2011 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评估的说明，在答题纸上回答问题 1 和问题。

【题目】

某网上购物电子商务公司拟升级正在使用的在线交易系统，以提高用户网上购物在线支付环节的效率和安全性。在系统的需求分析与架构设计阶段，公司提出的需求和关键质量属性场景如下：

(a)正常负载情况下，系统必须在 0.5 秒内对用户的交易请求进行响应；

(b)信用卡支付必须保证 99.999%的安全性；

(c)对交易请求处理时间的要求将影响系统的数据传输协议和处理过程的设计；

(d)网络失效后，系统需要在 1.5 分钟内发现错误并启用备用系统；

(e)需要在 20 人月内为系统添加一个新的 CORBA 中间件；

(f)交易过程中涉及到的产品介绍视频传输必须保证画面具有 600*480 的分辨率，20 帧/秒的速率；

(g)更改加密的级别将对安全性和性能产生影响；

(h)主站点断电后，需要在 3 秒内将访问请求重定向到备用站点；

(i)假设每秒中用户交易请求的数量是 10 个，处理请求的时间为 30 毫秒，则“在 1 秒内完成用户的交易请求”这一要求是可以实现的；

(j)用户信息数据库授权必须保证 99.999%可用；

(k)目前对系统信用卡支付业务逻辑的描述尚未达成共识，这可能导致部分业务功能模块的重复，影响系统的可修改性；

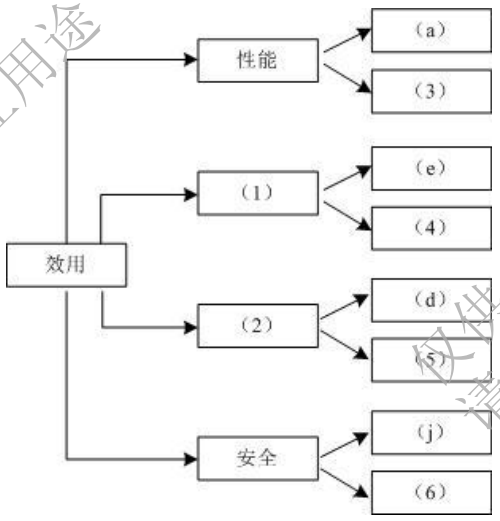
(l)更改 Web 界面接口必须在 4 人周内完成；

(m)系统需要提供远程调试接口，并支持系统的远程调试。

在对系统需求和质量属性场景进行分析的基础上，系统的架构师给出了三个候选的架构设计方案。公司目前正在组织系统开发的相关人员对系统架构进行评估。

【问题 1】(12 分)

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



仅供个人学习 请勿用于任何商业用途

【问题 1 解析】【与 2017 年第 1 题、2015 年第 1 题、2014 年第 4 题类似】

质量属性效用包括：性能、安全性、可用性、可修改性。

(1)~(2)空白处分别为可修改性、可用性。

(3)~(6)空白处分别为：

(3)—(f)—性能：交易过程中涉及到的产品介绍视频传输必须保证画面具有 600*480 的分辨率，20 帧/秒的速率。

(4)—(l)—可修改性：更改 Web 界面接口必须在 4 人周内完成。

(5)—(h)—可用性：主站点断电后，需要在 3 秒内将访问请求重定向到备用站点。

(6)—(b)—安全性：信用卡支付必须保证 99.999%的安全性。

【问题 2】(13 分)

在架构评估过程中，需要正确识别系统的架构风险、敏感点和权衡点，并进行合理的架构决策。请用 300 字以内的文字给出系统架构风险、敏感点和权衡点的定义，并从题干(a)~(m)中各选出 1 个对系统架构风险、敏感点和权衡点最为恰当的描述。

【问题 2 解析】

系统架构风险：架构设计中潜在的、存在问题的架构决策所带来的隐患(k)。

系统架构敏感点：为了实现某种特定的质量属性，一个或多个构件所具有的特性(c)。

系统架构权衡点：影响**多个质量属性**的特性，是多个质量属性的敏感点(**g：安全性和性能**)。

2. 阅读以下关于面向对象系统建模的叙述，在答题纸上回答问题 1 至问题 3。

【题目】

某软件公司成立项目组为某高校开发一套教职工信息管理系统。与教职工信息相关的数据需求和处理需求如下：

(1)数据需求：在教职工信息中能够存储学校所有在职的教工和职工信息，包括姓名、所属部门、出生年月、工资编号、工资额和缴税信息；部门信息中包括部门编号、部门名称、部门人数和办公地点信息。

(2)处理需求：能够根据编制内或外聘教职工的工资编号分别查询其相关信息；每个月的月底统一核发工资，要求系统能够以最快速度查询出教工或者职工所在部门名称、实发工资金额；由于学校人员相对稳定，所以数据变化及维护工作量很少。

项目组王工和李工针对上述应用需求分别给出了所设计的数据模型(如图 2-1 和图 2-2 所示)。王工遵循数据库设计过程，按照第三范式对数据进行优化和调整，所设计的数据模型简单且基本没有数据冗余；而李工设计的数据模型中存在大量数据冗余。

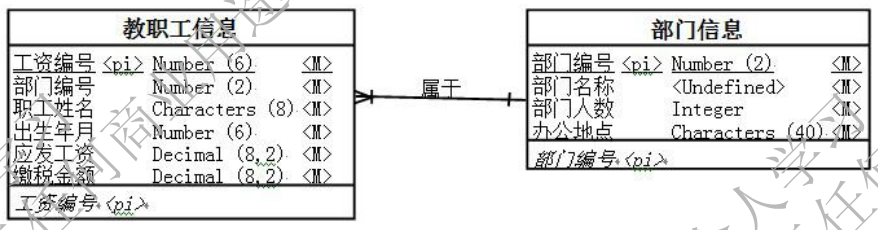


图 2-1 王工设计的数据模型

仅供个人学习 请勿用于任何商业用途

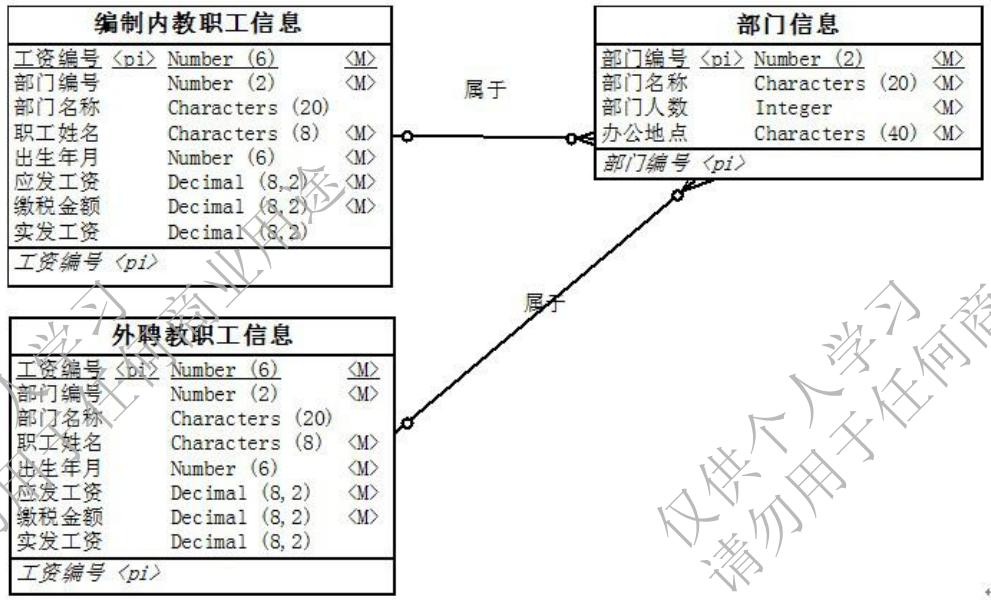


图 2-2 李工设计的数据模型

项目组经过分析和讨论，特别是针对数据处理中对数据访问效率的需求，最终选择了李工给出的数据模型设计方案。

【问题 1】(9 分)

请用 300 字以内的文字，说明什么是数据库建模中的反规范化技术，指出采用反规范化技术能获得哪些益处，可能带来哪些问题。

【问题 1 解析】

规范化设计后，数据库设计者希望牺牲部分规范化来提高性能，这种从规范化设计的回退方法称为反规范化技术。

采用反规范化技术的益处：降低连接操作的需求、降低外码和索引的数目，还可能减少表的数目，能够提高查询效率。

可能带来的问题：数据的重复存储，浪费了磁盘空间；可能出现数据的完整性问题，为了保障数据的一致性，增加了数据维护的复杂性，会降低修改速度。

【问题 2】(10 分)

请简要叙述常见的反规范化技术有哪些。

【问题 2 解析】

(1)增加冗余列：在多个表中保留相同的列，通过增加数据冗余减少或避免查询时的连接操作。

(2)增加派生列：在表中增加可以由本表或其它表中数据计算生成的列，减少查询时的连接操作并避免计算或使用集合函数。

(3)重新组表：如果许多用户需要查看两个表连接出来的结果数据，则把这两个表重新组成一个表来减少连接而提高性能。

(4)水平分割表：根据一列或多列数据的值，把数据放到多个独立的表中，主要用于表数据规模很大、表中数据相对独立或数据需要存放到多个介质上时使用。

(5)垂直分割表：对表进行分割，将主键与部分列放到一个表中，主键与其它列放到另一个表中，在查询时减少 I/O 次数。

【问题 3】(8 分)

请分析李工是如何应用反规范化技术来满足教职工信息管理需求的。

【问题 3 解析】

在教职工信息管理系统的需求中，能够根据编制内或外聘教职工的工资编号分别查询其

相关信息，数据查询要求有很高的处理效率。李工所设计的数据模型中采用了三种反规范化技术：

(1)增加冗余列：增加“部门名称”列，消除了数据查询中“教职工信息”表和“部门信息”表之间的连接；

(2)增加派生列：增加“实发工资”列，消除了实发工资的计算过程；

(3)水平分割表：将教职工信息表分割为“编制内教职工信息”表和“外聘教职工信息”表，减少了数据查询的范围。

3. 阅读以下有关嵌入式系统设计的说明，在答题纸上回答问题 1 至问题 3。

【题目】

某公司承接了某机载嵌入式系统的研制任务。该机载嵌入式系统由数据处理模块、大容量模块、信号处理模块、数据交换模块和电源模块等组成。数据处理模块有 2 个，分别完成数据融合和导航通讯任务；大容量模块主要功能是存储系统数据，同时要记录信号处理模块、数据处理模块的自检测、维护数据，向数据处理模块提供地图数据；信号处理模块的处理器为专用的 DSP，接收红外、雷达等前端传感器数据并进行处理，将处理后的有效数据(数据带宽较大)发送给数据处理模块；数据交换模块主要负责系统的数据交换；电源模块主要负责给其它模块供电，电源模块上没有软件。

要求该机载嵌入式系统符合综合化、模块化的设计思想，并考虑系统在生命周期中的可靠性和安全性，以及硬件的可扩展性和软件可升级性，还要求系统通讯延迟小，支持多模块上的应用任务同步。

【问题 1】(共 14 分)

在设计系统架构时，李工提出了如图 3-1 所示的系统架构，即模块间的网络通信采用光纤通信(Fiber Channel，FC)技术，而王工认为应采用 VME 总线架构，如图 3-2 所示。王工的理由是公司多年来基于 VME 总线技术设计了多个产品，技术成熟，且费用较小。但公司经过评审后，决定采用李工的方案。

仅供个人学习 请勿用于任何商业用途

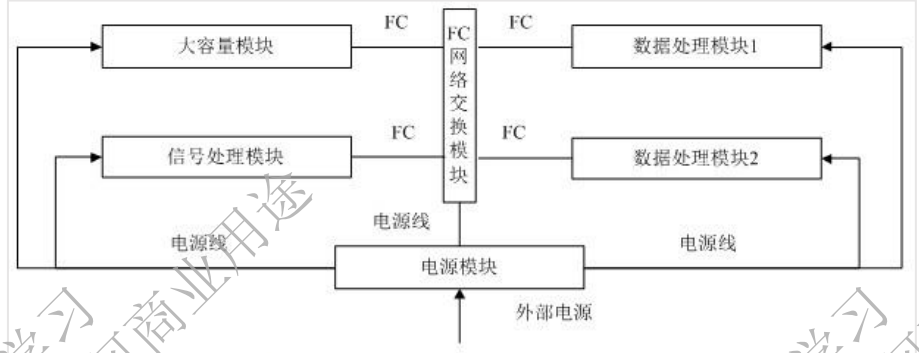


图 3-1　基于 FC 技术的机载嵌入式系统架构

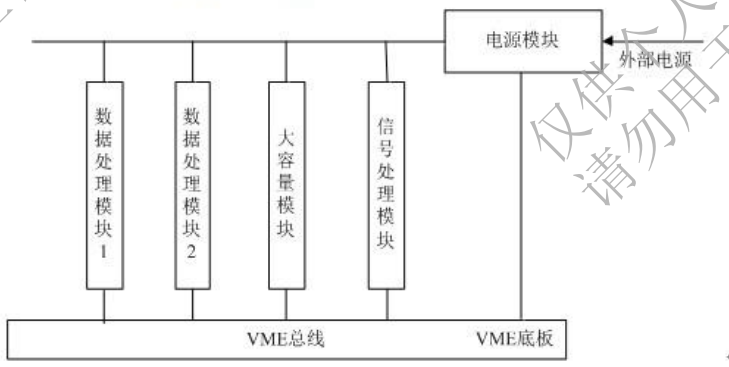


图 3-2　基于 VME 总线的机载嵌入式系统架构

请用 500 字以内的文字，说明 VME 和 FC 各自的特点，并针对机载嵌入式系统的要求，指出公司采用李工方案的理由。

【问题 1 解析】

1、VME 总线采用存储映射方式，多主机仲裁机制，同一时刻由单一主机控制，同时仲裁机制为菊花链方式。针对本系统要求，采用 VME 方案存在如下问题：

(1)当多主机设备仲裁时，按菊花链的连接次序一个主机处理完成后，才能将控制权交给另一主机控制总线，导致任务执行延时大，不能满足“系统通讯延迟小”以及“ 支持多模块上的应用任务同步”的要求。

(2)VME 总线方式限制了可扩展性。与 FC 相比，VME 总线实时性差，带宽低。

2、FC 采用消息包交换机制，支持广播和组播。针对本系统要求，采用 FC 方案有以下优点：

(1)由于采用消息包交换机制，支持广播和组播，任务执行并发性好，能满足“系统通讯延迟小”以及“ 支持多模块上的应用任务同步”的要求。

(2)FC 的误码率低，可靠性高。与 VME 比较，FC 实时性好，带宽高。

(3)允许在同一接口上传输多种不同的协议，对上层应用实现提供了便利。

(4)FC 采用消息机制，FC 可扩展性好，如模块较多可采用多个 FC 网络交换模块级联。

(5)FC 的传输距离远，当与外部其它设备相连时，比较方便。

(6)系统采用统一的 FC 网络代替了 VME 底板总线，降低总线驱动的功耗，简化了底板。

【问题 2】(共 5 分)

公司依据 ARINC653 标准，设计了满足 ARINC653 标准的操作系统，该操作系统对系统中可能发生的模块级、分区级和进程级的错误进行处理，实现了如图 3-3 所示的系统健康监控机制，请分别将备选答案中的各种错误和健康监控部件填入图 3-3 中的(1)~(5)。

仅供个人学习 请勿用于任何商业用途

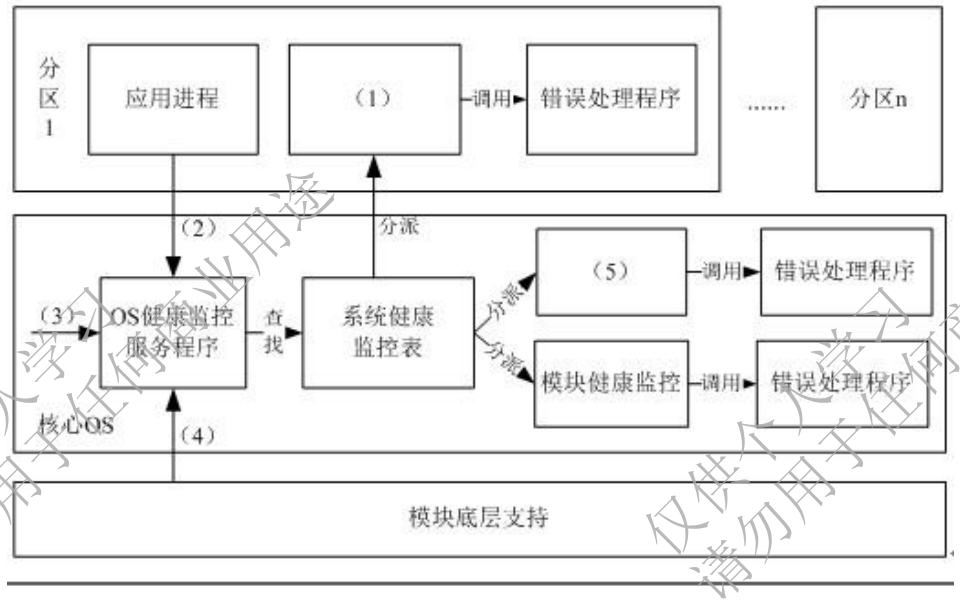


图 3-3 系统健康监控机制

备选答案：分区健康监控、分区初始化阶段出现的分区配置错误、分区切换时出现的错误、应用进程错误、进程健康监控。

注：ARINC653 标准(Avionics Application Software Standard Interface)是美国航空电子工程协会 AEEC 于 1997 年为航空民用飞机的模块化综合航空电子系统定义的应用程序接口标准，该标准提出了分区(Partition)的概念以及健康监控(health monitoring)机制。分区是应用的一种功能划分，也是操作系统调度的基本单位，严格按预先分配的时间片调度。分区间具有时空隔离特点。分区内的每一执行单元称为进程。

【问题 2 解析】

问题 2 是一个选择题,在解答本题时,关键在于区分不同的错误归属于哪一个错误级别。

模块级错误一般包括:

1、模块初始化时发生的模块配置错误;

2、模块初始化时的其他错误;

3、系统功能执行期间出现的错误;

4、分区切换时发生的错误;

5、电源故障。

分区级错误一般包括:

1、分区初始化阶段出现的分区配置错误;

2、分区初始化阶段出现的其它错误;

3、进程管理中的错误;

4、错误处理进程的错误。

进程级错误一般包括:

1、应用进程产生的应用错误;

2、非法操作系统请求;

3、进程执行错误(溢出、缓冲区冲突等)。

在图 3-3 所示的系统健康监控机制中，当系统出现故障时，通过故障检测机制(FDM)，报告给操作系统的 OS 健康监控服务程序，OS 健康监控服务程序查找系统健康监控表，从而根据错误的级别，分别派遣到模块级健康监控、分区级健康监控和进程级健康监控程序进一步对故障进行处理，注意：**进程级健康监控程序应作为分区内的一个进程**。

【答案】

(1) ~进程健康监控

(2) ~应用进程错误

(3) ~分区初始化阶段出现的分区配置错误
(4) ~分区切换时出现的错误
(5) ~分区健康监控

【问题 2】(共 6 分)
为了实现满足 ARINC653 标准的操作系统的时空分区隔离机制，项目组选择了 PowerPC 作为数据处理模块的处理器(CPU)。这样，当一个分区出现故障时，不会蔓延到模块中同一处理器的其它分区。请用 500 字以内的文字，说明如何采用 PowerPC 实现应用与内核以及诸应用之间的隔离和保护。

【问题 3 解析】
采用 PowerPC 实现系统隔离和保护的两种机制是:
第一种是内存管理机制(MMU)。MMU 能够实现逻辑地址到物理地址的转化，并且对访问权进行控制，既可以保护系统内核不受应用软件有意或无意的破坏，也可有效防止各用用软件之间的互相破坏。
第二种是 TRAP 系统调用机制。操作系统为实现对内核以及应用之间的保护，提供了用户态和系统态两种运行形态。操作系统内核在系统态运行，因此用户态的应用不能直接调用系统内核提供的功能接口，必须通过 TRAP 系统调用的方式进行。因此可以实现应用与内核之间的隔离与保护。

4. 阅读以下 Web 应用系统架构设计的说明，在答题纸上回答问题 1 至问题 3。

【题目】
某公司拟开发一个市场策略跟踪与分析系统，根据互联网上用户对公司产品信息的访问情况和产品实际销售情况来追踪各种市场策略的效果。其中互联网上用户对公司产品信息的访问情况需要借助两种不同的第三方 Web 分析软件进行数据采集与统计，并生成不同格式的数据报表；公司产品的实际销售情况则需要通过各个分公司的产品销售电子表格或数据库进行采集与汇总。得到相关数据后，还要对数据进行分析与统计，并通过浏览器以在线的方式向市场策略制定者展示最终的市场策略效果。

在对市场策略跟踪与分析系统的架构进行设计时，公司的架构师王工提出采用面向服务的系统架构，首先将各种待集成的第三方软件和异构数据源统一进行包装，然后将数据访问功能以标准 Web 服务接口的形式对外暴露，从而支持系统进行数据的分析与处理，前端则采 CSS 等技术实现浏览器数据的渲染与展示。架构师李工则认为该系统的核心在于数据的定位、汇聚与转换，更适合采用面向资源的架构，即首先为每种数据元素确定地址，然后将各种数据格式统一转换为 JSON 格式，通过对 JSON 数据的组合支持数据的分析与处理任务，处理结果经过渲染后在浏览器的环境中进行展示。在架构评估会议上，专家对这两种方案进行综合评价，最终采用了李工的方案。

【问题 1】(共 7 分)
请根据题干描述，对市场策略跟踪与分析系统的数据源特征与数据操作方式进行分析，完成表 4-1 中的(1)~(3)，并用 200 字以内的文字说明李工方案的优点。

表 4-1 系统数据源特征与数据操作方式

数据源类型	数据源特征		数据操作方式
	数据形态	数据访问实时性	
互联网用户访问信息	(1)	非实时	(3)
产品销售信息	电子表格与数据库	(2)	只读

【问题 1 解析】

仅供个人学习 请勿用于任何商业用途

本问题主要考查两种不同 Web 数据源的数据特点。

对于题干描述的市场策略跟踪与分析系统特征，对于互联网用户访问数据源来说，该数据的数据形态一般为数据报表形态，数据为非实时性访问，数据操作方式一般为只读方式。

对于产品销售信息，该数据源的数据形态一般为电子表格和数据库，数据访问方式为非实时访问。数据操作方式一般为只读方式。

【答案】

(1)~数据报表

(2)~非实时

(3)~只读

通过对系统的数据源特征和数据操作方式进行分析可以看出，待集成的数据均为持久型数据(文件或数据库)，系统对数据的访问均为只读非实时性的。针对上述应用特征，李工提出的面向资源的架构方式以对数据资源的只读访问为核心，通过数据唯一标识直接对各种数据进行访问与获取，系统架构清晰、实现简单、效率较高。

【问题 2】(12 分)

请从数据获取方式、数据交互方式和数据访问的上下文无关性三个方面对王工和李工的方案进行比较，并用 500 字以内的文字说明为什么没有采用王工的方案。

【问题 2 解析】

从数据获取方式看，王工的方案需要将现有的多个系统和异构的数据源包装为服务，采用 Web 服务暴露数据接口，客户端需要通过服务调用获取数据，这种方法工作量大，复杂度较高。李工的方案则绕开了复杂的功能封装，只需要明确数据的位置与标识，通过特定的网络协议直接使用标识定位并获取数据，与王工的方案相比工作量小，实现简单。

从数据交互方式看，王工的方案采用远程过程调用和异步 XML 消息等模式实现数据交互，这种方式适合于系统之间功能调用时进行的少量数据传输，而在进行单纯的数据访问时效率不高，稳定性也较差。李工的方案则以数据资源为核心，在对数据资源进行标识的基础上，通过标识符直接对数据资源进行访问与交互，实现简单且效率较高。

从数据访问的上下文无关性看，王工的方案中数据访问是上下文有关的，具体表现在每次客户端进行数据请求都需要附加唯一的请求标识，并且服务端需要区分不同的客户端请求，效率较低。李工的方案中数据访问是上下文无关的，客户端通过全局唯一的统一资源标识符(URI)请求对应的数据资源，服务端不需要区分不同的客户端请求。

【问题 3】(6 分)

表现层状态转换(REST)是面向资源架构的核心思想，请用 200 字以内的文字解释什么是 REST，并指出在 REST 中将哪三种关注点进行分离。

【问题 3 解析】

REST 从资源的角度来定义整个网络系统结构，分布在各处的资源由统一资源标识符(URI)确定，客户端应用程序通过 URI 获取资源的表现，并通过获得资源表现使得其状态发生改变。

REST 中将**资源**、**资源的表现**和**获取资源的动作**三者**进行分离**。

5. 阅读以下关于信息系统安全性的说明，在答题纸上回答问题 1 至问题 3。

【题目】

仅供个人学习 请勿用于任何商业用途

某大型跨国企业的 IT 部门一年前基于 SOA(Service-Oriented Architecture)对企业原有的多个信息系统进行了集成，实现了原有各系统之间的互连互通，搭建了支撑企业完整业务流程运作的统一信息系统平台。随着集成后系统的投入运行，IT 部门发现在满足企业正常业务运作要求的同时，系统也暴露出明显的安全性缺陷，并在近期出现了企业敏感业务数据泄漏及系统核心业务功能非授权访问等严重安全事件。针对这一情况，企业决定由 IT 部门成立专门的项目组负责提高现有系统的安全性。

项目组在仔细调研和分析了系统现有安全性问题的基础上，决定首先为在网络中传输的数据提供机密性(Confidentiality)与完整性(Integrity)保障，同时为系统核心业务功能的访问提供访问控制机制，以保证只有授权用户才能使用特定功能。

经过分析和讨论，项目组决定采用加密技术为网络中传输的数据提供机密性与完整性保障。但在确定具体访问控制机制时，张工认为应该采用传统的强制访问控制(Mandatory Access Control)机制，而王工则建议采用基于角色的访问控制(Role-Based Access Control)与可扩展访问控制标记语言(eXtensible Access Control Markup Language，XACML)相结合的机制。项目组经过集体讨论，最终采用了王工的方案。

【问题 1】(8 分)

请用 400 字以内的文字，分别针对采用对称加密策略与公钥加密策略，说明如何利用加密技术为在网络中传输的数据提供机密性与完整性保障。

【问题 1 解析】

1、对称加密策略

(1)机密性：发送者利用对称密钥对要发送的数据进行加密，只有拥有正确相同密钥的接收者才能将数据正确解密，从而提供机密性。

(2)完整性：发送者根据要发送的数据生成消息认证码(或消息摘要)，利用对称密钥对消息认证码进行加密并附加到数据上发送；接收者使用相同密钥将对方发送的消息认证码解密，并根据接收到的数据重新生成消息认证码，比较两个认证码是否相同以验证数据的完整性。

2、公钥加密策略

(1)机密性：发送者利用接收者的公钥对要发送的数据进行加密，只有拥有对应私钥的接收者才能将数据正确解密，从而提供机密性。

(2)完整性：发送者根据要发送的数据生成消息认证码(或消息摘要)，利用自己的私钥对消息认证码进行加密并附加到数据上发送;接收者利用对方的公钥将对方发送的消息认证码解密，并根据接收到的数据重新生成消息认证码，比较两个认证码是否相同以验证数据的完整性。

【问题 2】(9 分)

请用 300 字以内的文字，从授权的可管理性、细粒度访问控制的支持和对分布式环境的支持三个方面指出项目组采用王工方案的原因。

【问题 2 解析】

(1)授权的可管理性：RBAC 将用户与权限分离，与 MAC 相比，减小了授权管理的复杂性，更适合于大型企业级系统的安全管理。

(2)细粒度访问控制的支持：XACML 提供了统一的访问控制策略描述语言，策略表达能力强，可用来描述各种复杂的和细粒度的访问控制安全需求，更适合企业复杂业务功能的访问控制要求。

(3)分布式环境的支持：XACML 的标准性便于各子系统的协作交互，各子系统或企业业务部门可以分布管理访问控制权限，而 MAC 则通常需要对访问控制权限集中管理，不太适合企业基于 SOA 集成后的分布式系统。

【问题 3】(8 分)

图 5-1 给出了基于 XACML 的授权决策中心的基本结构以及一次典型授权决策的执行过程，请分别将备选答案填入图中的(1)~(4)。

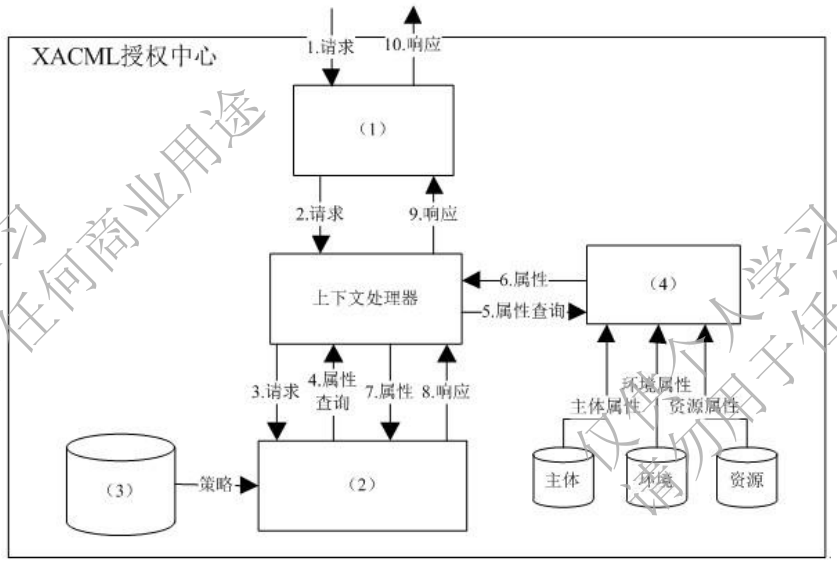


图 5-1 基于 XACML 的授权决策中心的基本结构

备选答案：策略管理点(PAP)、策略执行点(PEP)、策略信息点(PIP)、策略决策点(PDP)

【问题 3 解析】

问题 3 考查考生对 XACML 授权架构的理解。其中 PEP 是在具体应用环境下执行访问控制的实体，它接收外部的授权请求并生成相应的授权响应，因此（1）处应填 PEP；而 PDP 是系统中授权决策的实体，依据 XACML 描述的访问控制策略以及其他属性信息进行访问控制决策，因此（2）处应填 PDP；PAP 系统中产生和维护安全策略的实体，因此（3）处应填 PAP；PIP 是获取主体、资源和环境的属性信息的实体因此（4）处应填 PIP。

(1) ~策略执行点(PEP)

(2) ~策略决策点(PDP)

(3) ~策略管理点(PAP)

(4) ~策略信息点(PIP)

仅供个人学习 请勿用于任何商业用途