2019 年系统架构师考试科目二：案例分析

1、阅读以下关于软件架构设计与评估的叙述，在答题纸上回答问题 1 和问题 2。

某电子商务公司为了更好地管理用户，提升企业销售业绩，拟开发一套用户管理系统。该系统的基本功能是根据用户的消费级别、消费历史、信用情况等指标将用户划分为不同的等级，并针对不同等级的用户提供相应的折扣方案。在需求分析与架构设计阶段，电子商务公司提出的需求、质量属性描述和架构特性如下：

(a) 用户目前分为普通用户、银卡用户、金卡用户和自金用户四个等级，后续需要能够根据消费情况进行动态调整；

(b)系统应该具备完善的安全防护措施，能够对黑客的攻击行为进行检测与防御；

(c)在正常负载情况下，系统应在 0.5 秒内对用户的商品查询请求进行响应；

(d)在各种节假日或公司活动中，针对所有级别用户，系统均能够根据用户实时的消费情况动态调整折扣力度；

(e)系统主站点断电后，应在 5 秒内将请求重定向到备用站点；

(f)系统支持中文昵称，但用户名要求必须以字母开头，长度不少于 8 个字符；

(g)当系统发生网络失效后，需要在 15 秒内发现错误并启用备用网络；

(h)系统在展示商品的实时视频时，需要保证视频画面具有 1024×768 像素的分辨率，40 帧/秒的速率:

(i)系统要扩容时，应保证在 10 人月内完成所有的部署与测试工作；

(j)系统应对用户信息数据库的所有操作都进行完整记录；

(k)更改系统的 Web 界面接口必须在 4 人周内完成；

(l)系统必须提供远程调试接口，并支持远程调试。在对系统需求、质量属性描述和架构特性进行分析的基础上，该系统架构师给出了两种候选的架构设计方案，公司目前正在组织相关专家对系统架构进行评估。

【问题 1】(13 分)

针对用户级别与折扣规则管理功能的架构设计问题，李工建议采用面向对象的架构风格，而王工则建议采用基于规则的架构风格。请指出该系统更适合采用哪种架构风格，并从用户级别、折扣规则定义的灵活性、可扩展性和性能三个方面对这两种架构风格进行比较与分析，填写表中的(1)~(3)空白处。

架构风格名称	灵活性	可扩展性	性能
面向对象	将用户级别、折扣规则等封装为对象，在系统启动时加载	（2）	（3）
基于规则	（1）	加入新的用户级别和折扣规则时只需要定义新的规则，解释规则即可进行扩展。	需要对用户级别与折扣规则进行实时解释、性能较差。

【问题 1 解析】

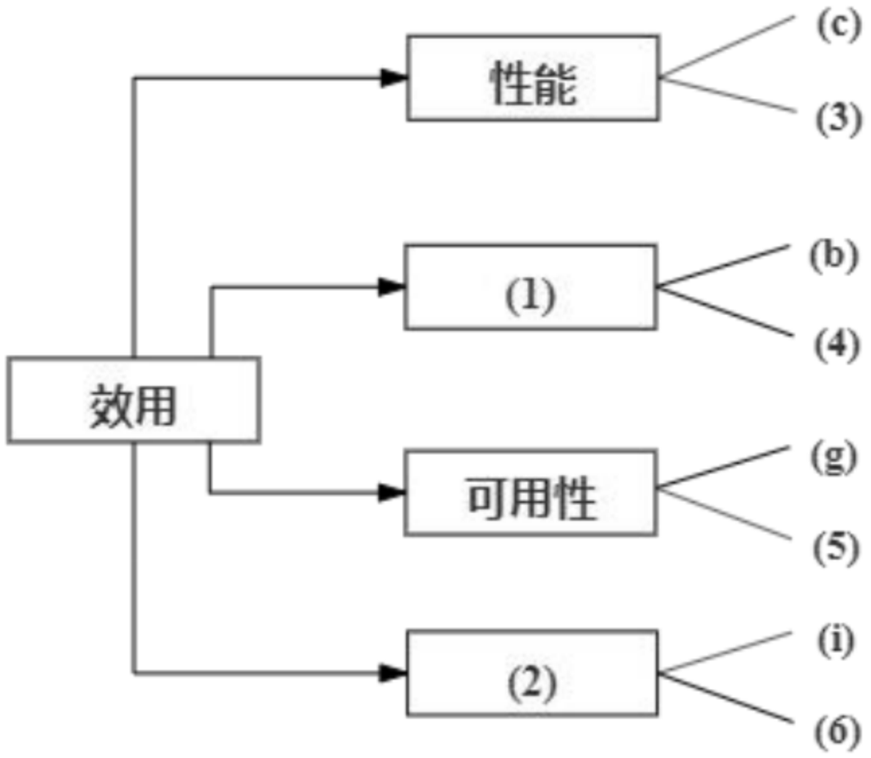
用户级别与折扣规则管理功能更适合采用基于规则的架构风格。

（1）将用户级别、折扣规则等描述为可动态改变的规则数据;

（2）加入新的用户级别和折扣规则时需要重新定义新的对象，并需要重启系统;
（3）用户级别和折扣规则已经在系统内编码，可直接运行，性能较好。

【问题 2】(12 分)

在架构评估过程中，质量属性效用树(utilitytree)是对系统质量属性进行识别和优先级排序的重要工具。请将合适的质量属性填入图中(1)、(2)空白处，并选择题干描述的(a)~(l)填入(3)~(6)空白处，完成该系统的效用树。



【问题 2 解析】

(1)—安全性
(2)—可修改性
(3)—(h)
(4)—(j)
(5)—(e)
(6)—(k)

2、阅读下列说明，回答问题 1 至问题 3，将解答填入答题纸的对应栏内。

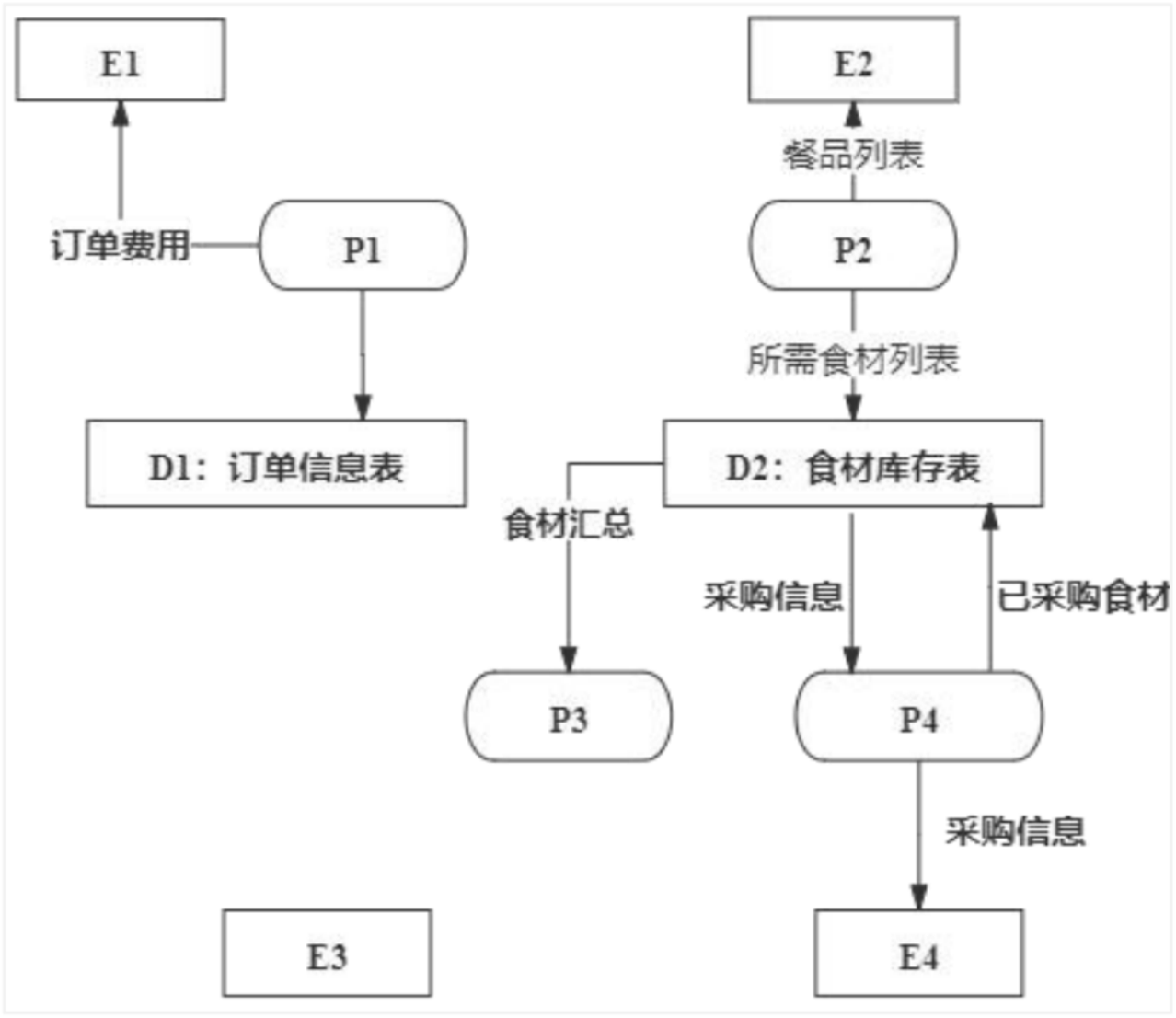
某软件企业为快餐店开发一套在线订餐管理系统，主要功能包括：

(1) 在线订餐：已注册客户通过网络在线选择快餐店所提供的餐品种类和数量后提交订单，系统显示订单费用供客户确认，客户确认后支付订单所列各项费用。

(2) 厨房备餐：厨房接收到客户已付款订单后按照订单餐品列表选择各类食材进行餐品加工。

(3) 食材采购：当快餐店某类食材低于特定数量时自动向供应商发起采购信息，包括食材类型和数量，供应商接收到采购信息后按照要求将食材送至快餐店并提交已采购的食材信息，系统自动更新食材库存。

(4) 生成报表：每个周末和月末，快餐店经理会自动收到系统生成的统计报表，报表中详细列出了本周或本月订单的统计信息以及库存食材的统计信息。现采用数据流图对上述订餐管理系统进行分析与设计，系统未完成的 0 层数据流图如图所示。



【问题 1】(8 分)

根据订餐管理系统功能说明，请在图 2-1 所示数据流图中给出外部实体 E1-E4 和加工 P1-P4 的具体名称。

【问题 1 解析】

E1：客户　　E2：厨房　　E3：经理　　E4：供应商

P1：在线订餐　　P2：厨房备餐　　P3：生成报表　　P4：食材采购

【问题 2】(8 分)

根据数据流图规范和订餐管理系统功能说明，请说明在图 2-1 中需要补充哪些数据流可以构造出完整的 0 层数据流图。

【问题 2 解析】

(1) 增加 E1 到 P1 数据流“餐品订单";

(2) 增加 P1 到 P2 数据流“餐品订单";

(3) 增加 D1 到 P3 数据流“订单汇总";

(4) 增加 P3 到 E3 数据流“统计报表”。

【问题 3】(9 分)

根据数据流图的含义，请说明数据流图和系统流程图之间有哪些方面的区别。

【问题 3 解析】

(1) 数据流图中的处理过程可并行；系统流程图在某个时间点只能处于一个处理过程。

(2) 数据流图展现系统的数据流；系统流程图展现系统的控制流。

(3) 数据流图展现全局的处理过程，过程之间遵循不同的计时标准；系统流程图中处理过程遵循一致的计时标准。

3、阅读以下关于嵌入式系统开放式架构相关技术的描述，在答题纸上回答问题 1 至问题 3。

信息物理系统(CyberPhysicalSystemsCPS)技术已成为未来宇航装备发展的重点关键技术之一。某公司长期从事嵌入式系统的研制工作，随着公司业务范围不断扩展，公司决定进入宇航装备的研制领域。为了做好前期准备，公司决定让王工程师负责编制公司进军宇航装备领域的战略规划。王工经调研和分析，认为未来宇航装备将向着网络化、智能化和综合化的目标发展，CPS 将会是宇航装备的核心技术，公司应构建基于 CPS 技术的新产品架构，实现超前的技术战略储备。

【问题 1】(9 分)

通常 CPS 结构分为感知层、网络层和控制层，请用 300 字以内文字说明 CPS 的定义，并简要说明各层的含义。

【问题 1 解析】

信息物理系统(CyberPhysicalSystems，CPS)作为计算进程和物理进程的统一体，是集计算、通信与控制于一体的下一代智能系统。信息物理系统通过人机交互接口实现和物理进程的交互，使用网络化空间，以远程的、可靠的、实时的、安全的、协作的方式操控一个物理实体。

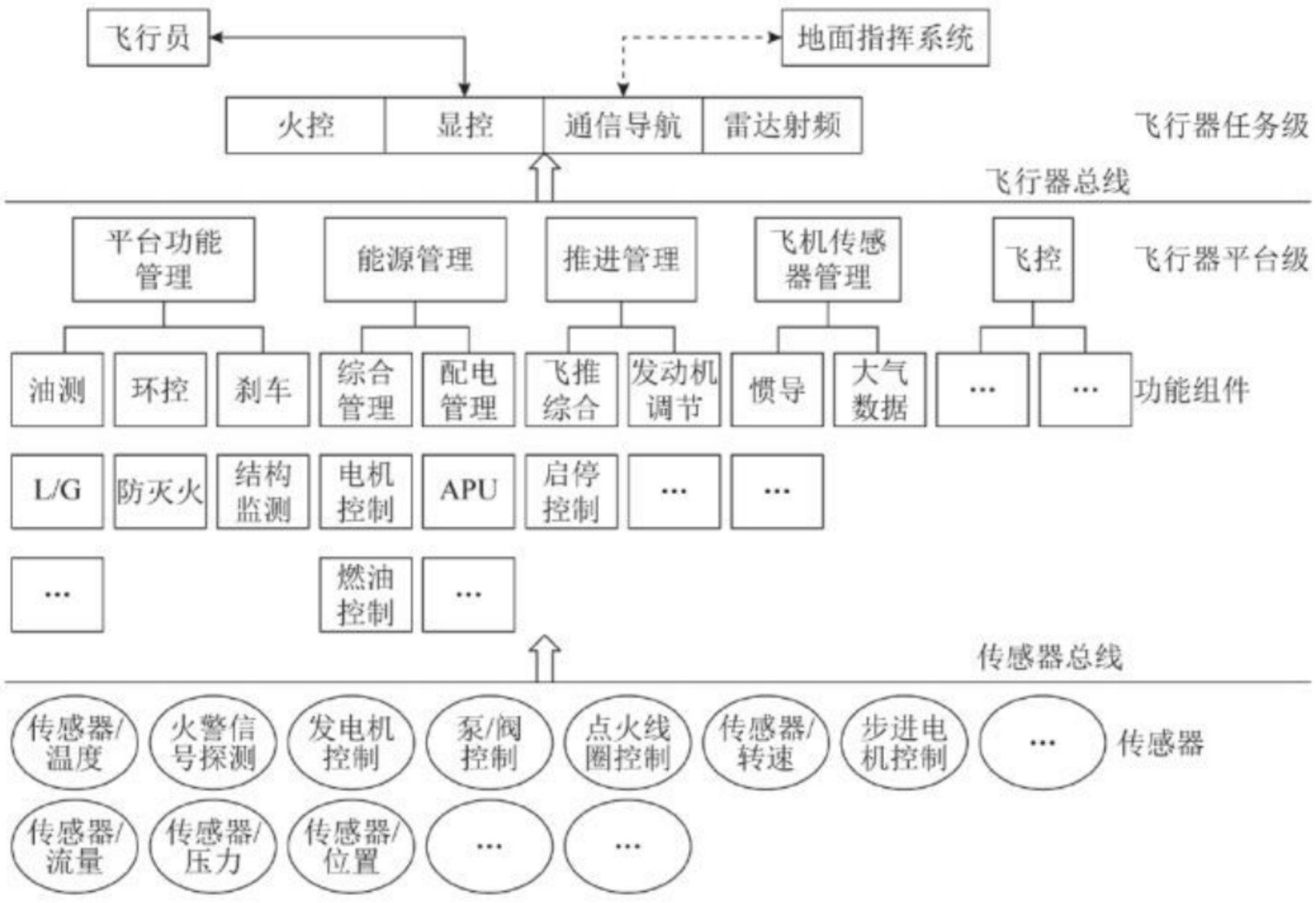
感知层：主要由传感器、控制器和采集器等设备组成，它属于信息物理系统中的末端设备。

网络层：主要是连接信息世界和物理世界的桥梁，实现的是数据传输，为系统提供实时的网络服务，保证网络分组传输的实时可靠。

控制层：主要是根据认知结果及物理设备传回来的数据进行相应的分析，将相应的结果返回给客户端。

【问题 2】(10 分)

王工在提交的战略规划中指出：飞行器中的电子设备是一个大型分布式系统，其传感器、控制器和采集器分布在飞机各个部位，相互间采用高速总线互连，实现子系统间的数据交换，而飞行员或地面指挥系统根据飞行数据的汇总决策飞行任务的执行。图给出了飞行器系统功能组成图。请参考图给出的功能图，依据你所掌握的 CPS 知识，说明以下所列的功能分别属于 CPS 结构中的哪层，哪项功能不属于 CPS 任何一层。



1、飞行传感器管理
2、步进电机控制
3、显控
4、发电机控制
5、环控
6、配电管理
7、转速传感器
8、传感器总线
9、飞行员
10、火警信号探测

【问题 2 解析】

感知层：2、4、7、10
网络层：8
控制层：1、3、5、6
不属于 CPS 结构中的功能：9

【问题 3】(6 分)

王工在提交的战略规划中指出：未来宇航领域装备将呈现网络化、智能化和综合化等特征，形成集群式的协同能力，安全性尤为重要。在宇航领域的 CPS 系统中，不同层面上都会存在一定的安全威胁。请用 100 字以内文字说明 CPS 系统会存在哪三类安全威胁并对每类安全威胁至少举出两个例子说明。

【问题 3 解析】

(1) 感知层安全威胁：感知数据破坏、信息窃听、节点捕获。
(2) 网络层安全威胁：拒绝服务攻击、选择性转发、方向误导攻击。
(3) 控制层安全威胁：用户隐私泄露、恶意代码、非授权访问。

4、阅读以下关于分布式数据库缓存设计的叙述，在答题纸上回答问题 1 至问题 3

某初创企业的主营业务是为用户提供高度个性化的商品订购业务，其业务系统支持 PC 端、手机 App 等多种访问方式。系统上线后受到用户普遍欢迎，在线用户数和订单数量迅速增长，原有的关系数据库服务器不能满足高速并发的业务要求。

为了减轻数据库服务器的压力，该企业采用了分布式缓存系统，将应用系统经常使用的数据放置在内存，降低对数据库服务器的查询请求，提高了系统性能。在使用缓存系统的过程中，企业碰到了一系列技术问题。

【问题 1】(11 分)

该系统使用过程中，由于同样的数据分别存在于数据库和缓存系统中，必然会造成数据同步或数据不一致性的问题。该企业团队为解决这个问题，提出了如下解决思路：应用程序读数据时，首先读缓存，当该数据不在缓存时，再读取数据库;应用程序写数据时，先写缓存，成功后再写数据库：或者先写数据库，再写缓存。王工认为该解决思路并未解决数据同步或数据不一致性的问题.请用 100 字以内的文字解释其原因。王工给出了一种可以解决该问题的数据读写步骤如下：

读数据操作的基本步骤：

1、根据 key 读缓存；
2、读取成功则直接返回；
3、若 key 不在缓存中时，根据 key(a);
4、读取成功后，(b)；
5、成功返回。

写数据操作的基本步骤：

1、根据 key 值写(c)；
2、成功后(d)；

3、成功返回。

请填写完善上述步骤中(a)—(d)处的空白内容。

【问题 1 解析】

存在双写不一致问题，在写数据时，可能存在缓存写成功，数据库写失败，或者反之，从而造成数据不一致。当多个请求发生时也可能产生读写冲突的并发问题

(a) 从数据库中读取数据或读数据库；

(b) 更新缓存中 key 值或更新缓存；

(c) 数据库；

(d) 删除缓存 key 或使缓存 key 失效或更新缓存(key 值)。

【问题 2】(8 分)

缓存系统一般以 key/value 形式存储数据，在系统运维中发现，部分针对缓存的查询，未在缓存系统中找到对应的 key，从而引发了大量对数据库服务器的查询请求，最严重时甚至导致了数据库服务器的宕机。经过运维人员的深入分析，发现存在两种情况：

(1) 用户请求的 key 值在系统中不存在时，会查询数据库系统，加大了数据库服务器的压力；

(2)系统运行期间，发生了黑客攻击，以大量系统不存在的随机 key 发起了查询请求，从而导致了数据库服务器的宕机。经过研究，研发团队决定，当在数据库中也未查找到该 key 时，在缓存系统中为 key 设置空值，防止对数据库服务器发起重复查询。请用 100 字以内文字说明该设置空值方案存在的问题，并给出解决思路。

【问题 2 解析】

存在问题：不在系统中的 key 值是无限的，如果均设置 key 值为空，会造成内存资源的极大浪费，引起性能急剧下降。

解决思路：查询缓存之前，对 key 值进行过滤，只允许系统中存在的 key 进行后续操作(例如采用 key 的 bitmap 进行过滤)。

【问题 3】（6 分）

缓存系统中的 key 一般会存在有效期，超过有效期则 key 失效;有时也会根据 LRU 算法将某些 key 移出内存。当应用软件查询 key 时，如 key 失效或不在内存，会重新读取数据库，并更新缓存中的 key。

运维团队发现在某些情况下，若大量的 key 设置了相同的失效时间，导致缓存在同一时刻众多 key 同时失效，或者瞬间产生对缓存系统不存在 key 的大量访问，或者缓存系统重启等原因，都会造成数据库服务器请求瞬时爆量，引起大量缓存更新操作，导致整个系统性能急剧下降，进而造成整个系统崩溃。

请用 100 字以内文字，给出解决该问题的两种不同思路。

【问题 3 解析】

思路 1：缓存失效后，通过加排它锁或者队列方式控制数据库写缓存的线程数量，使得缓存更新串行化；

思路 2：给不同 key 设置随机或不同的失效时间，使失效时间的分布尽量均匀；

思路 3：设置两级或多级缓存，避免访问数据库服务器。

5、阅读以下关于 Web 系统架构设计的叙述，在答题纸上回答问题 1 至问题 3。

【题目】

某公司拟开发一个物流车辆管理系统，该系统可支持各车辆实时位置监控、车辆历史轨迹管理、违规违章记录管理、车辆固定资产管理、随车备品及配件更换记录管理、车辆寿命管理等功能需求。其非功能性需求如下：

(1) 系统应支持大于 50 个终端设备的并发请求；

(2) 系统应能够实时识别车牌，识别时间应小于 1s；

(3) 系统应 7×24 小时工作；

(4) 具有友好的用户界面；

(5) 可抵御常见 SQL 注入攻击：；

(6) 独立事务操作响应时间应小于 3s；

(7) 系统在故障情况下，应在 1 小时内恢复；

(8) 新用户学习使用系统的时间少于 1 小时。

面对系统需求，公司召开项目组讨论会议，制订系统设计方案，最终决定基于分布式架构设计实现该物流车辆管理系统，应用 Kafka、Redis 数据缓存等技术实现对物流车辆自身数据、业务数据进行快速、高效的处理。

【问题 1】(4 分)

请将上述非功能性需求(1)～(8)归类到性能、安全性、可用性、易用性这四类非功能性需求。

【问题 1 解析】

性能：(1)、(2)、(6)

安全性：(5)

可用性：(3)、(7)

易用性：(4)、(8)

【问题 2】(14 分)

经项目组讨论，完成了该系统的分布式架构设，如图 5-1 所示。请从下面给出的(a)~(j)中进行选择，补充完善图中(1)-(7)处空白的内容。

(a) 数据存储层

(b) Struct2

(c) 负载均衡层

(d) 表现层

(e) HTTP 协议

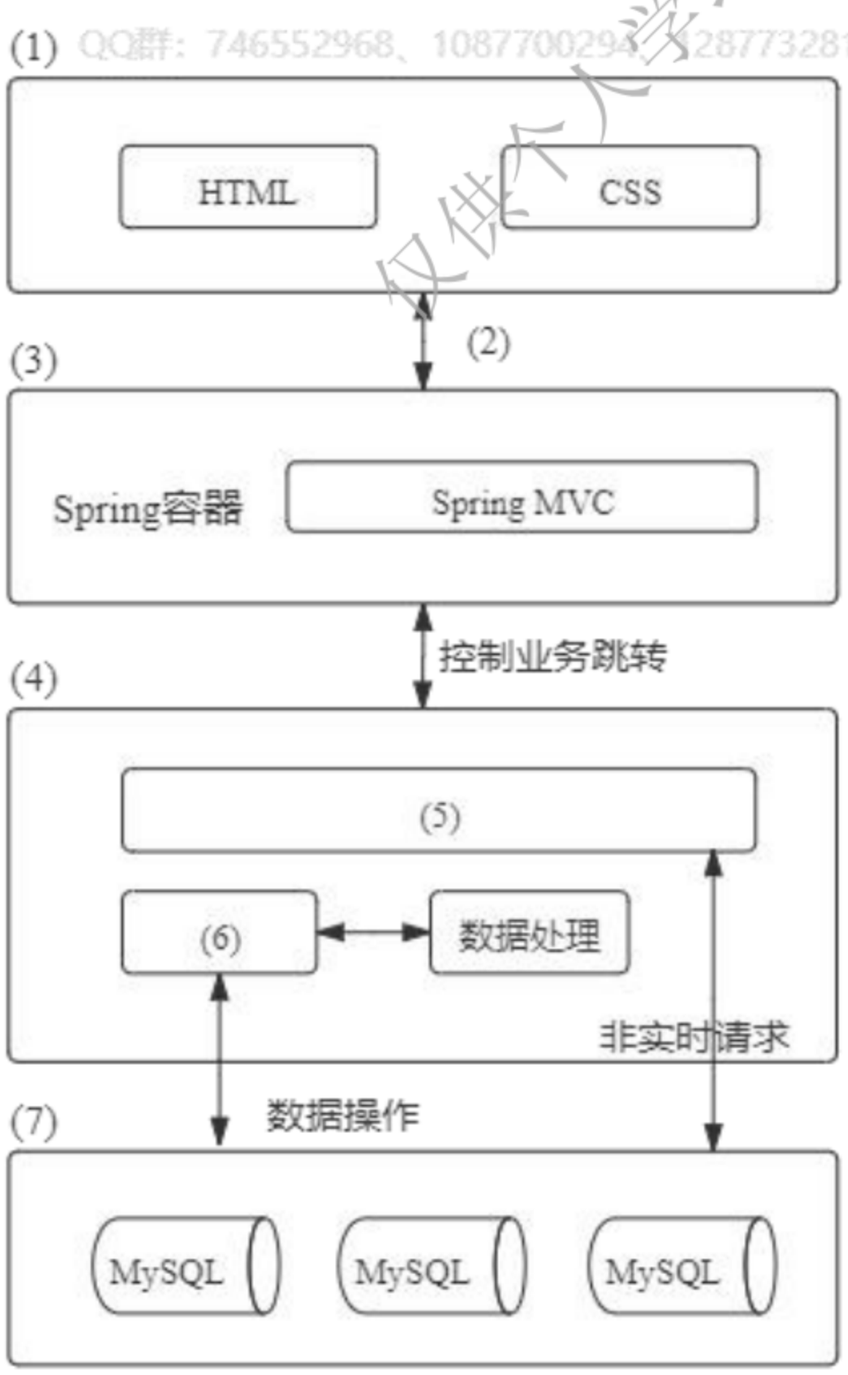
(f) Redis 数据缓存

(g) Kafka 分发消息

(h) 分布式通信处理层

(i) 逻辑处理层

(j) CDN 内容分发



【问题 2 解析】

(1)—(d)　(2)—(e)　(3)—(i)　(4)—(h)　(5)—(g)

(6)—(f)　(7)—(a)

【问题 3】(7 分)

该物流车辆管理系统需抵御常见的 SQL 注入攻击，请用 200 字以内的文字说明什么是 SQL 注入攻击，并列举出两种抵御 SQL 注入攻击的方式。

【问题 3 解析】

SQL 注入攻击：是黑客对数据库进行攻击的常用手段之一。随着 B/S 模式应用开发的发展，使用这种模式编写应用程序的程序员也越来越多。但是由于程序员的水平及经验也参差不齐，相当大一部分程序员在编写代码的时候，没有对用户输入数据的合法性进行判断，使应用程序存在安全隐患。用户可以提交一段数据库查询代码，根据程序返回的结果，获得某些他想得知的数据，这就是所谓的 SQLInjection，即 SQL 注入。

可以通过以下方式抵御 SQL 注入攻击：

1、使用正则表达式；
2、使用参数化的过滤性语句；
3、检查用户输入的合法性；
4、用户相关数据加密处理；
5、存储过程来执行所有的查询；
6、使用专业的漏洞扫描工具。