2013 年系统架构师考试科目二：案例分析

1. 阅读以下关于企业应用系统集成架构设计的说明，在答题纸上回答问题 1 和问题 2。

【题目】

某航空公司希望对构建于上世纪七、八十年代的主要业务系统进行改造与集成，提高企业的竞争力。由于集成过程非常复杂，公司决定首先以 Ramp Coordination 系统为例进行集成过程的探索与验证。

在航空业中，Ramp Coordination 是指飞机从降落到起飞过程中所需要进行的各种业务活动的协调过程。通常每个航班都有一位员工负责 Ramp Coordination，称之为 Ramp Coordinator 由 Ramp Coordinator 协调的业务活动包括检查机位环境、卸货和装货等。

由于航班类型、机型的不同，Ramp Coordination 的流程有很大差异。图 1-1 (a)所示的流程主要针对短期中转航班，这类航班在机场稍作停留后就起飞；图 1-1(b)所示的流程主要针对到达航班，通常在机场过夜后第二天起飞；图 1-1(c)所示的流程主要针对离港航班，这类航班是每天的第一班飞机。这三种类型的航班根据长途/短途、国内/国外等因素还可以进一步细分，每种细分航班类型的 Ramp Coordination 的流程也略有不同。

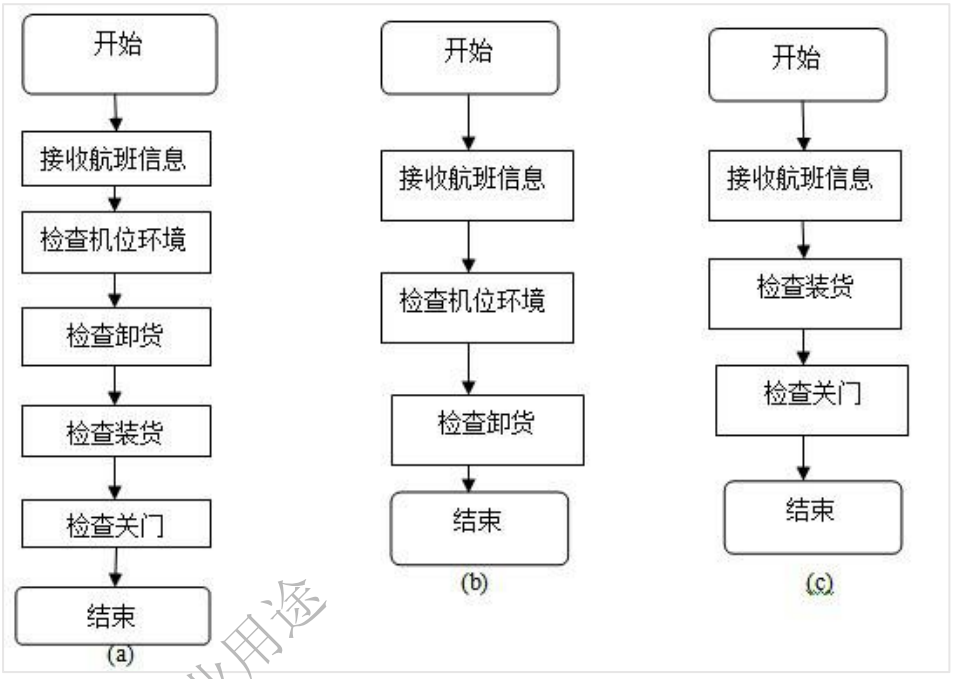


图 1-1 Ramp Coordination 业务流程

为了完成上述业务，Ramp Coordination 信息系统需要从乘务人员管理系统中提取航班乘务员的信息、从订票系统中提取乘客信息、从机务人员管理系统中提取机务人员信息、接收来自航班调度系统的航班到达事件。其中乘务人员管理系统和航班调度系统运行在大型主机系统中，机务人员管理系统运行在 Unix 操作系统之上，订票系统基于 Java 语言，具有 Web 界面，运行在 Linux 操作系统之上。

目前 Ramp Coordination 信息系统主要由人工完成所有协调工作，效率低且容易出错。

公司领导要求集成后的 Ramp Coordination 信息系统能够针对不同需求迅速开展业务流程，灵活、高效地完成协调任务。

针对上述要求，公司 IT 部门的架构师经过分析与讨论，最终采用面向服务的架构，以服

务为中心进行 Ramp Coordination 信息系统的集成工作。

【问题 1】(10 分)

服务建模是对 Ramp Coordination 信息系统进行集成的首要工作，公司的架构师首先对 Ramp Coordination 信息系统进行服务建模，识别出系统中的两个主要业务服务组件：

(1)Ramp Control：负责 Ramp Coordination 信息系统中相关各种业务活动的组件；

(2)Flight Management：负责航班相关信息的管理，包括航班日程，乘客信息等。

针对上述服务模型，结合题干描述，请为每个业务服务组件提供的服务进行分析与整理，完成表 1-1 中的空白部分。

表 1-1 业务组件服务提供的服务

业务服务组件	提供服务名称
Ramp Control	
Flight Management	

【问题 1 解析】

问题 1 要求指出业务服务组件 RampControl 和 Flight Management 分别提供的服务名称。很多考生在看到这类问题时，都觉得自己没有做过面向服务架构设计中的服务设计，觉得题目难度已经超出自己的能力范围，而无法答题。其实不然，因为服务的划分，与传统开发中的功能模块划分一样，只是粒度大一些而已。只要认真看题，并分析系统提供了哪些功能，哪些功能归属于 RampControl，哪些应归属于 Flight Management，答案是很容易得出的。如题目“通常每个航班都有一位员工负责 Ramp Coordination，称之为 Ramp Coordinator 由 Ramp Coordinator 协调的业务活动包括检查机位环境、卸货和装货等。”从此就可以看出 Ramp Control 提供的服务包括：机位环境查询服务、卸货检查服务、装货检查服务。从流程图可以看出此组件还应包括检查关门服务。这样，整个流程图中，只余下接收航班信息服务适合划分至 Flight Management 组件。

(1)检查机位环境、检查卸货、检查装货、检查关门

(2)接收航班信息

【问题 2】(15 分)

对 Ramp Coordination 信息系统的集成涉及到对乘务人员管理系统、航班调度系统、机务人员管理系统和订票系统的组织与协调，公司架构师决定采用企业服务总线(Enterprise Service Bus，ESB)技术进行系统集成，请用 200 字以内的文字对 ESB 的定义进行描述，给出 ESB 的五个主要功能，并针对题干描述，将恰当的内容填入图 1-2 中的(1)~(6)。

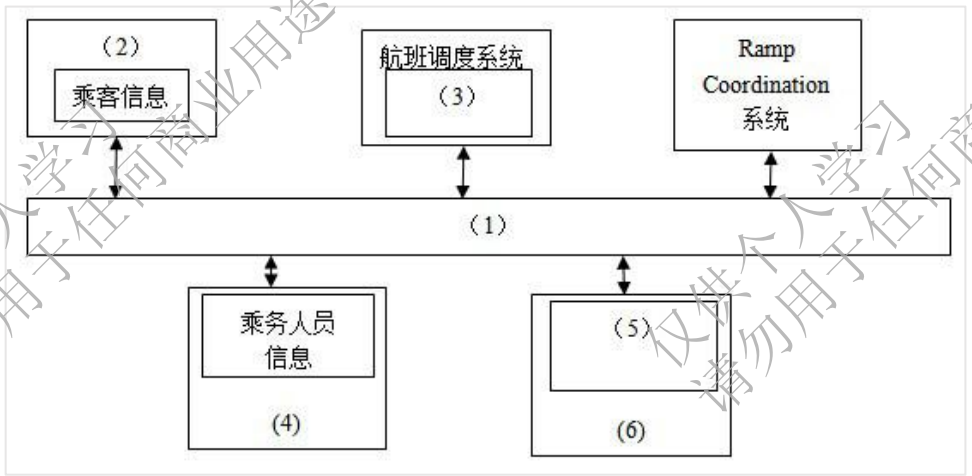


图 1-2 系统集成框架图

【问题 2 解析】

对于问题 2 中的填图问题，主要是通过题目中给出的信息，以及图中其它同类位置的信息来判断。如：图中中心模块连接了各个分支模块，每个分支模块结构相同，所以可从分支模块表达的信息看出，外框要填写的是“**系统”，而内框是“**信息”，依据这个规则，在题干中很容易得出答案。中心部分，自然就是连接件 ESB 了。

【答案】

ESB 是传统中间件技术与 XML、Web 服务等技术结合的产物，主要支持异构系统集成。ESB 基于内容的路由和过滤，具备复杂数据的传输能力，并可以提供一系列的标准接口。

ESB 的主要功能：

(1)服务位置透明性；

(2)传输协议转换；

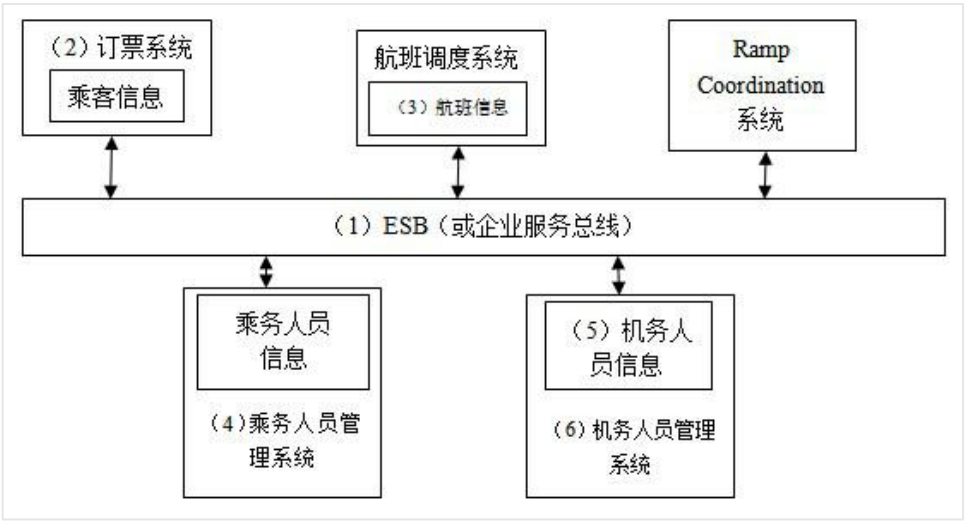
(3)消息格式转换；

(4)消息路由；

(5)消息增强；

(6)安全性；

(7)监控与管理。



2. 阅读以下关于某项目开发计划的说明，在答题纸上回答问题 1 至问题 4。

【题目】

某软件公司拟开发一套电子商务系统，王工作为项目组负责人负责编制项目计划。由于该企业业务发展需要，CEO 急于启动电子商务系统，要求王工尽快准备一份拟开发系统的时间和成本估算报告。

项目组经过讨论后，确定出与项目相关的任务如表 2-1 所示。其中，根据项目组开发经验，分别给出了正常工作及加班赶工两种情况下所需的时间和费用。

表 2-1 项目开发任务进度及费用

任务名称	正常工作	加班工作	前置任务
A. 系统调研	4 天/7200 元	3 天/8400 元	-
B. 提交项目计划	2 天/1600 元	1 天/1900 元	A
C. 需求分析	6 天/9600 元	4 天/14200 元	B
D. 系统设计	12 天/22200 元	8 天/27600 元	C
E. 数据库开发	3 天/5100 元	2 天/5700 元	D
F. 网页开发	6 天/8700 元	5 天/10000 元	D
G. 报表开发	4 天/6000 元	任务外包无法赶工	D
H. 测试修改	7 天/9800 元	4 天/12800 元	E,F,G
I. 安装部署	4 天/4000 元	2 天/5000 元	H

【问题 1】(7 分)

请用 400 字以内文字说明王工拟编制的项目计划中应包括哪些内容。

【问题 1 解析】

(1)项目背景

(2)项目经理、项目经理的主管领导、客户方联系人、客户方的主管领导，项目领导小组(项目管理团队)和项目实施小组人员

(3)项目的总体技术解决方案

(4)所选择的项目管理过程及执行水平

(5)对这些过程的工具、技术和输入输出的描述

(6)选择的项目的生命周期和相关的项目阶段

(7)项目最终目标和阶段性目标

(8)进度计划

(9)项目预算

(10)变更流程和变更控制委员会

(11)对于内容、范围和时间的关键管理评审，以便于确定悬留问题和未决决策

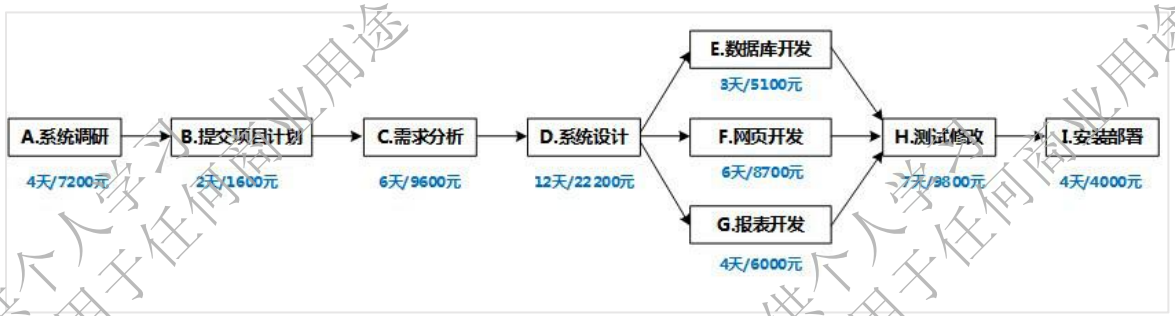
【问题 2】(8 分)

请根据表 2-1，分别给出正常工作和最短工期两种情况下完成此项目所需的时间和费用。

【问题 2 解析】

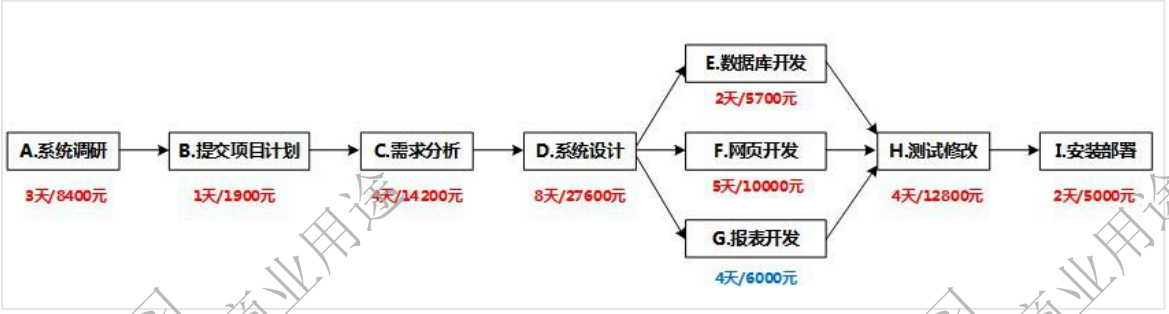
正常工作成本=7200 元+1600 元+9600 元+22200 元+5100 元+8700 元+6000 元+9800 元+4000 元=74200 元。

正常工作工期=4+2+6+12+6+7+4=41 天。



最短工期成本=8400 元+1900 元+14200 元+27600 元+5700 元+10000 元+6000 元+12800 元+5000 元=91600 元。

最短工期=3+1+4+8+5+4+2=27 天。



【问题 3】(4 分)

如果项目在系统调研阶段用了 7 天时间才完成，公司要求尽量控制成本，王工可在后续任务中采取什么措施来保证项目能按照正常工作进度完成？

【问题 3 解析】

要缩短项目的工期，主要有两种方法：

赶工：对成本和进度进行权衡，确定如何尽量少增加费用的前提下最大限度地缩短项目所需要的时间，称为赶进度也称赶工。

快速跟进：调整逻辑关系,通过对各种逻辑关系并行确定来缩短项目周期。在进行项目设计中，当风险不大时，通过精心安排而使项目的前后阶段相互搭接以加快项目进展速度的做法叫快速跟进。

其中快速跟进由于只是将部分工作提前开始,所以不会明显增加成本,在当前的环境中,是比较合适的方法。

【问题 4】(6 分)

如果企业 CEO 想在 34 天后系统上线，王工应该采取什么措施来满足这一要求？这种情况下完成项目所需的费用是多少？

【问题 4 解析】

标准时长 41 天的任务，要 34 天完成，应赶工 7 天。首先计算压缩时间增加费用，得到下表：

任务名称	正常工作	加班工作	可压缩天数	压缩 1 天增加费用
A.系统调研	4 天/7200 元	3 天/8400 元	1	1200 元
B.提交项目计划	2 天/1600 元	1 天/1900 元	1	300 元
C.需求分析	6 天/9600 元	4 天/14200 元	2	2300 元
D.系统设计	12 天/22200 元	8 天/27600 元	4	1350 元
E.数据库开发	3 天/5100 元	2 天/5700 元	1	600 元
F.网页开发	6 天/8700 元	5 天/10000 元	1	1300 元
G.报表开发	4 天/6000 元	任务外包无法赶工	0	
H.测试修改	7 天/9800 元	4 天/12800 元	3	1000 元
I.安装部署	4 天/4000 元	2 天/5000 元	2	500 元

压缩成本由小到大排列为：B<I<E<H<A<F<D<C

优先选择压缩成本低的任务，B、I、E、H 刚好 7 天。**但是压缩 E 并不会缩短 1 天的工期(E、F、G 共同决定阶段最短工期)**，进而选择 A 费用为：

8400+1900+9600+22200+5100+8700+6000+12800+5000=79700 元。

3. 阅读以下有关嵌入式软件 FMEA 方法和相关案例的说明，在答题纸上回答问题 1 至问题 3。

【题目】

故障(失效)模型影响分析 FMEA 是分析产品所有可能的故障模式及其可能产生的影响，并按每个故障模式产生影响的严重程度及其发生概率予以分类的一种归纳分析方法。近年来，FMEA 方法已被广泛用于安全关键系统的嵌入式软件可靠性分析工作。

某软件公司承担了一项通信软件的开发项目。该项目由 FC 系统、DY 系统和 GD 系统组成，而 DY 系统(TMS320C25S)软件负责按系统的通信协议完成与 FC 系统的通信，图 3-1 给出了该通信软件的约定层次图。公司高层将项目交给王工程师，王工认为此项目是安全关键系统，安全等级应为 II 类(致命的)，因此应开展软件的 FMEA 分析。

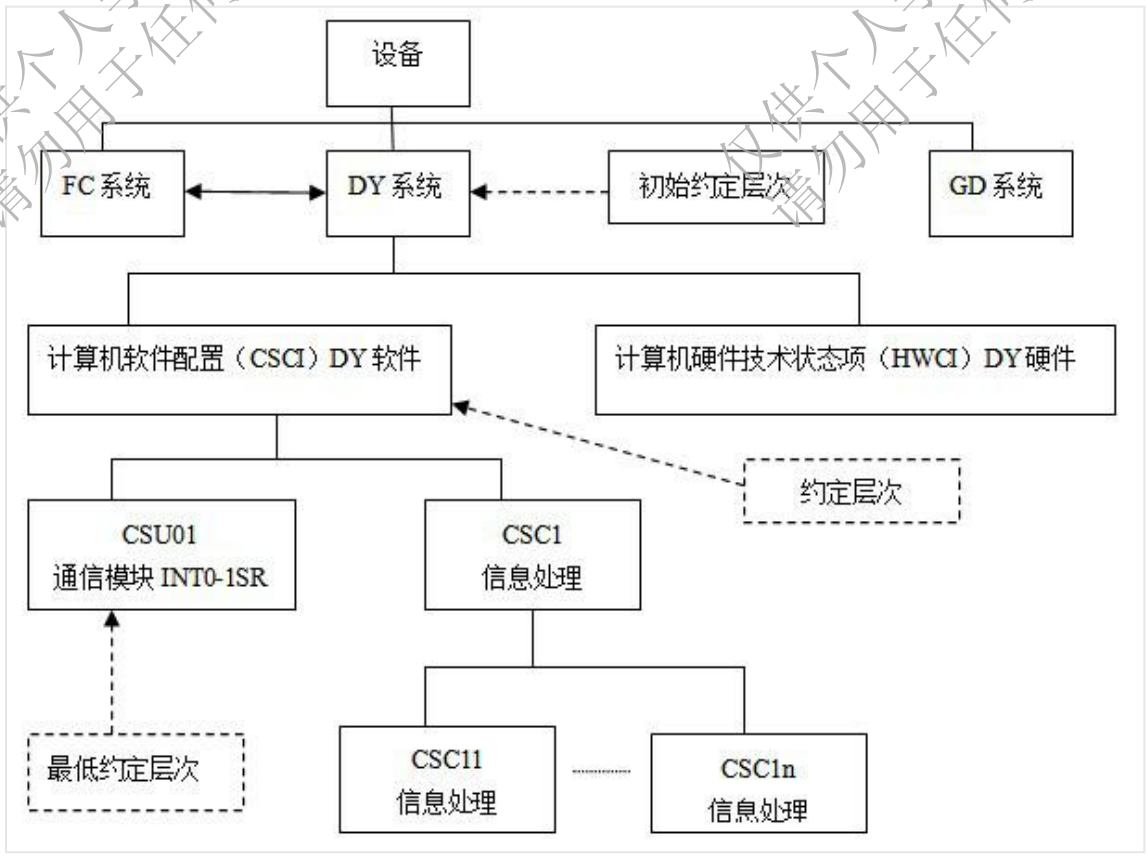


图 3-1 某设备通信软件的约定层次图

【问题 1】(共 8 分)

请阅读以下有关 FMEA 的描述，将恰当的内容填入(1)～(7)。

FMEA 是 FMA(故障模式分析)和 FEA(故障影响分析)的组合，它对系统各种可能的风险进行评价、分析后，在现有技术的基础上消除这些风险或将这些风险降低到可接受的水平。为达到最佳效益，FMEA 必须在产品研制初期进行。

FMEA 实际是一组系列化的活动，其主要活动包括：

(1)_____；

(2)_____；

(3)_____。

由于产品故障可能与设计、制造过程、使用、承包商/供应商以及服务有关，因此 FMEA 又细分为(4)FMEA、(5)FMEA、(6)FMEA 和(7)FMEA 四类。

【问题 1 解析】

(1)找出产品/过程中潜在的故障模式

(2)根据相应的评价体系对找出的潜在故障模式进行风险量化评估
(3)列出故障起因/机理，寻找预防或改进措施
(4)设计
(5)过程
(6)使用
(7)服务

【问题 2】(共 10 分)

从图 3-1 可以看出，CSU01 信模块是该项目的关键模块，主要功能定义为：总线通信控制器自动完成一帧数据的接收，存入数据缓冲区，并产生中断(INT0)通知 CPU 从数据缓冲区中读取数据；CPU 读完数据后，将准备好的发送数据写至数据缓存区，写完后通知总线通信控制器自动完成一帧数据的发送。CRC 校验由外部电路完成判别，其结果通过数据线上的相应位进行标识。针对 CSU01 通信模块，简要描述实施 FMEA 的具体内容，填写完成表 3-1 的(1)~(5)。

表 3-1 CSU01 通信模块 FMEA 步骤的主要内容

序号	主要步骤	具体内容
1	故障模式确定	(1)
2	故障原因分析	(2)
3	故障影响分析	(3)
4	危害性分析	(4)
5	改进措施	(5)

【问题 2 解析】

(1)根据通信协议，可按接收数据功能和发送数据功能分别确定故障模式
(2)故障原因分为总线通信控制器原因、对方发送的原因和自身程序的原因
(3)针对每个故障模式分析基对本模块直至整个 DY 系统造成的影响
(4)采用风险优先数 RPN 方法进行该通信模块的危害性分析
(5)根据以上故障模式、原因、影响及危害性的分析结果，综合考虑故障的影响及 SRPN 值等情况，对每个故障模式制定了相应的改进措施。

【问题 3】(共 7 分)

表 3-2 给出针对该项目的 CSU01 通信模块的软件故障(失效)模型影响分析 FMECA 表(局部)，请根据此题描述情况填写表 3-2 中的(1)~(7)。

注：表 3-2 中的 SRPN(软件风险优先数)=SESR(软件故障模式的严酷度等级)×SOPR(软件故障模式的发生概率等级)×SDDR(软件故障模式的被检测难度等级)。

表 3-2 通信模块 INT0-ISR 的软件 FMECA 表(局部)

序号	单元	功能	故障模式	故障原因	故障影响			危害性分析				改进措施
					局部影响	高一层次影响	最终影响	SESR	SOPR	SDDR	SRPN	
1	INT0-ISR	数据接收	通信接口非接收状态	（1）	模块单元无法进入	无法产生INT0中断	通信功能丧失	8	7	4	224	初始化时写 0C300H 地址单元后，读 0C300H 的 D7 位，直到确认通信接口为接收状态。判别中加以计数限制，以保证规定时间到时，记录故障标志并报错
2			中断允许处于禁止状态	程序使用 DINT 和 EINT 不当	模块单元无法进入	（2）	通信功能丧失	8	7	4	224	严格检查 DINT 和 EINT 的语句位置
3			CRC 错误	（3）	接收数据异常	接收数据错误	（4）	7	5	6	210	首先读 0C200H 地址单元的 D0 位，判别 CRC 是否正确，若 CRC 错误，则放弃此帧
4		数据发送	尚未发送就强行设置接收状态	（5）	影响发送数据的正确性	发送数据错误	通信错误	7	6	5	（6）	写 0C200H 地址单元后，读 0C200H 地址单元的 D7 位，判别是否已发送完，再通过写 0C300H 地址单元设置通信接口为接收状态。注：此措施与模式 10 和 11 相结合
5			（7）	总线通信控制器错误	发送数据失败，如果程序处理不当可能造成死循环	发送数据失败，处理不当此单元可能无法退出	通信功能丧失，处理不当可能死机	8	6	7	336	写 0C200H 地址单元后，读 0C200H 地址单元的 D7 位，判别是否已发送完，并加以计数限制，以保证规定时间到时，记录故障标志并退出此模块

【问题 3 解析】

(1)程序写 0C300H 地址单元不当

(2)无法响应 INT0 中断

(3)线路误码

(4)通信错误

(5)程序控制错误

(6)210

(7)数据发送始终不成功数据发送始终不成功

4. 阅读以下有关表现层设计方面的说明，在答题纸上回答问题 1 至问题 3。

【题目】

某商业银行欲开发一套个人银行系统，为用户提供常见的金融服务，包括转账、查询、存款变更和个人信息管理等功能。该软件除了业务需求外，还有一些特殊的表现层需求：

(1)根据用户级别的不同，界面和可用功能是不同的；

(2)支持 Web、Windows、手机 App 等多种不同类型的界面；

(3)考虑到将来功能的扩展，需要系统支持界面的定制以及动态生成等功能，以降低系统维护和新功能发布的成本。

经过对需求的讨论，该银行初步决定采用 MVC 模式设计该个人银行系统的表现层，采用 XML 作为 GUI 的描述语言，并应用 XML 的界面管理技术来实现灵活的界面配置、界面动态生成和界面定制。

【问题 1】(共 9 分)

MVC 模式强制性地将一个应用处理流程按照模型、视图、控制的方式进行分离，三者的协作关系如图 4-1 所示。

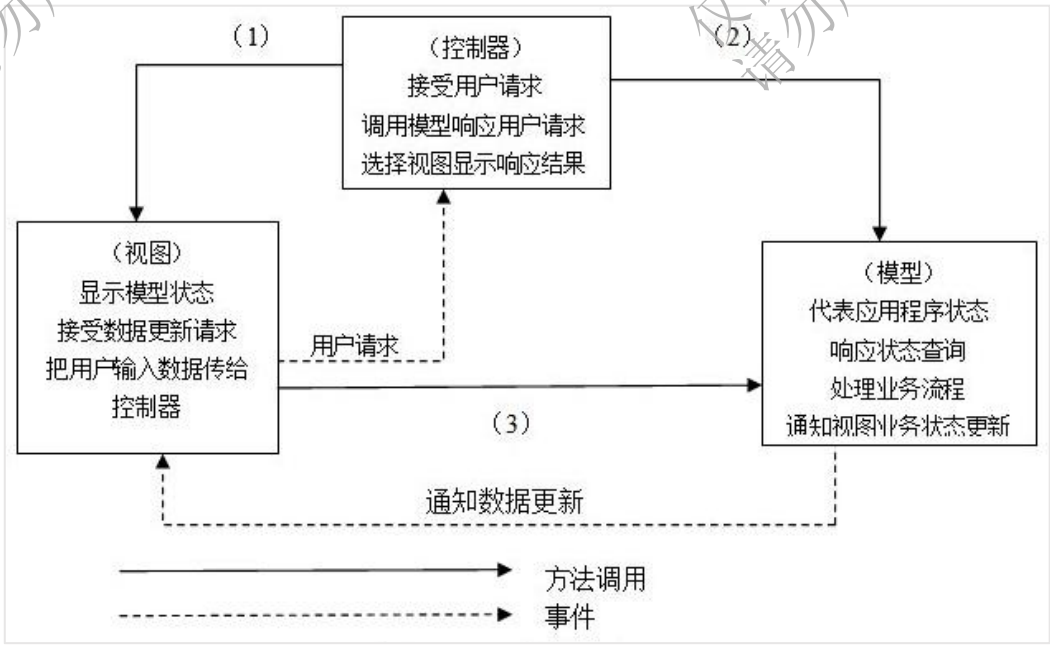


图 4-1 MVC 设计模式

请填写图 4-1 中的(1)～(3)，并简要说明在该个人银行系统中采用 MVC 模式对界面设计的作用。

【问题 1 解析】

(1)选择视图　　(2)业务视图　　(3)状态查询

MVC 模式对该个人银行系统的作用：

(1)允许多种界面的扩展，视图的变更与增加，与模型无关；

(2)易于维护，控制器和视图随着模型的扩展而扩展，只要保持公共接口，控制器和视图的旧版本可以继续使用；

(3)可支持功能强大的用户界面。

【问题 2】(4 分)

请从设计模式的角度，简要说明设计方案采用 XML 作为 GUI 描述语言的机制。

【问题 2 解析】

从设计模式的角度来说，整个 XML 表现层解析的机制是一种策略模式。在调用显示 GUI 时，不是直接调用特定的表现技术的 API，而是装载 GUI 对应的 XML 配置文件，然后根据特定的表现技术的解析器解析 XML，得到 GUI 视图实例对象。这样，对于 GUI 开发人

员来说，GUI 视图只需要维护一套 XML 文件即可。

【问题 3】(12 分)

基于 XML 的界面管理技术可实现灵活的界面配置、界面动态生成和界面定制，其思路是用 XML 生成配置文件及界面所需的元数据，按不同需求生成界面元素及软件界面，其技术框图如图 4-2 所示。

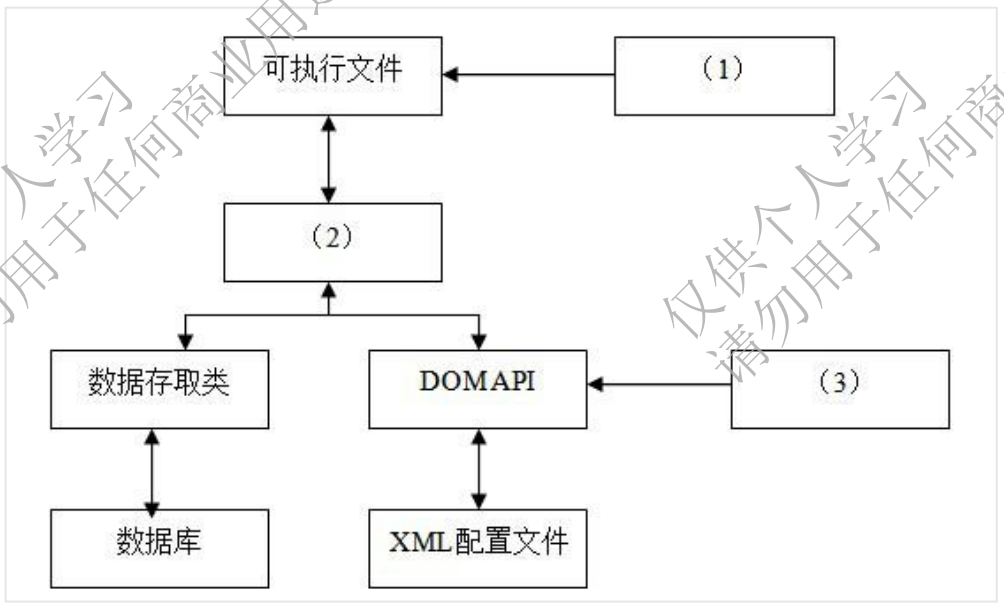


图 4-2 基于 XML 的界面管理技术框架

请将恰当的内容填入图 4-2 中的(1)～(3)，并简要解释说明其含义。

【问题 3 解析】

（1）界面定制模块

(2)界面动态生成模块

(3)界面配置模块

界面配置是对用户界面的静态定义，通过读取配置文件的初始值对界面配置。由界面配置对软件功能进行裁剪、重组和扩充，以实现特殊需求。

界面定制是对用户界面的动态修改过程，在软件运行过程中，用户可按需求和使用习惯，对界面元素(如菜单、工具栏、键盘命令)的属性(如文字、图标、大小、位置等)进行修改。软件运行结束，界面定制的结果被保存。

系统通过 DOM API 读取 XML 配置文件的表示层信息(初始界面大小、位置等)，通过数据存取类读取数据库中的数据层信息，运行时由界面元素动态生成界面。界面配置和定制模块在软件运行前后，修改配置文件，更改界面内容。

5. 阅读以下有关软件与信息安全方面的说明，在答题纸上回答问题 1 至问题 3。

【题目】

某软件公司拟开发一套信息安全支撑平台，为客户的局域网业务环境提供信息安全保护。该支撑平台的主要需求如下：

(1)为局域网业务环境提供用户身份鉴别与资源访问授权功能；

(2)为局域网环境中交换的网络数据提供加密保护；

(3)为服务器和终端机存储的敏感持久数据提供加密保护；

(4)保护的主要实体对象包括局域网内交换的网络数据包、文件服务器中的敏感数据文件、数据库服务器中的敏感关系数据和终端机用户存储的敏感数据文件：

(5)服务器中存储的敏感数据按安全管理员配置的权限访问；

(6)业务系统生成的单个敏感数据文件可能会达到数百兆的规模；

(7)终端机用户存储的敏感数据为用户私有；

(8)局域网业务环境的总用户数在 100 人以内。

【问题 1】(9 分)

在确定该支撑平台所采用的用户身份鉴别机制时，王工提出采用基于口令的简单认证机制，而李工则提出采用基于公钥体系的认证机制。项目组经过讨论，确定采用基于公钥体系的机制，请结合上述需求具体分析采用李工方案的原因。

【问题 1 解析】

(1)基于口令的认证方式实现简单，但由于口令复杂度及管理方面的原因，易受到认证攻击；而在基于公钥体系的认证方式中，由于其密钥机制的复杂性，同时在认证过程中私钥不在网络上传输，因此可以有效防止认证攻击，与基于口令的认证方式相比更为安全。

(2)按照需求描述，在完成用户身份鉴别后，需依据用户身份进一步对业务数据进行安全保护，且受保护数据中包含用户私有的终端机数据文件，在基于口令的认证方式中，用户口令为用户和认证服务器共享,没有用户独有的直接秘密信息,而在基于公钥的认证方式中，可基于用户私钥对私有数据进行加密保护，实现更加简便。

(3)基于公钥体系的认证方式协议和计算更加复杂，因此其计算复杂度要高于基于口令的认证方式，但业务环境的总用户数据在 100 人以内，用户规模不大，运行环境又为局域网环境，因此基于公钥体系的认证方式可以满足平台效率要求。

【问题 2】(7 分)

针对需求(7)，项目组经过讨论，确定了基于数字信封的加密方式，其加密后的文件结构如图 5-1 所示。请结合需求说明对文件数据进行加密时，应采用对称加密的块加密方式还是流加密方式，为什么？并对该机制中的数据加密与解密过程进行描述。

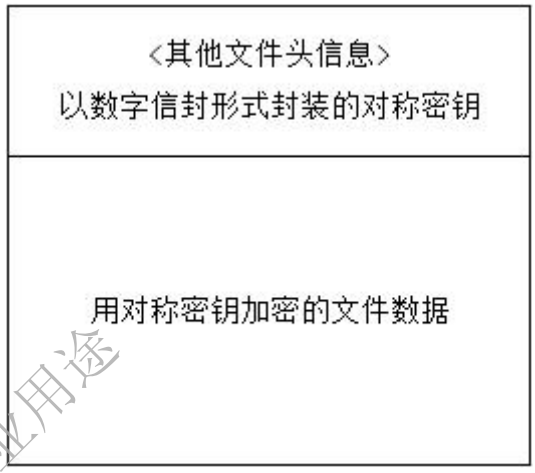


图 5-1 加密数据文件结构

【问题 2 解析】

应采用流加密方式。因为需求中提及“单个敏感数据文件可能会达到数百兆的规模”，文件数据量较大，使用流加密方式可以获得更高的加解密效率。

数据加密与解密过程如下：

其加密过程为：首先生成一个对称密钥，使用用户公钥加密这个对称密钥后存储在文件头，然后用生成的对称密钥加密文件数据存储。

其解密过程为：用户首先使用自己的私钥解密被加密的对称密钥，再用该对称密钥解密出数据原文。

【问题 3】(9 分)

对数据库服务器中的敏感关系数据进行加密保护时，客户业务系统中的敏感关系数据主要是特定数据库表中的敏感字段值，客户要求对不同程度的敏感字段采用不同强度的密钥进行防护，且加密方式应尽可能减少安全管理与应用程序的负担。目前数据库管理系统提供的基本数据加密方式主要包括加解密 API 和透明加密两种，请用 300 字以内的文字对这两种方式进行解释，并结合需求说明应采用哪种加密方式。

【问题 3 解析】

目前数据库管理系统提供的基本数据加密支持主要有以下两种：

（1）加解密 API：数据库管理系统提供可在 SQL 语句中调用的加解密 API，应用可以利用这些 API 构建自己的基础架构，对数据进行加密保护。

（2）透明加密：安全管理员为数据库敏感字段选择加密方式及密钥强度，应用访问受保护数据时只需使用口令打开或关闭密钥表，对数据的加密和解密由数据库管理系统自动完成。

加解密 API 方式的灵活性强，但构建和管理复杂；而透明加密方式管理简单，应用程序负担轻，但灵活性较差。用户要求尽可能减少安全管理与应用程序的负担，因此应选择透明加密方式。