1. 综合题(共40分，含4个小题)

Suppose the business context of an enterprise with a product center and many stores including the tasks as are shown below: 假设一个企业的业务环境包括一个产品中心和许多商店，包括如下所示的任务：

1. All of the products in each store are supplied by the product center.
2. A shopping guide help a customer plays order for some products on the scene of a store with portable equipment.
3. A shopping guide uses a portable equipment to identify each product and look through the product information in detail for helping the sale.
4. A shopping guide use a portable equipment to take stock ( 盘点 ).
5. The administrator of the store use personal computer to know something about the sales and the customers involving in the sales periodically.

1、每个商店的产品都由产品中心提供。

2、一个购物指南帮助客户在一家商店的场景中使用便携式设备，对一些产品起着订单的帮助。

3、购物指南使用便携式设备来识别每一个产品，并通过详细的产品信息来帮助销售。

4、物指南使用便携式设备进行盘点（盘点）。

5、本店的管理者使用个人计算机对销售人员和客户定期对销售情况有了解。

An IT team are asked to design a software system for the company to help the persona of the context to accomplish the tasks efficiently and effectively based on the RFID identify technology (射频识别). With this technology, the information of a product could be stored in the RFID card（A card works as the meal card does in the canteen）and detected by the portable data detect terminal of PDA with RFID Reader and Writer. The system should include four aspects of the inventory(存货清单), the sales, the stock and the returned goods as well as achieving the goals of portable shopping guide, playing order rapidly on the scene, taking stock quickly on the spot and CRM (Customer Relationship Management). IT团队被要求设计一个公司的帮助下有效地完成任务的人的软件系统和基于RFID识别技术有效（射频识别）。利用这种技术，一个产品的信息可以存储在RFID卡（一卡作为餐卡在食堂）和便携式数据检测PDA与RFID读写终端检测。该体系应包括四个方面的库存（存货清单）、销售、库存、退货以及实现便携式购物指南的目标，播放顺序迅速在现场，盘点现场快和CRM（客户关系管理）。

As a software architect, you are asked to design software architecture to achieve the goals of the system following the steps of the ADD. 作为一个软件架构师，你被要求设计软件体系结构，以实现该系统的目标，之后的步骤。

* 1. Please separately give 5 quality attribute scenarios to define the security and 5 scenarios to define the modifiability of the system (Score 10). 请分别给5个质量属性场景定义安全和5个场景，定义系统的可修改性（10分）。

As to the system described above,

Security could be defined by the 5 scenarios as follows:

1. Integrity of data: The system should deny unauthorized visit. The shopping guide cannot use PDA subsystem to revise the order that have been played.
2. Confidentiality of data: The shopping guide can read the customer information relative to play the order, but cannot read the customer information in more detail.
3. Resist attacks: The system should offer authorize the user and has an effective access control system.
4. Detect attacks: Malicious attack should be detected by the system.
5. Recover from the attacks: Should audit and trace the user’s behavior.

And modifiability could be defined by the 5 scenarios as follows:

1. Support to the modification of the PDA.
2. Support to the modification of the users and the rights of users.
3. Support to the modification of the RFID cards and the products.
4. Support to the modification of the work of flow for the tasks of playing order.
5. Support to the modification of the Database and web server.

如上所述的系统，

安全可以被定义为如下5种情况：

（1）数据的完整性：系统应拒绝未经授权的访问。导购不能使用PDA系统修改打过的订单。

（2）资料的机密性：购物指南可以读取客户信息，而不可播放该命令，但无法更详细地读取客户信息。

（3）抗攻击：系统应提供授权用户，并具有有效的存取控制系统。

（4）检测攻击：系统中的恶意攻击。

（5）从攻击中恢复：应审核和跟踪用户的行为。

和可变性可以由5种情况如下定义：

（1）支持PDA的改性。

（2）支持对用户和用户权利的修改。

（3）支持对射频识别卡及产品的修改。

（4）支持对游戏任务的工作流程的修改。

（5）支持对数据库和网络服务器的修改。

* 1. Please separately present 5 tactics to achieve the security and 5 tactics to achieve modifiability (Score 10). 2请分别提出5个策略来实现安全和5策略实现可变性（10分）。

|  |  |
| --- | --- |
| Security tactics | Modifiability tactics |
| * + - * 1. Maintain the integrity and confidentiality of the data of customer, product or order via an RBAC subsystem;         2. Provide identity authentication mechanism on the PDA;         3. Monitor user’s behavior on the server;         4. Audit the users’ behavior via the system logs；         5. Limit the exposure and access of the data.   1）维护客户数据的完整性和保密性，产品或订单通过RBAC系统；  2）提供对PDA的身份认证机制；  3）监视用户在服务器上的行为；  4）通过系统日志审核用户行为；  5）限制数据的曝光和访问。 | 1. Localize the changes by abstract common services, e.g. provide the unified identity authentication ; 2. Prevent ripple effects via hiding information; Defer the binding time via the configuration document, e.g. configure the data of enumeration； 3. Separate system into 3 parts：the data presentation, the business logic and the data accessing； 4. Use the intermediary to prevent the ripple effects.   1）本地化的变化，抽象的共同服务，例如提供统一的身份验证；  2）通过隐藏信息来防止纹波效应；通过配置文件推迟绑定时间，例如配置枚举数；  3）分系统分为3部分：数据表示、业务逻辑和数据访问；  4）利用中介机构，以防涟漪效应。 |

* 1. To trade off the usability and the security, please choose an architecture pattern for the system with detail explanations (Score 10). 为了交易的可用性和安全性，请选择一个系统的架构模式与详细的解释（得分10）。

（1）Hierarchy distribution architecture pattern could be adopted.

（2）In detail, C/S and B/S hybrid distribution pattern could be selected to trade off the usability and security for the system.

（3）Also, MVC architecture pattern could be utilized to enhance the usability of the system without losing the security.

（4）RBAC subsystem could be used to balance the usability and security.

（1）可采用分层分布结构模式。

（2）详细说明，可选择以可供选择的方式，以供系统的可用性和安全性，以供选择。

（3）另外，MVC架构模式可以用来提高系统的可用性不失安全。

（4）基于角色的访问控制子系统可以用来平衡安全性和易用性。

* 1. Please present the *component-and-connector* view of the system design based on the modeling language of UML2.0 and explain the technical rationale of the view (Score 10). 4。请提供基于UML2.0建模语言设计系统的组件和连接器的看法和解释视图的技术原理（10分）。

为了平衡易用性、安全性和可修改性。



As is shown in the picture, the system is divided into the levels as follows：

1. View level which is composed of the pages of . aspx.
2. Controller level which is composed of controller components dealing with the business logic.
3. Model level which is composed of service components dealing with service, model component, and DAO component.
4. Database level which is composed of SQL Server 2005 to store the data with persistence.
5. Service level which is also composed of service component for connection and exchanging of the data on the heterogeneous devices or system.

如图所示，系统分为以下等级：

（1）。认为一级由网页组成。aspx。

（2）由控制器组件组成的控制器级处理业务逻辑。

（3）由服务组件组成的模型级处理服务、模型组件和道组件。

（4）。数据库由SQL Server 2005数据存储的持久性。

（5）服务水平，也由服务组件组成，用于连接和交换异构设备或系统中的数据。

The technical rationale of the view includes:

1. Reference model: hierarchy model
2. Architecture pattern: the CS and BS hybrid pattern for distribution system;
3. Reference framework:
   1. WinForm GUI framework on the PDA part；
   2. Web service technology is used to exchange the data of PDA and database of SQL Server 2005.
   3. Asp .NET MVC3 framework on the PC part；
   4. ORM framework;
   5. Spring.Net MVC AOP framework：From the special business logic services, abstract the common services such as access control, system log, concurrency control, transaction processing and so on, as a result, the modifiability of the system is enhanced significantly.

视图的技术原理包括：

（1）参考模型：层次模型

（2）建筑模式：配电系统的政务和混合模式；

（3）参考框架：

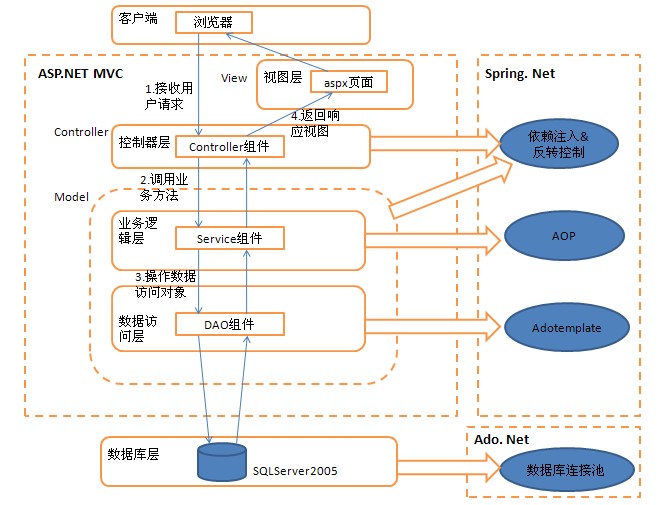
a）在PDA部分WinForm界面框架；

B）Web服务技术应用到PDA和SQL Server 2005数据库的数据交换。

c）在PC部分ASP。NET MVC3框架；

d）ORM框架；

e）Spring.NET AOP框架：MVC从特定业务逻辑服务，摘要共同服务，如访问控制、系统日志、并发控制、事务处理等，因此，系统的可修改性显著提高。



(4)The model level of the system could be divided into the following parts:

该系统的模型水平可以分为以下几个部分：

