系统架构设计师案例分析试题加答案（三）

系统架构设计师考试属于软考中的一项高级资格考试，考试分综合知识、案例分析和论文 3 个科目。下午的案例分析是考试的一大难点，希赛小编为大家整理了几道系统架构设计师案例分析试题，希望对大家有所帮助。

试题三

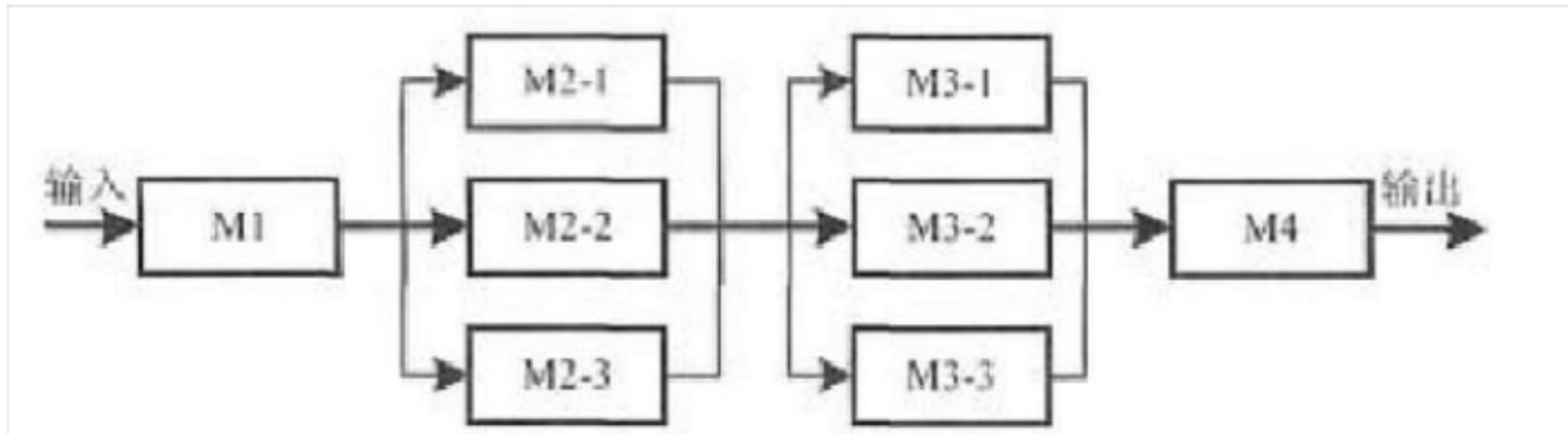
阅读以下信息系统可靠性问题的说明，回答问题。

某软件公司开发一项基于数据流的软件，其系统的主要功能是对输入数据进行多次分析、处理和加工，生成需要的输出数据。需求方对该系统的软件可靠性要求很高，要求系统能够长时间无故障运行。该公司将该系统设计交给王工负责。王工给出该系统的模块示意图如图所示。王工解释：只要各个模块的可靠度足够高，失效率足够低，则整个软件系统的可靠性是有保证的。

王工建议的软件系统模块示意图

李工对王工的方案提出了异议。李工认为王工的说法有两个问题：第一，即使每个模块的可靠度足够高，但是整个软件系统模块之间全部采用串联，则整个软件系统的可靠度明显下降。假设各个模块的可靠度均为 0.99 则整个软件系统的可靠度为 0.994 ≈0.96 ：第二，软件系统模块全部采用串联结构时，一旦某个模块失效，则

意味着整个软件系统失效。李工认为，应该在软件系统中采用冗余技术中的动态冗余或者软件容错的 N 版本程序设计技术，对容易失效或者非常重要的模块进行冗余设计，将模块之间的串联结构部分变为并联结构，来提高整个软件系统的可靠性。同时，李工给出了采用动态冗余技术后的软件系统模块示意图，如图所示。



李工建议的系统模块示意图

刘工建议，李工方案中 M1 和 M4 模块没有采用容错设计，但 M1 和 M4 发生故障有可能导致严重后果。

因此，可以在 M1 和 M4 模块设计上采用检错技术，在软件出现故障后能及时发现并报警，提醒维护人员进行处理。

注：假设各个模块的可靠度均为 0.99 。

1、在系统可靠性中，可靠度和失效率是两个非常关键的指标，请分别解释其含义。

2、请解释李工提出的动态冗余和 N 版本程序设计技术，给出图中模块 M2 采用图动态冗余技术后的可靠度。

请给出采用李工设计方案后整个系统可靠度的计算方法，并计算结果。

3、请给出检错技术的优缺点，并说明检测技术常见的实现方式和处理方式。

参考答案

1、可靠度就是系统在规定的条件下、规定的时间内不发生失效的概率。

失效率又称风险函数，也可以称为条件失效强度，是指运行至此刻系统未出现失效的情况下，单位时间系统出现失效的概率。

[解析]本题考查信息系统中可靠性的设计，是比较传统的题目，要求考生细心分析题目中所描述的内容。

本问题考查信息系统可靠性的两个基本指标 :可靠度和失效率。可靠性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。考虑到软件本身的复杂性，软件可靠性的定义是：在规定的条件下，在规定的时间内，软件不引起系统失效的概率。

在软件可靠性的定量描述中，软件可靠性可以基于使用条件、规定时间、系统输入、系统使用和软件缺陷等变量构建数学表达式，来对软件可靠性进行定量描述。相关概念有规定时间、失效概率、可靠度、失效强度、失效率、平均无失效时间等。其中可靠度是表示可靠性最直接的方式，是软件系统在规定的条件下、规定的实践内不发生失效的概率。而失效率又称风险函数，也可以称为条件失效强度，是指运行至此刻系统未出现失效的情况下，单位时间系统出现失效的概率。

2、动态冗余又称为主动冗余，它是通过故障检测、故障定位及故障恢复等手段达到容错的目的。其主要方式是多重模块待机储备，当系统检测到某工作模块出现错误时，就用一个备用的模块来替代它并重新运行。各备用模块在其待机时，可与主模块一样工作，也可以不工作。前者叫热备份系统(双重系统)，后者叫冷备份系统(双工系统、双份系统)。N 版本程序设计是一种静态的故障屏蔽技术，其设计思想是用 N 个具有相同功能的程序同时执行一项计算，结果通过多数表决来选择。其中 N 个版本的程序必须由不同的人独立设计，使用不同的方法、设计语言、开发环境和工具来实现，目的是减少 N 个版本的程序在表决点上相关错误的概率。

M2 采用动态冗余后的可靠度为：R=1-(1-0.99)3 ≈0.999999

李工的方案同时采用了串联和并联方式，其计算方法为首先计算出中间 M2 和 M3 两个并联系统的可靠度，再按照串联系统的计算方法计算出整个系统的可靠度。R=0.99 ×0.999999 ×0.999999 ×0.99 ≈0.98 本问题考查在常规的软件设计中，应用各种方法和技术，使程序设计在兼顾用户功能和性能需求的同时，全面满足软件的可靠性要求。常见的软件可靠性技术主要有容错设计、检错设计和降低复杂度设汁等技术。其中，容错设计技术主要有冗余设计、恢复块设计和 N 版本程序设计三种方法。①冗余设计冗余是指在正常系统运行所需的基础上加上一定数量的资源，包括信息、时间、硬件和软件。冗余是容错技术的基础，通过冗余资源的加入，可以使系统的可靠性得到较大的提高。主要的冗余技术有结构冗余(硬件冗余和

软件冗余)、信息冗余、时间冗余和冗余附加四种。结构冗余是常用的冗余技术，按其工作方式，可分为静态冗余、动态冗余和混合冗余三种。具体阐述如下。

·静态冗余。静态冗余又称为屏蔽冗余或被动冗余，常用的有三模冗余和多模冗余。静态冗余通过表决和比较来屏蔽系统中出现的错误。例如，三模冗余是对三个功能相同，但由不同的人采用不同的方法开发出的模块的运行结果进行表决，以多数结果作为系统的最终结果。即如果模块中有一个出错，这个错误能够被其他模块的正确结果“屏蔽”。由于无须对错误进行特别的测试，也不必进行模块的切换就能实现容错，故称为静态容错。

·动态冗余。动态冗余又称为主动冗余，它是通过故障检测、故障定位及故障恢复等手段达到容错的目的。其主要方式是多重模块待机储备，当系统检测到某工作模块出现错误时，就用一个备用的模块来顶替它并重新运行。各备用模块在其待机时，可与主模块一样工作，也可不工作。前者叫做热备份系统(双重系统)，后者叫做冷备份系统(双工系统、双份系统)。在热备份系统中，两套系统同时、同步运行，当联机子系统检测到错误时，退出服务进行检修，而由热备份子系统接替:[作，备用模块在待机过程中其失效率为 0；处于冷备份的子系统平时停机或者运行与联机系统无关的运算，当联机子系统产生故障时，人工或自动进行切换，使冷备份系统成为联机系统。在运行冷备份时，不能保证从系统断点处精确地连续工作，因为备份机不能取得原来的机器上当前运行的全部数据。

·混合冗余。混合冗余技术是将静态冗余和动态冗余结合起来，且取两者之长处。它先使用静态冗余中的故障屏蔽技术，使系统免受某些可以被屏蔽的故障的影响。而对那些无法屏蔽的故障则采用主动冗余中的故障检测、故障定位和故障恢复等技术，并且对系统可以做重新配置。因此，混合冗余的效果要大大优于静态冗余和动态冗余。然而，由于混合冗余既要有静态冗余的屏蔽功能，又要有动态冗余的各种检测和定位等功能，它的附加硬件的开销是相当大的，所以混合冗余的成本很高，仅在对可靠性要求极高的场合中采用。

·信息冗余。信息冗余是在实现正常功能所需要的信息外，再添加一些信息，以保证运行结果正确性的方法。例如，检错码和纠错码就是信息冗余的例子。这种冗余信息的添加方法是按照一组预定的规则进行的。符合添加规则而形成的带有冗余信息的字称为码字，而那些虽带有冗余信息但不符合添加规则的字则称为非码字。当系统出现故障时，可能会将码字变成非码字，于是在译码过程中会将引起非码字的故障检测出来，这就是检错码的基本思想。纠错码则不仅可以将错误检测出来，还能将由故障引起的非码字纠正成正确的码字。

由此可见，信息冗余的主要任务在于研究出一套理想的编码和译码技术来提高信息冗余的效率。编码技术中应用最广泛的是奇偶校验码、海明校验码和循环冗余校验码。

·时间冗余。时间冗余是以时间(即降低系统运行速度)为代价以

减少硬件冗余和信息冗余的开销来达到提高可靠性的目的。在某些实际应用中，硬件冗余和信息冗余的成本、体积、功耗、重量等开销可能过高，而时间并不是太重要的因素时，可以使用时间冗余。时间冗余的基本概念是重复多次进行相同的计算，或称为重复执行(复执)，以达到故障检测的目的。实现时间冗余的方法很多，但是其基本思想不外乎是对相同的计算任务重复执行多次，然后将每次的运行结果存放起来再进行比较。若每次的结果相同，则认为无故障；若存在不同的结果，则说明检测到了故障。不过，这种方法往往只能检测瞬时性故障而不宜检测永久性的故障。

·冗余附加。冗余附加是指为实现上述冗余技术所需的资源和技术，包括程序、指令、数据，以及存放和调用它们的空间等。动态冗余又称为主动冗余，它是通过故障检测、故障定位及故障恢复等手段达到容错的目的。其主要方式是多重模块待机储备，当系统检测到某工作模块出现错误时，就用一个备用的模块来顶替它并重新运行。各备用模块在其待机时，可与主模块一样工作，也可不工作。前者叫做热备份系统(双重系统)，后者叫做冷备份系统(双工系统、双份系统)。在热备份系统中，两套系统同时、同步运行，当联机子系统检测到错误时，退出服务进行检修，而由热备份子系统接替工作，备用模块在待机过程中其失效率为 0；处于冷备份的子系统平时停机或者运行与联机系统无关的运算,当联机子系统产生故障时，人工或自动进行切换，使冷备份系统成为联机系统。在运行冷备份时，不能保证从系统断点处精确地连续工作，因为备份机不能取得

原来的机器上当前运行的全部数据。

②恢复块设计恢复块设计是一种动态的故障屏蔽技术，采用后向恢复策略。恢复块设计提供具有相同功能的主块和几个后备块，一个块就是一个执行完整的程序段，主块首先投入运行，结束后进行验证测试，如果没有通过验证测试，系统经现场恢复后由后备块1运行。后备块1运行结束后也进行验证测试，如果没有通过验证测试，系统经现场恢复后由后备块2运行。重复这一过程，可以重复到耗尽所有的后备块，或者某个程序故障行为超出了预料，从而导致不可恢复的后果。在程序设计时，应保证实现主块和后备块之间的独立性，避免相关错误的产生，使主块和后备块之间的共性错误降到最低程度。

恢复块设计依赖于一个裁决者，那就是验证测试(可接受测试)，由它来决定同一算法不同实现的计算结果是否正确。带有恢复块的系统被分成故障可恢复的块。整个系统就由这些容错块组成。每一块至少包含一个一级模块、一个二级模块和一个例外处理模块，以及一个验证测试模块。验证测试模块完成故障检测功能，它本身的故障对恢复块方法而言是共性的，因此，必须确保它的正确性。同时，验证测试模块是为了确定模块计算结果的正确性，它必须尽可能的简单。③N版本程序设计N版本程序设计是一种静态的故障屏蔽技术，其设计思想是用N个具有相同功能的程序同时执行一项计算，结果通过多数表决来选择。其中N个版本的程序必须由不同的人独立设计，使用不同的方法、设计语言、开发环境和工具来实现，

目的是减少 N 个版本的程序在表决点上相关错误的概率。④可靠性计算计算机系统是一个复杂系统，影响其可靠性的因素很多，很难直接进行可靠性分析，往往需要建立对应的数学模型。组合模型是分析系统可靠性的一种常用方法。组合模型下可靠度的计算方法如下。串联系统：R=R1 ×R2 ×……×Rn 并联系统：R=1-(1-R1) ×(1-R2) ×……×(1-Rn) 串联和并联混合系统则根据实际情况，灵活运用上述两个计算公式。M2 采用动态冗余后，成为并联系统，则其可靠度为：R=1-(1-0.99)3=0.999999 。李工给出的方案同时采用了串联和并联方式，其计算方法为首先计算出中间 M2 和 M3 两个并联系统的可靠度,再按照串联系统的计算方法计算出整个系统的可靠度。R=0.99 ×0.999999 ×0.999999 ×0.99=0.98

3、检错技术实现的代价一股低于容错技术和冗余技术，但有一个明显的缺点，就是不能自动解决故障，出现故障后如果不进行人工干预，将最终导致软件系统不能正常运行。检错技术常见的实现方式：最直接的一种实现方式是判断返回结果，如果返回结果超出正常范围，则进行异常处理；计算运行时间也是一种常用技术，如果某个模块或函数运行时间超过预期时间，可以判断出现故障；还有置状态标志位等多种方法，自检的实现方式需要根据实际情况来选用。检错技术的处理方式，大多数都采用“查处故障-停止软件运行-报警”的处理方式。但根据故障的不同情况，也有采用不停止或部分停止软件系统运行的情况，这一般由故障是否需要实时处理来决定。本问题考查软件可靠性设计中的检错技术。检错技术常见

的实现方式有很多种，最直接的一种实现方式是判断返回结果，如果返回结果超出正常范围，则进行异常处理；计算运行时间也是一种常用技术，如果某个模块或函数运行时间超过预期时间，可以判断出现故障；还有置状态标志位等多种方法，自检的实现方式需要根据实际情况来选用。检错技术的处理方式也有多种，大多数都采用“查处故障-停止软件运行-报警”的处理方式。但根据故障的不同情况，也有采用不停止或部分停止软件系统运行的情况，这一般由故障是否需要实时处理来决定。检错技术实现的代价一般低于容错技术和冗余技术，但有一个明显的缺点，就是不能自动解决故障，出现故障后如果不进行人工干预，将最终导致软件系统不能正常运行。