

5.1 软件需求的来源

软件需求来自(所属)系统的系统用例。系统用例是系统存在的价值,即使系统用例不发生变化,也可以通过改变系统中的软件、硬件改善系统用例的实现流程,从而改进提升系统的能力。

软件需求是被系统架构设计师分配出来的,在系统设计阶段,系统架构设计师将系统的每个能力需求(系统用例)分配给相应的软件和硬件。

所以,CSCI 的用例来自系统用例的序列图。

5.2 软件是系统的部件

软件和硬件是组成系统的部件。在一个系统中,通过对软件和硬件之间的协作关系进行良好的设计,从而对系统的外部提供有价值的服务。服务的优劣自然受到软件和硬件部件的影响。

软件作为系统的部件,可以被业务工人使用,可以直接被外部涉众使用,可以被系统外部的其他系统使用,也可以被系统内部的其他部件使用。也就是说,软件用例的主执行者可以是业务工人,可以是组织的外部涉众,可以是系统外部的其他系统,也可以是系统内部的其他部件。

5.3 分析方法综述

软件需求的分析方法与系统需求的分析方法完全一致,仅仅是研究对象发生了变化。系统需求分析的研究对象是系统,软件需求分析的研究对象是软件。

按照 GJB 2786A 的要求,软件需求分析的一个依据性文件是系统设计阶段形成的“软件研制任务书”。

在软件研制任务书的基础上,将 CSCI 作为研究对象,对任务书规定的软件用例(CSCI 能力需求)进行详细分析,描述每个用例的规格。相应的工作内容记录在“软件需求规格说明”中的第 3 章的 3.1 要求的状态和方式,以及 3.2 CSCI 能力需求中。

软件需求分析的第二步工作是基于软件用例规格说明,进行外部接口分析,确定 CSCI 的外部接口的物理形式、数据协议等。相应的工作内容记录在“软件需求规格说明”中的第 3 章的 3.3 CSCI 外部接口中。

软件需求分析的第三步工作是确定软件的内部接口。此处的内部接口指该 CSCI 所包含的多个软件实体之间的接口。即在系统设计阶段,按照 GJB 2786A 定义的 CSCI 划分原则,将一些软件实体(如某些 DSP 软件和某些 FPGA 软件)的集合打包作为一个 CSCI 时,需要在此处明确这些软件实体之间的接口需求。相应的工作内容记录在《软件需求规格说明》中的第 3 章的 3.4 CSCI 内部接口中。

软件需求分析的第四步工作是确定 CSCI 内部数据需求。内部数据需求是指与功能需求相关的数据需求,即找到“问题域”中存在的业务实体,确定它们之间的逻辑关系、数量关系和结构规则。相应的工作内容记录在“软件需求规格说明”中的第 3 章的 3.5 CSCI 内部数据需求中。

软件需求分析的第五步工作是分析 CSCI 的质量因素。按照相关国标的要求,主要对 6 类 27 种质量特性进行分析。相应的工作内容记录在“软件需求规格说明”中的第 3 章的 3.6 适应性需求、3.7 安全性需求和 3.11 软件质量因素中。

软件需求分析的第六步工作是进行设计约束分析。这类约束主要包括四类:业务环境约束、使用环境约束、构建环境约束、技术环境约束。相应的工作内容记录在“软件需求规格说明”中的第 3 章的 3.12 设计和实现约束中。

5.4 分析之第一步——CSCI 能力需求分析

CSCI 能力需求分析的主要工作就是确定 CSCI 的每个用例的规格。建议用表 5-1 模板描述 CSCI 的用例规格,CSCI 用例规约与系统用例规约完全一致,只是所描述的对象不同。

表 5-1 CSCI 用例规格表

用例名称	动宾结构命名		项目唯一标识符	UC-CSCI-001
任务书章节				
简要描述	用例目标简述：CSCI 用例的职责			
参与者	主执行者：必须有主执行者。主执行者包括三类：时间、外部系统（软件、硬件）和人（业务工人、组织外的人） 辅助执行者：视具体情况而定，也可以没有辅助执行者			
前置条件	用例开始前 CSCI 需要满足的约束，且是 CSCI 能够检测到的			
主流程（代表用例核心价值的路径）	步骤	描 述		
	1	主语是主执行者		
	2	(1) 一定聚焦于 CSCI 与外部的交互过程 (2) 不要没有主语，且主语只能是主执行者或 CSCI (3) 使用主动语句，突出主语承担的责任 (4) 使用 CSCI 所属系统的领域（核心域）的词语 (5) 不要描述交互过程中设计的细节 (6) 不要描述 CSCI 不能负责的事情		
扩展流程	1a	对应基本流程中某个步骤中，CSCI 要处理的意外和分支 注意：扩展一定是动作选项，不能是数据选项。因为扩展将改变用例的流程，选择不同的数据并不能改变用例的流程，就不是扩展		
	1a1	针对 1a 所描述的意外，CSCI 的处理过程		
子流程		对应基本流程中多次重复的一组步骤集合		
后置条件	用例结束后，CSCI 需要满足的约束，且是 CSCI 能够检测到的			
规则与约束	业务规则、数据约束、性能需求等			

仍然用 3.4.4 节的自动售饮料机为例,3.4.4 节演示了系统用例规约,本节演示自动售饮料机的控制软件的用例规约。

根据 3.4.4 节的自动售饮料机的系统用例——售卖饮料用例(见表 3-3),进行系统设计,规划出以下几个系统部件:投币装置、饮料推送装置、找零装置、控制软件;使用 UML 序列图对用例进行交互建模后,得到控制软件的用例:售卖饮料,其用例规约见表 5-2。

需要说明的是,这仅仅是个示例,与实际自动饮料售卖机没有任何关系。

表 5-2 自动售饮料机控制软件的用例——售卖饮料用例规约表

用例名称	售卖饮料		项目唯一标识符	UC-CSCI-001
研制要求章节				
简要描述	软件收到投币装置开始售卖信号后,经过与顾客交互,驱动饮料推送装置输出饮料,驱动找零装置退出零钱			
参与者	主执行者: 投币装置 辅助执行者: 顾客、推送装置、找零装置			
前置条件	无			
主 流 程	步骤	描 述		
	1	投币装置向软件发送售卖信号		
	2	软件启动计时 T1,验证售卖信号为“开始售卖”		
	3	软件根据硬币数量,计算金额		
	4	软件提示饮料种类,开始计时 T2		
	5	顾客选择饮料种类		
	6	软件检查顾客选择饮料的库存		
	7	软件检查记录的找零信息		
	8	软件请求饮料推送装置推送购买的饮料		
	9	软件记录相应饮料数量、库存零钱数额		
扩展流程 1	2a	信号为“投入硬币不足”		
	2a1	软件提示继续投币,回到主流程 1		
	2b	T1 时间内未收到投币装置发送的开始售卖信号		
	2b1	软件提示超时,并请求投币装置退出已投入硬币,结束用例		
扩展流程 2	3a	需要找零		
	3a1	软件检查所记录的 5 角零钱数额		
	3a2	软件记录需要找零的金额		
	3a1-a	零钱不足		
	3a1-a1	软件提示无零钱,并请求投币装置退出已投入硬币,用例结束		
扩展流程 3	5a	T2 时间内,顾客未选择饮料种类		
	5a1	软件请求投币装置退出已投入硬币,用例结束		
	5b	顾客取消购买		
	5b1	软件请求投币装置退出已投入硬币,用例结束		
扩展流程 4	6a	顾客选择的饮料已售空		
	6a1	软件提示所选饮料已售空		
	6a2	返回主流程 4		
扩展流程 5	8a	需找零		
	8a1	软件请求找零装置退出找零金额的硬币		
子流程		无		

续表

后置条件	饮料数量、库存零钱数额发生变更
规则与约束	(1) 饮料种类包括：可乐、雪碧、红茶，单价 1.50 元 (2) 找零只有 5 角硬币 (3) 投币装置发送的“售卖信号”包括： ① “开始售卖”信号=“开始售卖”+1 元硬币数量+5 角硬币数量 ② “投入硬币不足”信号

5.5 分析之第二步——CSCI 外部接口需求分析

CSCI 的外部接口是指该 CSCI 与系统外部，以及系统内部的其他硬件和软件之间的接口。

首先，确定 CSCI 外部接口图。CSCI 的外部接口图来自 CSCI 的用例图，即 CSCI 用例图中的主执行者和辅助执行者一定是 CSCI 的外部接口图中对应的外部实体对象。

与系统外部接口分析同理，要避免出现以下几类问题。

(1) CSCI 外部接口图中出现的均应该是物理实体，不能在接口的两端出现“某接口”“某数据”“某信息”之类的非实体对象。

(2) 外部接口图中要如实体现接口的物理形态，如以太网、串口、I/O 口等，且数量要与实际一致，不要将多路同物理形态的接口合并为一个。

之后，根据外部接口图给出全部外部接口的概述，见表 5-3。

表 5-3 CSCI 外部接口描述

序号	接口名称	标识	接口类型	接口用途	涉及的用例	外部实体名称	外部实体状态
			网络、串口、CAN 总线、I/O 口等				新研、改进、复用

其中，接口用途需要描述该接口上交互的数据，以及交互数据的目的。需要注意的是，在一个接口上，需要交互不同的数据，以支持不同的 CSCI 用例，所以此处需要分开详细描述。

最后，确定每个接口的规格，见表 5-4。

表 5-4 某接口说明

接口名称	某接口	接口标识	JK-OU-001
接口实体	接口两端的软件或硬件	接口类型	网络等
接口用途	简述接口两端的软件或硬件使用该接口的用途		
接口数据	(1) 说明该接口上传输数据的种类 (2) 说明该接口上传输数据的编码格式：如果每类数据使用相同的编码格式，用其他的表说明该格式；否则，逐一说明每类数据使用的编码格式；如果编码格式为标准格式，说明即可 (3) 说明每类数据的具体格式定义。如果数据较多，可以在附录中或使用 GJB 438B 的“接口设计说明”模板详细说明		

续表

接口通信特征	通信链路	如网络的带宽、串口速率等
	数据传输	非周期/周期性、单向或双向传输
接口协议特征	说明接口是否有同步机制,详细说明同步机制是如何设计的 接口上的每类数据的传输层协议等	

5.6 分析之第三步——CSCI 内部接口需求分析

CSCI 内部接口包含两种情况：一是当 CSCI 是单个软件实体时,CSCI 的内部接口就是指该软件的部件之间的接口；二是当 CSCI 是多个软件实体的集合时,CSCI 的内部接口就是指这些软件实体之间的接口。

在软件需求分析活动中,CSCI 应该被当作黑盒对待。因此,对第一种情况,CSCI 的内部组成部件还没有被软件架构设计师设计出来,其内部接口无法明确,需留待软件设计时明确。对第二种情况,参照 CSCI 外部接口分析的内容进行分析即可。

5.7 分析之第四步——CSCI 内部数据需求分析

CSCI 内部数据需求是指从 CSCI 用例中提取的相关数据需求,用 UML 的类表示就是指实体类,即 CSCI 用例的基本流程实现中的主要承载实体。一个用例可以有多个实体类参与,一个实体类也可以参与多个用例。

内部数据需求分析的目标是找到“问题域”中存在的实体类,确定它们之间的逻辑关系、数量关系和结构规则。可以用 UML 的类图表示这些实体类之间的关系。

此时的类图关注的重点是数据需求,即只关心类和类的属性,不关心类的操作。

对嵌入式软件而言,内部数据需求分析方法相同,只是此时分析得到的实体类在软件设计时,映射为软件的全局变量。例如,一个 8 门礼花炮点火控制软件,由于每门礼花炮的空中爆炸时间不同,需要按照射手设置的每门礼花炮的发射时间点火。因此,软件需要掌握每门礼花炮的相关信息:是否有礼花炮、是否需要发射、礼花炮的发射时间。这个实体类在软件设计阶段映射为一个全局结构数组。

```
struct{
uint yp;           //是否有礼花炮
uint fs;           //是否需要发射
uint tm;           //礼花炮的发射时间
}pao[8];
```

5.8 分析之第五步——软件质量因素分析

按照 GJB 438B 要求“本条应描述合同(或软件研制任务书)规定的或由较高一级规格说明派生出的软件质量因素方面的 CSCI 需求(若有)。用例包括有关 CSCI 功能性、可靠性、易用性、效率、维护性、可移植性和其他属性的定量要求。”

分析方法与 3.8 节介绍的系统质量因素分析方法相同,只是研究对象从“系统”换为“CSCI”。同样需要强调此处应遵循“万事皆可度量”的原则,以满足 GJB 438B 要求的“定量要求”。

5.9 分析之第六步——设计和实现约束分析

软件设计约束的分析方法与 3.9 节介绍的系统设计约束分析方法相同,只是研究对象从“系统”换为“CSCI”。

软件设计约束可能包括:界面样式(如网络交换机设备统型要求的人机交互界面样式)、报表格式、第三方开发平台、开发语言等。

5.10 软件需求规格说明模板解析

5.10.1 范围

范围的主要内容包括:标识、系统概述、系统历史、项目的各相关方、适用的 CSCI、软件概述。

1. 标识

- (1) 系统名称:按照合同中名称定义。
- (2) 系统标识:按照项目总体单位要求标识。
- (3) 系统版本:按照项目总体单位要求定义。
- (4) 系统简称:缩略名。

2. 系统概述

- (1) 系统所属的组织机构。
- (2) 该组织机构的职责。
- (3) 该组织机构中使用系统的业务工人角色。
- (4) 系统的主要用途。

3. 系统历史

概述系统开发、运行和维护历史。

系统分为两种情况:一是该类组织中以前没有此类系统,完全是新研制系统;二是该类组织中以前有此类系统,这次研制的系统是对原系统的改进。

对第一种情况,无系统历史信息。对第二种情况,应说明原系统的相关信息,包括:研制总体单位、鉴定时间、运行期间发生的变更情况等。

4. 项目的各相关方

- (1) 需方:出资研制系统的机构。
- (2) 用户:最终使用系统的机构。
- (3) 使用总体:系统能力需求的论证机构。
- (4) 研制总体:系统的总承包方。
- (5) 开发方:系统的承研方和分承研方。
- (6) 保障机构:系统交付后负责保障维护的机构。

5. 适用的 CSCI

示例如表 5-5 所示。

表 5-5 适用的 CSCI 列表(示例)

CSCI 名称	CSCI 标识	CSCI 包含的软件	版本	技术状态
此处的名称、标识必须与系统设计说明完全一致				新研、改进、货架、沿用

6. 软件概述

(1) 用图说明本 CSCI 在系统/子系统物理位置；可以直接使用系统设计说明文档的系统部件章节中的系统结构图的局部。

(2) 概述 CSCI 的用途。

5.10.2 需求

需求是软件需求规格说明文档的主要内容。需求包括三类：功能需求、质量因素和设计约束。

在 GJB 438B 模板中的对应关系如下。

(1) 模板的 3.2 CSCI 能力需求是指软件的功能需求。

(2) 模板的 3.6 适应性需求、3.7 安全性需求、3.8 保密性需求、3.11 系统质量因素和 3.13 人员需求是质量因素类需求。

(3) 模板的 3.12 设计和实现约束是指设计约束类需求。

(4) 模板的 3.1 要求的状态和方式是与软件使用要求(用途)密切相关的要求。

(5) 模板的 3.3 CSCI 外部接口需求、3.4 CSCI 内部接口需求和 3.5 CSCI 内部数据需求是支撑功能需求的接口需求和数据需求。

(6) 模板的 3.9 CSCI 环境需求和 3.10 计算机资源需求是指 CSCI 运行所依赖的计算机软件和硬件资源需求。

(7) 模板的 3.14 培训需求、3.15 保障需求、3.16 其他需求、3.17 包装需求等主要是指支持软件交付的需求。

1. 要求的状态和方式

(1) CSCI 仅有一种运行状态时,对该状态进行描述即可。

(2) CSCI 有多种运行方式和状态时,可先用表 5-6 说明方式与状态的关系。

表 5-6 要求的状态和方式(示例)

	方式 1	方式 2	方式 3
状态 1	√		
状态 2		√	
状态 3		√	√

(3) 用文字或状态图说明这些状态/方式之间如何转换。

(4) CSCI 有多种运行方式或状态时,需按表 5-7 说明本文的需求在哪个状态/方式下有效。

表 5-7 要求的状态和方式与 CSCI 能力关系(示例)

	状态 1	状态 2	状态 3
用例 1	√		
用例 2		√	
用例 3		√	√

2. CSCI 能力需求

(1) 如果本 CSCI 在系统设计阶段已经明确的任务中包含多个软件,则在此处用 UML 构件图说明这些软件之间的关系,如图 5-1 所示。

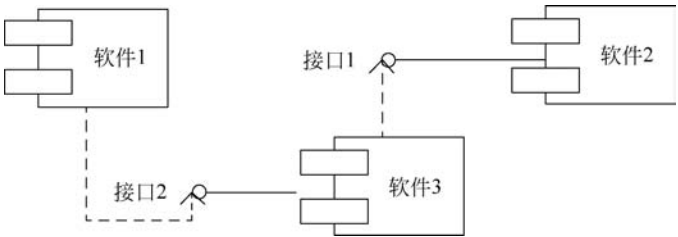


图 5-1 CSCI 包含软件之间的关系(示例)

(2) 用表格说明 CSCI 所包含的软件用途,如表 5-8 所示。

表 5-8 CSCI 包含的软件(示例)

软件名称	软件标识	版本	软件用途	技术状态
软件 1				新研/改进/沿用/货架
软件 2				

(3) 画出 CSCI 的 UML 用例图(见图 5-2),并列表说明各个用例(见表 5-9)。

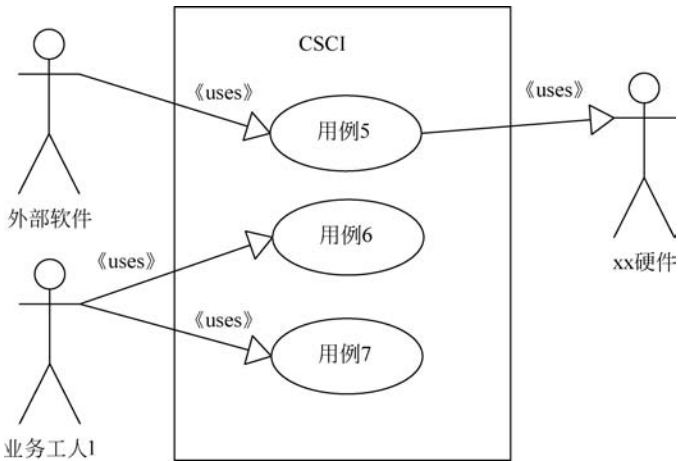


图 5-2 CSCI 用例图(示例)

表 5-9 CSCI 的用例列表(示例)

序 号	用 例 名 称	标 识	功 能 描 述	技 术 状 态
1	用例 1			新研/改进/沿用
2	用例 2			

(4) 按照要求,以每个 CSCI 用例为小章节分条说明 CSCI 能力需求。每个 CSCI 用例使用如下 CSCI 用例规约表进行描述,见表 5-10。

表 5-10 CSCI 用例规约表(示例)

用例名称	动宾结构命名		项目唯一标识符	UC-CSCI-001
研制要求章节				
简要描述	用例目标简述：CSCI 用例的职责			
参与者	主执行者：必须有主执行者。主执行者包括三类：时间、外部系统(软件、硬件)和人(业务工人、组织外的人) 辅助执行者：视具体情况而定,可以没有辅助执行者			
前置条件	该用例开始前,CSCI 需要满足的约束,且是 CSCI 能够检测到的			
主流程(代表用例核心价值的 路径)	步骤	描 述		
	1	主语是主执行者		
	2	(1) 一定聚焦于 CSCI 与外部的交互过程 (2) 不要没有主语,且主语只能是主执行者或 CSCI (3) 使用主动语句,突出主语承担的责任 (4) 使用 CSCI 所属系统的领域(核心域)的词语 (5) 不要描述交互过程中设计的细节 (6) 不要描述 CSCI 不能负责的事情		
扩展流程	1a	对应基本流程中某个步骤中,CSCI 要处理的意外和分支。 注意：扩展一定是动作选项,不能是数据选项。因为扩展将改变用例的流程,选择不同的数据并不能改变用例的流程,就不是扩展		
	1a1	针对 1a 所描述的意外,CSCI 的处理过程		
子流程		对应基本流程中多次重复的一组步骤集合		
后置条件	该用例结束后,CSCI 需要满足的约束,且是 CSCI 能够检测到的			
规则与约束	业务规则、数据约束、性能需求等			

3. CSCI 外部接口需求

(1) 画出 CSCI 与软件外部的其他硬件和软件之间的接口图。注意: 此处的外部接口图应该与系统设计说明的系统内部接口图中与此 CSCI 相关部分的描述完全一致。

(2) 使用表 5-11 说明 CSCI 外部接口的相关信息。注意: 表 5-11 内容应该与系统设计说明的系统内部接口的描述完全一致。

表 5-11 CSCI 外部接口需求表(示例)

序号	接口名称	标识	接口类型	接口用途	外部接口实体	外部接口实体状态

(3) 对识别的接口逐条进行说明。

注意,表 5-12 中内容应与系统设计说明的系统内部接口的描述完全一致。

表 5-12 接口需求表(示例)

接口名称	某接口		接口标识	JK-OU-001
接口实体	接口两端的软件或硬件		接口类型	网络等
接口用途	简述接口两端的软件或硬件使用该接口的用途			
接口数据	(1) 说明该接口上传输数据的种类 (2) 说明该接口上传输的数据的编码格式：如果每类数据使用相同的编码格式,用其他的表说明该格式；否则,逐一说明每类数据使用的编码格式；如果编码格式为标准格式,说明即可 (3) 说明每类数据的具体定义。如果数据较多,可以在附录中或使用 GJB 438B 的“接口设计说明”模板详细说明			
接口通信特征	通信链路	如网络的带宽、串口速率等		
	数据传输	非周期/周期性、单向或双向传输		
接口协议特征	说明接口是否有同步机制,详细说明同步机制是如何设计的 接口上的每类数据的传输层协议等			

4. CSCI 内部接口需求

(1) 如果本 CSCI 在系统设计阶段已经明确的任务中仅包含一个软件,或暂时无法明确软件个数,需要在 CSCI 软件设计阶段确定的,此处可留待设计时描述。

(2) 如果本 CSCI 在系统设计阶段已经明确的任务中包含多个软件,则应说明该 CSCI 包含的每个软件之间的接口。

(3) 画出 CSCI 所包含的软件之间的接口。

(4) 用接口需求表说明 CSCI 所包含的软件之间接口的相关信息。

5. CSCI 内部数据需求

(1) 从各个 CSCI 用例中找出软件需要处理的实体类。

(2) 画出 CSCI 所包含的实体类的 UML 类图,如图 5-3 所示。

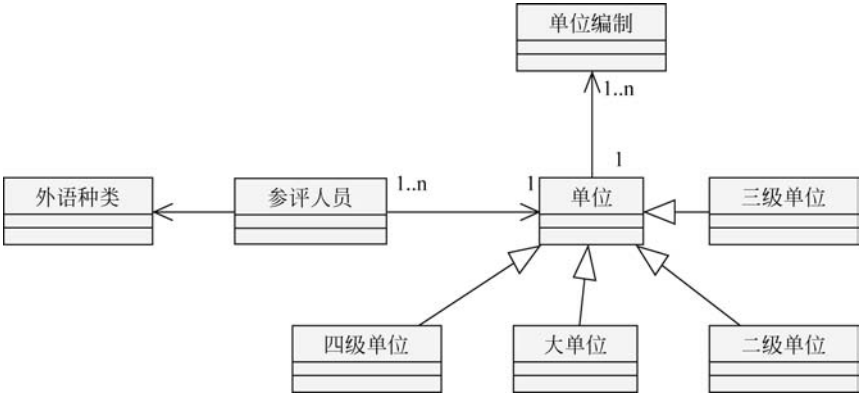


图 5-3 CSCI 类图(示例)

(3) 用表格说明所有实体类的相关信息,如表 5-13 所示。

表 5-13 CSCI 的内部类列表(示例)

序 号	类 名 称	标 识	涉及的用例
			是指该类在哪些软件用例中出现

(4) 逐条说明识别出的每个类的数据需求,见表 5-14。

表 5-14 某类(示例)

序号	属性名称	取值范围	精度要求	组成格式	是否为公共属性
		是指具有物理意义的取值范围		使用数据字典的词条法表示: =、+、[/]、()、* ... *、{ } ⁿ (重复次数) 如: 编号由 2 位字母、6 位数字和 1 个可选 <i>x</i> 组成。编号 = {[A...Z/a...z]} ² + {0...9} ⁶ + (<i>x</i>)	CSCI 的公共数据的来源

6. 适应性需求

GJB 438B 原文要求“本条应描述关于 CSCI 将提供的与安装有关的数据(如场地的经纬度或场地所在地的赋税代码)的需求(若有),应指定对要求 CSCI 使用的运行参数(如指明与运行有关的目标常数或数据记录的参数)的需求,这些运行参数可以根据运行需要而改变。”

提示: 是指在不同用户现场安装时需要修改的安装数据,并指明这些参数涉及的 CSCI,如地理数据配置文件、菜单配置文件、通信端口参数等。

例如,某电机控制软件可以部署运行在一个系统的多处电机的控制板上,软件运行时需要加载不同的配置文件,根据配置参数自主适配不同的电机。那么,该软件的适应性需求就应说明配置文件参数如何适配不同的电机。

7. 安全性需求

GJB 438B 原文要求“本条应描述关于防止或尽可能降低对人员、财产和物理环境产生意外危险的 CSCI 需求(若有)。”

提示:

(1) 要从本软件自身的安全性上考虑,而非外界提供的安全措施(如全系统的网络安全等)。

(2) 软件自身安全性主要体现在两方面: ①防止恶意入侵的安全性,如防止非法用户登录的需求、防止数据库核心数据被篡改的需求、防止保存在本地的数据文件被篡改的需求、防止数据丢失后软件无法运行的需求、防止重要作战指令被误发的需求等; ②防止人员、设备受到伤害的安全性,如意外地发出一个“自动驾驶关闭”命令,软件没有进行安全连锁判断或提示飞行员确认的前提下直接执行了该指令,可能导致飞机失事。

(3) 安全性需求要明确,要具备可测试性。

(4) 不要混淆需求和解决方案。

例如,某 CSCI 的安全性需求为“在软件的入口、出口及其他关键点上,应对重要的物理

量进行合理性检查,并采取措施进行处理,以便进行故障隔离。”

这条安全性需求存在以下问题。

首先,不符合安全性需求定义的两条原则,不属于安全性需求范畴。

其次,需求描述不明确,“其他关键点”和“重要的物理量”等没有明确的定义,软件架构设计人员难以对此条需求给出有效的设计决策;测试人员更是难以确定测试内容。

另外,有混淆需求和设计的嫌疑。这条描述已经站在了“解决方案域”内,给出的是一种检查输入输出数据是否合理的方案,但是这条方案针对的是什么需求并不明确。

8. 保密性需求

GJB 438B 原文要求“本条应描述与维护保密性有关的 CSCI 需求(若有)。(若适用)这些需求应包括: CSCI 必须在其中运行的保密性环境、所提供的保密性的类型和级别、CSCI 必须经受的保密性风险、减少此类风险所需的安全措施、必须遵循的保密性政策、CSCI 必须具备的保密性责任、保密性认证/认可必须满足的准则等。”

提示: 保密性需求是指 CSCI 使用环境中是否存在数据存储、销毁、传输等保密性需求。

另外需要注意的是,需求都应是明确的要求,而非笼统的要求。例如,保密性需求“在紧急情况下,需要销毁重要数据”就是不明确的需求,应该明确说明销毁哪些重要数据。

9. CSCI 环境需求

提示: 此处的 CSCI 环境需求应与系统设计说明的软件部件的运行环境保持一致。

CSCI 运行环境需求表示例见表 5-15 所示。

表 5-15 CSCI 运行环境需求表(示例)

序号	硬件名称	类 型	软件名称	类 型
		处理器、存储器、输入/输出设备、辅助存储器、通信/网络设备		操作系统、地理信息系统、数据库系统、Office 办公软件、通信软件、框架软件、其他第三方软件等

10. 计算机资源需求

1) 计算机硬件需求

GJB 438B 原文要求“本条应描述针对本 CSCI 必须使用的计算机硬件的需求(若有)。(若适合)这些需求应包括: 各类设备的数量; 处理机、存储器、输入/输出设备、辅助存储器、通信/网络设备及所需其他设备的类型、大小、容量和其他所需的特征。”

提示: 对 CSCI 环境需求中的计算机硬件需求进行详细说明。

计算机硬件需求表示例如表 5-16 所示。

表 5-16 计算机硬件需求表(示例)

序号	硬件名称	类 型	资源配置说明	来 源	数 量
		处理器、存储器、输入/输出设备、辅助存储器、通信/网络设备			

2) 计算机硬件资源使用需求

GJB 438B 原文要求“本条应描述本 CSCI 的计算机硬件资源使用需求(若有),例如:最大允许利用的处理机能力、内存容量、输入/输出设备的能力、辅助存储设备容量和通信/网络设备的能力。这些需求(例如陈述为每一个计算机硬件资源能力的百分比)应包括测量资源使用时所处的条件(若有)。”

提示:对计算机硬件需求中的各项硬件的使用要求进行详细说明。

计算机硬件资源使用需求表示例如表 5-17 所示。

表 5-17 计算机硬件资源使用需求表(示例)

序号	硬件名称	类 型	使 用 要 求	备 注
		处理器、存储器、输入/输出设备、辅助存储器、通信/网络设备	软件占用 CPU、内存余量要求、占用带宽要求	

3) 计算机软件需求

GJB 438B 原文要求“本条应描述本 CSCI 必须使用或必须被并入本 CSCI 的计算机软件的需求(若有)。例子包括:操作系统、数据库管理系统、通信/网络软件、实用软件、输入和设备仿真软件、测试软件和制造软件。要列出每一个这样的软件项的正确名称、版本和参考文档。”

提示:对 CSCI 环境需求中的计算机软件需求进行详细说明。

计算机软件需求表示例如表 5-18 所示。

表 5-18 计算机软件需求表(示例)

序号	软件名称	类 型	版 本	来 源	备注
		操作系统、地理信息系统、数据库系统、通信/网络软件、实用软件、输入和设备仿真软件		自备、自研、货架、第三方提供	

4) 计算机通信需求

GJB 438B 原文要求“本条应描述本 CSCI 必须使用的计算机通信方面的需求(若有)。例子包括:要连接的地理位置;配置和网络拓扑;传输技术;数据传送速率;网关;要求的系统使用时间;被传送/接收的数据的类型和容量;传送/接收/响应的时间限制;数据量的峰值;以及诊断特性。”

提示:这条要求应该是指 CSCI 在运行环境中,与其他软件和硬件进行通信的需求,这个已经属于系统内部的通信需求。例如,CSCI 通过什么速率的串口与其他 CSCI 通信;如果通过 CAN 总线与其他 CSCI 通信,对传送/接收的数据容量是否有要求;使用 IO 口通信是否有诊断特性需求等。

11. 软件质量因素

GJB 438B 原文要求“本条应描述合同(或软件研制任务书)规定的或由较高一级规格说明派生出的软件质量因素方面的 CSCI 需求(若有)。例子包括有关 CSCI 功能性、可靠性、易用性、效率、维护性、可移植性和其他属性的定量要求。”

提示:此处的软件质量因素原则上直接来源于软件研制任务书的要求;也可以结合系

统规格说明中与本 CSCI 相关的质量属性进行分析。质量因素分析示例见表 5-19。

表 5-19 软件质量因素表(示例)

质量属性类型	质量子特性	CSCI 的质量因素要求
功能性	安全性 ZL-AQ	访问安全性
		数据安全性
		通信安全性
可靠性	容错性 ZL-RC	接口容错要求
		人为输入容错要求
		降级使用要求；如情报质量差时的相关能力需求
		在关键能力需求中能够识别控制的故障模式
	易恢复性 ZL-HF	数据备份与恢复要求
		软件失效后重新启动需恢复至失效前状态
		硬件网络设备重启动,软件需自动恢复与外部连接
易用性	易操作性 ZL-CZ	完成一次业务操作的时间要求
		完成一次业务操作页面流转的次数
		人机交互界面组织符合业务逻辑
效率	资源特性 ZL-ZY	数据存储量
		数据库访问量
		数据传输量
	时间特性 ZL-SJ	服务调用时间
		关键算法时间
维护性	易分析性 ZL-FX	诊断缺陷的粒度
	易改变性 ZL-GB	功能易改变
		数据易改变
		流程易改变
可移植性	适应性 ZL-SY	操作系统兼容性
		同一个 CSCI 可适用于不同对象；例如,卫星状态监测软件适用于不同卫星；电机控制软件适用于不同位置的电机
	易安装性 ZL-AZ	一键安装、在线更新

示例 1,某星载嵌入式软件,其可靠性需求为“为防止空间单粒子效应,软件应有措施保证每次加载正确的程序。”针对这条需求,软件设计人员给出设计决策为“存储在 Flash 中的程序代码采用三备份存储,当程序装载时采用三取二判决进行装载。”

示例 2,对关键等级较高的嵌入式软件,通常都有恢复性需求“软件在故障后能够恢复运行”。针对这条需求,软件设计人员给出设计决策为“采用硬件看门狗,软件定时喂狗,若超时则软件被重新启动。”

12. 设计和实现约束

提示：四类约束＝业务环境约束＋使用环境约束＋构建环境约束＋技术环境约束。这四类约束分布在不同层面的需求。

业务环境约束。属于业务级需求,来自出资方的约束,如上线时间、预算、集成、业务规则、行业法律法规(禁止使用解释性编程语言)等；由出资方指定技术选型(某平台、必须使用某数据库系统、必须遵循某数据标准、应与原某系统集成、应与某系统互连互通等)。

使用环境约束。属于用户级需求,来自使用方的约束,如使用者的专业能力、何种人群、分布式使用、使用环境有电磁干扰、车船移动等因素。

构建环境约束。属于开发级需求,来自开发和维护人员的约束,如开发人员的技术水平、业务知识、管理水平等。

技术环境因素。来自业界当前技术环境约束,如技术平台、中间件、编程语言成熟度等。

13. 人员需求

GJB 438B 原文要求“本条应描述与使用或支持本 CSCI 的人员有关的需求(若有)”。

注意: 本条不应该描述与开发人员相关的需求,也不是单纯描述 CSCI 使用人员的数量、技能需求。

本条的目的是通过对软件使用或支持人员的数量、技能等信息进行分析,得到对 CSCI 质量因素方面的需求。例如“允许多少用户同时使用”等。

14. 培训需求

对具备人机交互界面的软件而言,对使用人员进行培训是有必要的。所以,本条应该描述与培训相关的需求。例如,需要培训的操作人员(角色)、数量、培训使用的教材(包括操作手册、用户手册、电子交互手册,以及其他教材)等。

注意: 本条不是对软件使用方提出需求,而是站在需求方的角度,对系统研制方提出培训需求,要求研制方对软件使用方进行培训,要求研制方提供合适有效的培训资料。

15. 软件保障需求

GJB 438B 原文要求“本条应描述与软件保障考虑有关的 CSCI 需求,这些考虑可以包括:对系统维护、软件保障、系统运输方式、对现有设施的影响和对现有设备的影响”。

本条的目的通过对软件交付后,如何使得软件保障机构能够保障软件正常运转进行分析,得到与保障工作相关的软件质量因素方面的需求。

注意: 本条不是对软件保障机构提要求,而是站在需方的角度,对软件研制方提出要求,要求研制方基于软件的维护保障工作的顺利实施,分析本 CSCI 需要承担的职责。

16. 其他需求

GJB 438B 原文要求“本条应描述上述各条未能覆盖的其他 CSCI 需求(若有)”。

这条的目的是如果需方还有在合同中,以及上述需求中未覆盖到的其他需求,包括研制方应提供的文档需求,可以在本条进行说明。

17. 包装需求

GJB 438B 原文要求“本条应描述为了交付而对 CSCI 进行包装、加标记和处理的需求(若有)”。

这条的目的很明确,站在需方或研制总承包方的角度,对 CSCI 交付时的包装提出要求。例如,以光盘为载体交付程序安装包,光盘外包装上应贴标签,标签应明示软件名称、标识、版本、时间、厂家、联系人等信息;以纸质为载体提交需交付的软件用户手册,手册的外包装要求等。

18. 需求的优先顺序和关键程度

GJB 438B 原文要求“本条(若适用)应描述本文档中诸需求的优先顺序、关键程度或所赋予的指示其相对重要性的权重”。

这条包含两方面的要求,一是需求的优先次序,优先次序是研制方优先实现 CSCI 需求

的依据；二是需求的关键性,关键性是研制方需要特别关注是否需要特殊处理(如 CSCI 设计时需要给出专门的设计决策等)的依据。

例如,优先顺序定义为 1 和 2。1 是需要优先实现的基本需求；2 是增强需求。

CSCI 需求的关键程度通常来自系统需求的关键程度。系统需求的关键程度是从系统安全性和保密性角度考虑的,建议由高至低分为三个等级(A、B、C)。

在系统设计阶段,由系统架构设计师将系统的每个能力需求(系统用例)分配给相应的软件和硬件。所以,CSCI 需求是从属于某个系统需求的,其关键程度等同于相应的系统需求的关键程度。

需求优先顺序和关键程度列表例如表 5-20 所示。

表 5-20 需求优先顺序和关键程度列表(示例)

序 号	需求 名称	需求 标识	优先 顺序	关 键 程 度

5.10.3 合格性规定

GJB 438B 原文要求“本条应描述所定义的合格性方法,并为第 3 章中的每个需求指定为确保需求得到满足所应使用的方法”。

合格性规定是 CSCI 合格性测试的依据。按照 GJB 2786A 的要求,CSCI 合格性测试应具有独立性(即必须由独立于 CSCI 研制团队的人员承担 CSCI 合格性测试)。本条的目的是站在需方的角度,为每条 CSCI 需求提出验证其合格性的方法。

GJB 438B 提出的合格性方法包括：演示、测试、分析、审查和特殊的合格性方法。详见表 5-21。

表 5-21 合格性规定(示例)

序号	需求 名称	需求 标识	合格性方法
1			演示
2			使用某测试设备进行测试
3			分析某测试结果数据
4			审查某源代码
5			审查某文档

5.10.4 需求可追踪性

使用正向追踪表,说明系统的每个需求(系统/子系统规格说明中的三类需求)和本 CSCI 的能力需求(软件需求规格说明中的三类需求)的对应关系。

使用逆向追踪表,说明本 CSCI 的每个软件需求(软件需求规格说明中的三类需求)来自哪些系统需求。

思 考 题

112

题目 1 为什么从自动售饮料机的系统用例中得到的软件用例是一个,而不是两个或三个,如“取消购买”不是系统用例吗?

题目 2 软件用例和系统用例有何关系?

6.1 CSCI 级设计决策

GJB 438B 中明确指出 CSCI 级设计决策包括两部分内容,一是“CSCI 行为设计的决策”,即“忽略其内部实现,从用户角度出发描述系统将怎样运转以满足需求”;二是“其他影响组成该 CSCI 的软件单元的选择与设计的决策”。

这段话中,对 CSCI 而言,更准确的说法应该是“忽略其内部实现,从 CSCI 外部角度出发描述 CSCI 将怎样运转以满足其需求”。

从 GJB 438B 的要求看,CSCI 级设计决策和系统级设计决策比较,除了研究对象不同:一个是 CSCI,一个是系统,研究内容和研究方法并没有大的区别。

因此,参考 4.1 系统架构设计方法,CSCI 级设计决策过程同样包括与需求对接阶段和概念架构设计阶段。

第一阶段,与需求对接阶段。采用需求矩阵分析方法得到三类需求中的关键性需求。

第二阶段,概念架构设计阶段。对于 CSCI 来说,概念架构设计的主要任务是基于 CSCI 级关键需求矩阵,确定 CSCI 级概念架构和设计决策。其实,CSCI 级概念架构就是设计决策的一种——CSCI 行为设计决策,即“忽略其内部实现,从 CSCI 外部角度出发描述 CSCI 将怎样运转以满足其关键功能需求”。

(1) 对使用环境约束和开发环境约束,给出 CSCI 级设计决策。

(2) 对关键功能,给出 CSCI 概念性架构设计决策。

(3) 采用目标-场景-决策表考虑关键质量属性,调整和完善概念架构设计决策。

6.2 CSCI 体系结构设计

CSCI 体系结构设计是指对 CSCI 的每个用例的行为的内部实现进行设计,设计的结果一定是模块化的软件单元(类或函数),以及这些软件单元之间的协作关系,即静态关系和动态关系。

6.2.1 CSCI 部件

CSCI 部件是指构成这个 CSCI 的软件单元。按照 GJB 2786A 的定义“软件单元可以出现在层次结构的不同层上,并可以由其他软件单元组成。”

这句话包含两层意思,一是 CSCI 部件应该按照层次组织,分层结构能够保证层与层之