代號：01340
頁次：4－1

111年專門職業及技術人員高等考試建築師、31類科技師（含第二次食品技師）、大地工程技師考試分階段考試（第二階段考試）暨普通考試不動產經紀人、記帳士考試試題

等　　別：高等考試
類　　科：資訊技師
科　　目：系統分析與資訊安全
考試時間：2小時　　座號：_____

※注意：㈠禁止使用電子計算器。
㈡不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。
㈢本科目除專門名詞或數理公式外，應使用本國文字作答。

一、軟體開發流程（Software development process）對於建置一個資訊系統的成功非常重要，包含需求分析、架構設計、細部設計、程式撰寫、測試與維護。

㈠請比較計畫驅動（Plan-driven）和敏捷流程（Agile processes）的特性與應用的不同點，請就溝通、文件與程式、客戶與合約、需求變更、開發階段與週期等面向說明。（15分）

㈡國際房屋仲介公司將建置系統以管理其待售房屋（House）和客戶（Customer）資訊，進行需求擷取後整理以下需求，請完成以下初步類別圖中的（I）、（II）、（III）、（IV）和所有類別的關聯。（15分）

1. 有兩種客戶，包含賣房客戶（Seller）和買房客戶（Buyer）。

2. 一個銷售人員（Sales）負責許多客戶，客戶和待售房屋資料由負責的銷售人員登錄。

3. 新的買房客戶資料登錄時

⑴ 登錄客戶姓名（Name）、年齡（Age）、電話（Tel）。

⑵ 登錄客戶對買房的條件（Criteria）資料，包含地點（Location）、類型（Type）、坪數大小（Size）、屋齡（Age）、價格（Price）。

⑶ 系統將符合標準的待售房屋加入候選房屋列表（Candidate list）。

4. 新的待售房屋資料登錄時

⑴ 登錄房屋的條件資料，包含地點（Location）、類型（Type）、坪數大小（Size）、屋齡（Age）、價格（Price）。

⑵ 列出該待售房屋符合客戶買房條件的客戶名單。

⑶ 向負責這些客戶的銷售人員發送電子郵件。

5.每位銷售人員

⑴查詢所有待售房屋的條件資料。

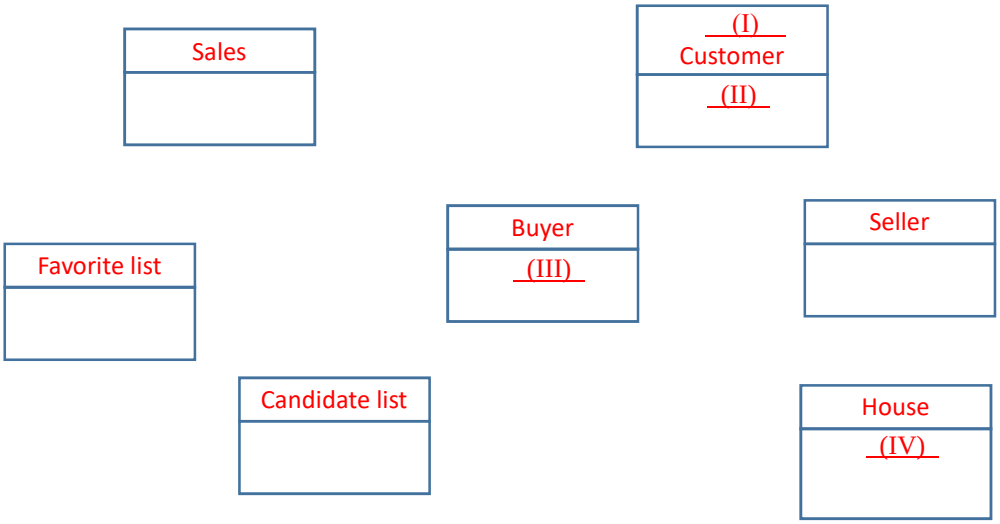
⑵查詢所負責客戶的資料。

⑶買房客戶參觀待售房屋後，若客戶喜歡，系統將其加入喜愛房屋列表（Favorite list）。

⑷房屋售出後，將其資料設定已售出，系統自動將此從客戶候選房屋列表與喜愛列表刪除。

6. 客戶

⑴查詢所有待售房屋的條件資料



二、軟體品質保證（Software quality assurance, SQA）是監控軟體開發流程以確保軟體符合品質標準（如 ISO/IEC 9126, ISO 25010）的方法。軟體品質則包含許多特性，例如效能（Performance efficiency）、相容性（Compatibility）、可使用性（Usability）、可靠性（Reliability）、安全（Security）、可維護性（Maintainability）和可移植性（Portability）等。

㈠關於軟體品質保證與軟體品質控制（Software quality Control），請比較其任務特性的不同，包含著重點、工具性、面對缺陷（Defect）的處理方式等。（10 分）

㈡請說明可維護性可分為那些子特性，並以銀行存提款系統為例，說明如何測量可維護性。（10 分）

三、IEC 62443 是針對「工業通信網路-網路和系統的 IT 安全性」（Industrial communication networks - IT security for networks and systems）國際標準。在 Part 4-1 安全產品發展生命週期需求中，特別強調「基於安全的設計（Secure by design）」之最佳實務，並且實施安全實作（Secure implementation）。

㈠請說明何謂「基於安全的設計」。（5 分）

㈡請說明何謂縱深防禦（Defense in depth design），並以網路銀行轉帳子系統為例說明如何實踐面對 SQL Injection 和 Cross-site Scripting 安全問題。（10 分）

㈢實作安全程式非常重要，請指出以下 C 函式的問題，以及如何修正。（10 分）

```
struct node {
   int value;
   struct node *next;
};
void free_list(struct node *head){
   for (struct node *p = head; p != NULL; p = p->next)
      free(p);
}
```

四、資訊系統的安全性非常重要，要落實安全的軟體生命週期，須從安全需求規格、安全設計階段著手整體資訊系統安全，並以安全程式設計原則與最佳實務撰寫程式。程式安全分類可協助開發者辨識安全問題，了解程式碼錯誤可能引發的安全問題，提升軟體安全。程式安全分類可以有：「輸入驗證及表示（Input Validation and Representation）」、「應用程式介面誤用（API Abuse）」、「安全特性（Security Features）」、「時間與狀態（Time and State）」、「錯誤處理（Error Handling）」、「程式碼品質（Code Quality）」、「封裝（Encapsulation）」等。

㈠「時間與狀態」的安全問題，是在多核心 CPU 或分散式系統中，兩個事件發生在幾乎同一時間；程式設計多執行緒（Threads）、多程序（Process）等造成執行期之時間與狀態及訊息間產生非預期的交互作用。請說明這些狀況可能導致的安全問題有那些。（5 分）

㈡「輸入驗證及表示」是程式處理使用者或外部輸入的安全性問題，請說明此問題可能導致的攻擊有那些。（10 分）

㈢「錯誤處理」不適當是十分常見的程式安全缺陷問題，請舉出兩種「錯誤處理」不適當的類別或狀況。（10 分）