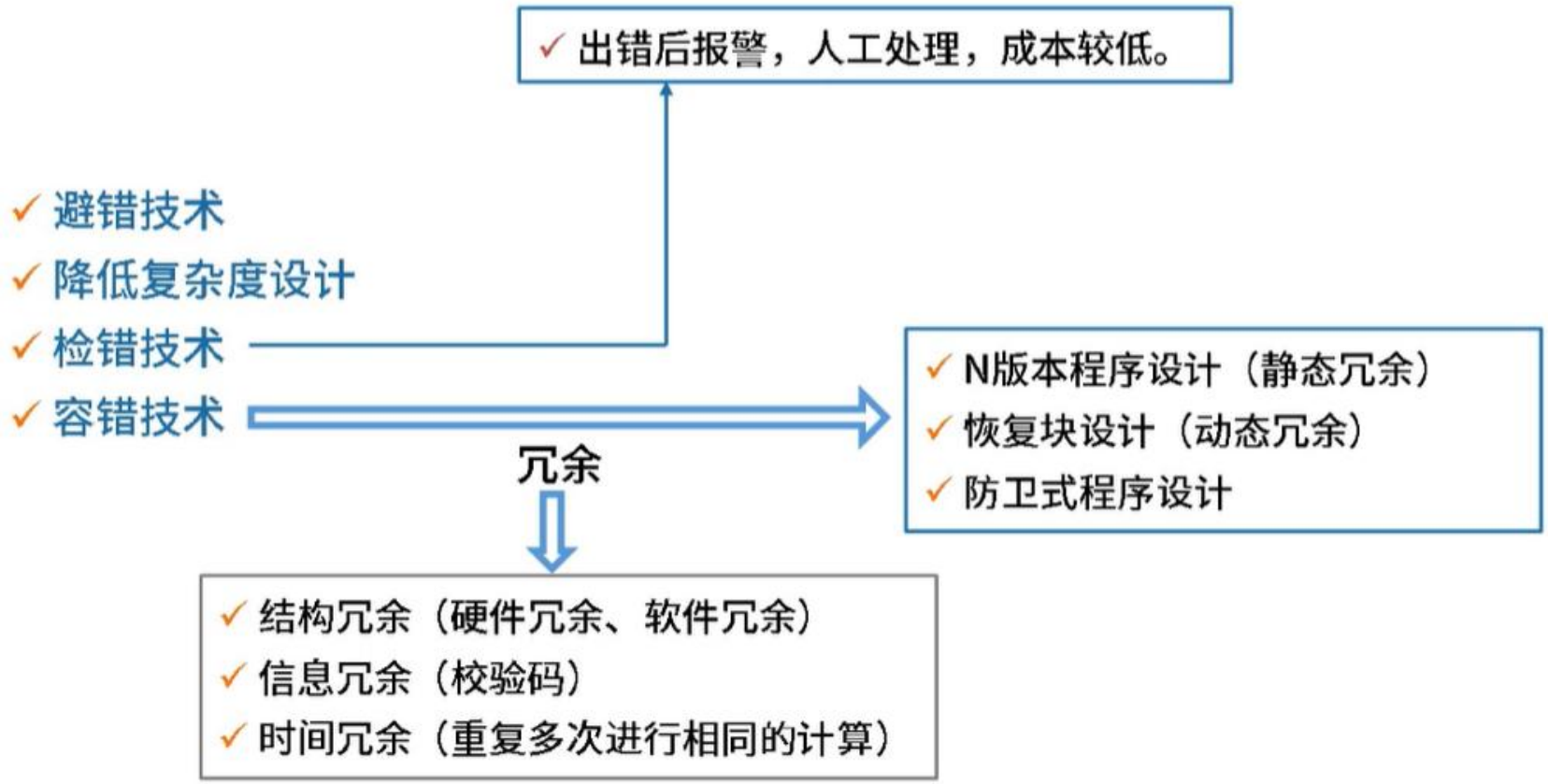
失效强度(Failure Intensity)的物理解释就是单位时间软件系统出现失效的概率。

可靠度为R(t)的系统平均失效前时间(Mean Time To Failure,MTTF)定义为从t=0时到故障发生时系统的持续运行时间的期望值。

平均恢复前时间(Mean Time To Restoration,MTTR)是随机变量恢复时间的期望值，就是从出现故障到修复成功中间的这段时间，它包括确认失效发生所必需的时间，记录所有任务的时间，还有将设备重新投入使用的时间。MTTR越短表示易恢复性越好。

MTBF(Mean Time Between Failures,平均故障间隔时间)定义为：失效或维护中所需的平均时间，包括故障时间以及检测和维护设备的时间。

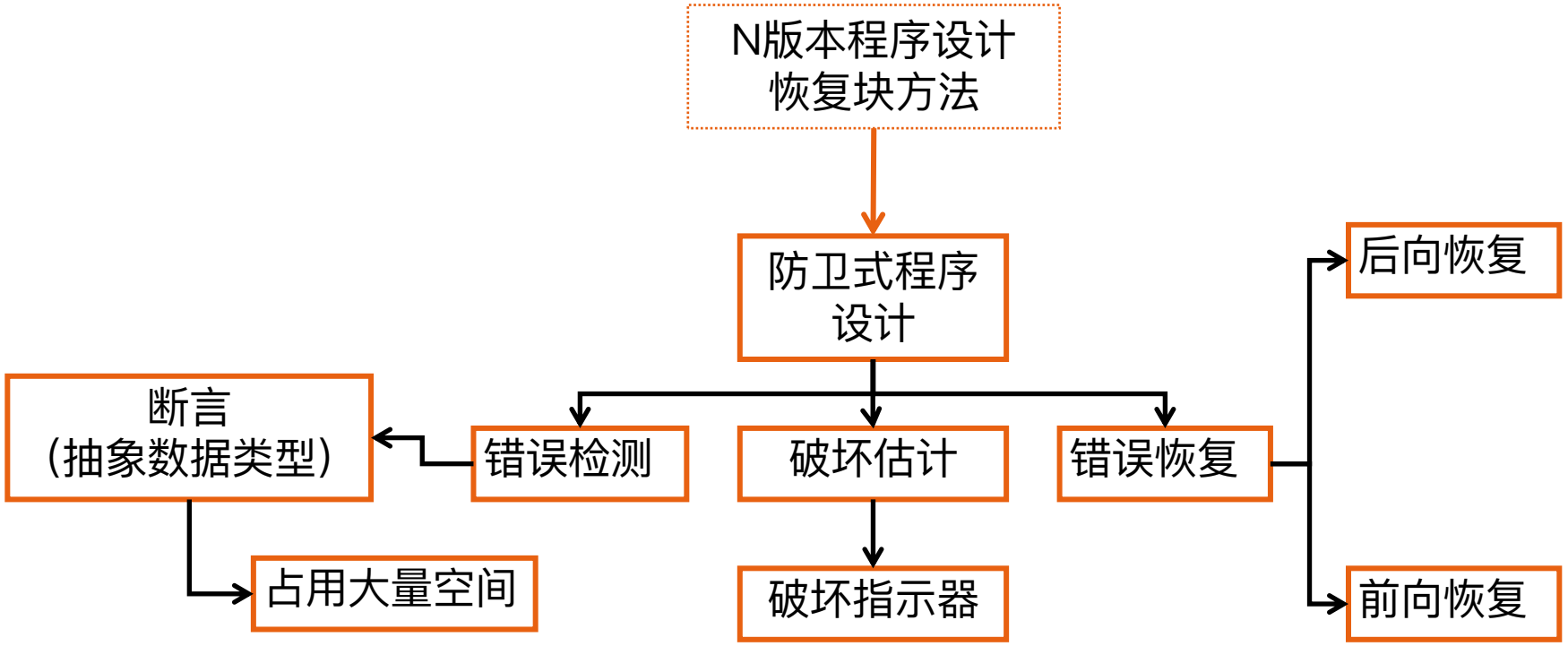
软件可靠性设计


✓ 出错后报警，人工处理，成本较低。
✓ 避错技术
✓ 降低复杂度设计
✓ 检错技术
✓ 容错技术
✓ N版本程序设计（静态冗余）
✓ 恢复块设计（动态冗余）
✓ 防卫式程序设计
冗余
✓ 结构冗余（硬件冗余、软件冗余）
✓ 信息冗余（校验码）
✓ 时间冗余（重复多次进行相同的计算）

软件容错技术

三 防卫式程序设计

防卫式程序设计是一种**不采用任何传统的容错技术就能实现软件容错的方法**，其实现策略包括**错误检测、破坏估计和错误恢复**三个方面。



软件容错技术

四 双机容错

通常在系统配置中可以采用相应的容错技术，通过系统的整体来提供相应的可靠性，
主要有双机热备技术和服务器集群技术

1）**双机热备技术**

- 双机热备模式（主系统 、备用系统）
- 双机互备模式（同时提供不同的服务，心不跳则接管）
- 双机双工模式（同时提供相同的服务，集群的一种）

2 ）**服务器集群技术**

集群技术是指一组相互独立的服务器在网络中组合成为单一的系统工作，并以单一系统的模式加以管理。此单一系统为客户工作站提供高可靠性的服务

软件可靠性模型分类

可靠性模型大致分为10种：

（1）种子法模型利用捕获一再捕获抽样技术估计程序中的错误数，在程序中预先有意“播种”一些设定的错误“种子”，然后根据测试出的原始错误数和发现的诱导错误的比例，来估计程序中残留的错误数。其优点是简便易行，缺点是诱导错误的“种子”与实际的原始错误之间的类比性估量困难。

（2）失效率类模型用来研究程序的失效率。

（3）曲线拟合类模型用回归分析的方法研究软件复杂性、程序中的缺陷数、失效率、失效间隔时间，包括参数方法和非参数方法两种。

（4）可靠性增长模型是预测软件在检错过程中的可靠性改进，用增长函数来描述软件的改进过程。

（5）程序结构分析模型是根据程序、子程序及其相互间的调用关系，形成一个可靠性分析网络。

（6）输入域分类模型选取软件输入域中的某些样本“点”运行程序，根据这些样本点在“实际”使用环境中的使用概率的测试运行时的成功/失效率，推断软件的使用可靠性。这类模型是输入域的概率分布的确定及对软件运行剖面的正确描述。

（7）执行路径分析方法类模型的分析方法与上面的模型相似，先计算程序各逻辑路径的执行概率和程序中错误路径的执行概率，再综合出该软件的使用可靠性。Shooman分解模型属于此类。

（8）非齐次泊松过程模型(NHPP)是以软件测试过程中单位时间的失效次数为独立泊松随机变量，来预测在今后软件的某使用时间点的累计失效数。

（9）马尔可夫过程模型包括完全改错的线性死亡模型。不完全改错的线性死亡模型。完全改错的非静态线性死亡模型。

（10）贝叶斯模型是利用失效率的试验前分布和当前的测试失效信息，来评估软件的可靠性。

可靠性相关案例模拟

试题三

阅读以下关于嵌入式系统可靠性设计方面的描述，回答问题1至问题3。

【说明】

某宇航公司长期从事宇航装备的研制工作，嵌入式系统的可靠性分析与设计已成为该公司产品研制中的核心工作，随着宇航装备的综合化技术发展，嵌入式软件规模发生了巨大变化，代码规模已从原来的几十万扩展到上百万，从而带来了由于软件失效而引起系统可靠性降低的隐患。公司领导非常重视软件可靠性工作，决定抽调王工程师等5人组建可靠性研究团队，专门研究提高本公司宇航装备的系统可靠性和软件可靠性问题，并要求在三个月内，给出本公司在系统和软件设计方面如何考虑可靠性设计的方法和规范。可靠性研究团队很快拿出了系统及硬件的可靠性提高方案，但对于软件可靠性问题始终没有研究出一种普遍认同的方法。

【问题1】（共9分）

请用200字以内文字说明系统可靠性的定义及包含的4个子特性，并简要指出提高系统可靠性一般采用哪些技术?

【问题2】（共8分）

王工带领的可靠性研究团队之所以没能快速取得软件可靠性问题的技术突破，其核心原因是他们没有搞懂高可靠性软件应具备的特点。软件可靠性一般致力于系统性地减少和消除对软件程序性能有不利影响的系统故障。除非被修改，否则软件系统不会随着时间的推移而发生退化。请根据你对软件可靠性的理解，给出表3-1所列出的硬件可靠性特征对应的软件可靠性特征之间的差异或相似之处，将答案写在答题纸上。

可靠性相关案例模拟

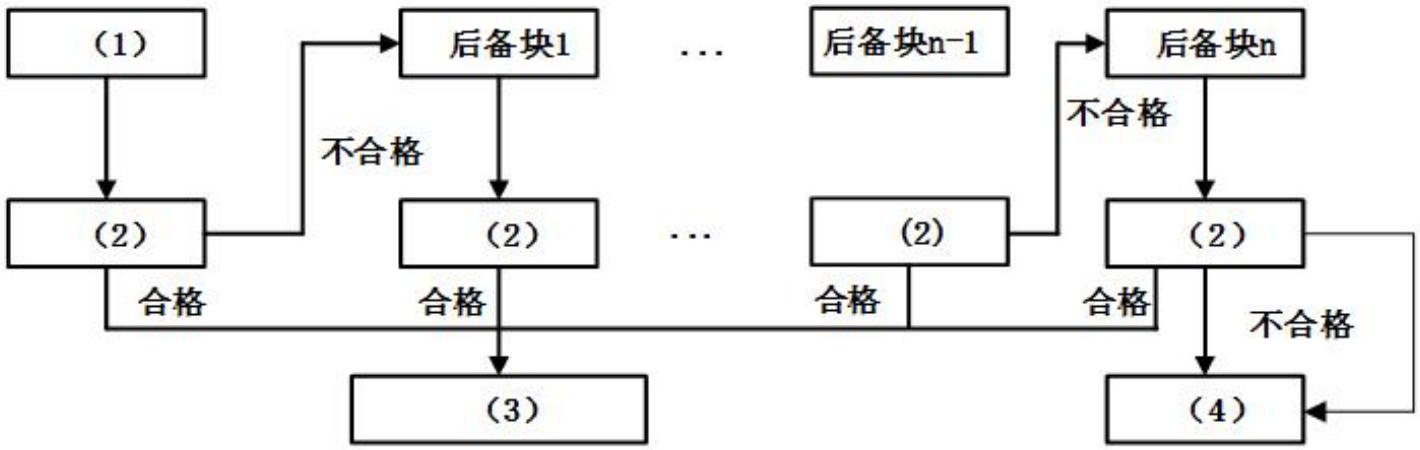
表3-1 硬件和软件可靠性对比

序号	硬件可靠性	软件可靠性
1	失效率服从浴缸曲线。老化状态类似于软件调试状态	（1）
2	即使不适用，材料劣化也会导致失效	（2）
3	硬件维修会恢复原始状态	（3）
4	硬件失效之前会有报警	（4）

【问题3】（共8分）

王工带领的可靠性研究团队在分析了大量相关资料基础上，提出软件的质量和可靠性必须在开发过程构建到软件中，也就是说，为了提高软件的可靠性，必须在需求分析、设计阶段开展软件可靠性筹划和设计。研究团队针对本公司承担的飞行控制系统制定出了一套飞控软件的可靠性设计要求。飞行控制系统是一种双余度同构型系统，输入采用了独立的两路数据通道，在系统内完成输入数据的交叉对比、表决制导率计算，输出数据的交叉对比、表决、输出等功能，系统的监控模块实现对系统失效或失步的检测与定位。其软件的可靠性设计包括恢复块方法和N版本程序设计方法。请根据恢复块方法工作原理完成图3–1,在(1)～(4)中填入恰当的内容。并比较恢复块方法与N版本程序设计方法，将比较结果(5)～(8)填入表3–2中。

可靠性相关案例模拟



恢复块方法图

	恢复块方法	N版本程序设计
硬件运行环境	单机	多机
错误检测方法	验证测试程序	(5)
恢复策略	(6)	向前恢复
实时性	(7)	(8)

表3-2 恢复块方法与N版本程序设计的比较

典型习题–案例模拟

答案

【问题1】

可靠性(Reliability)是指产品在规定的条件下和规定的时间内完成规定功能的能力。子特性：成熟性，容错性，易恢复性，可靠性的依从性。

提高可靠性的技术：

(1)N版本程序设计 (2)恢复块方法 (3)防卫式程序设计

(4)双机热备或集群系统

(5)冗余设计

【问题2】

(1)不考虑软件演化的情况下，失效率在统计上是非增的

(2)如果不使用该软件，永远不会发生失效

(3)软件维护会创建新的软件代码

(4)软件失效之前很少会有报警

【问题3】

(1)主块 (2)验证测试 (3)输出正确结果 (4)异常处理 (5)表决 (6)后向恢复 (7)差 (8)好

THANKS