

<项目名称/首字母缩略词>

# 系统设计文档

版本 XX

月/日/年

目录

[一、](#_Toc7163744) [简介](#_Toc7163744) [1](#_Toc7163744)

[1.1](#_Toc7163745)  [SDD 的目的](#_Toc7163745) [1](#_Toc7163745)

[2.](#_Toc7163746) [总体概述和设计指南/方法](#_Toc7163746) [2](#_Toc7163746)

[2.1](#_Toc7163747) [概述](#_Toc7163747) [2](#_Toc7163747)

[2.2](#_Toc7163748) [假设/约束/风险](#_Toc7163748) [2](#_Toc7163748)

[2.2.1](#_Toc7163749) [假设](#_Toc7163749) [2](#_Toc7163749)

[2.2.2](#_Toc7163750) [约束条件](#_Toc7163750) [2](#_Toc7163750)

[2.2.3](#_Toc7163751) [风险](#_Toc7163751) [3](#_Toc7163751)

[2.3](#_Toc7163752) [与联邦企业架构保持一致](#_Toc7163752) [3](#_Toc7163752)

[3.](#_Toc7163753) [设计注意事项](#_Toc7163753) [4](#_Toc7163753)

[3.1](#_Toc7163754) [目标和指南](#_Toc7163754) [4](#_Toc7163754)

[3.2](#_Toc7163755) [开发方法及突发事件](#_Toc7163755) [4](#_Toc7163755)

[3.3](#_Toc7163756) [架构策略](#_Toc7163756) [4](#_Toc7163756)

[3.4](#_Toc7163757) [性能工程](#_Toc7163757) [5](#_Toc7163757)

[4.](#_Toc7163758) [系统架构与架构设计](#_Toc7163758) [6](#_Toc7163758)

[4.1](#_Toc7163759) [逻辑视图](#_Toc7163759) [6](#_Toc7163759)

[4.2](#_Toc7163760) [硬件架构](#_Toc7163760) [6](#_Toc7163760)

[4.2.1](#_Toc7163761) [安全硬件架构](#_Toc7163761) [6](#_Toc7163761)

[4.2.2](#_Toc7163762) [性能硬件架构](#_Toc7163762) [7](#_Toc7163762)

[4.3](#_Toc7163763) [软件架构](#_Toc7163763) [7](#_Toc7163763)

[4.3.1](#_Toc7163764) [安全软件架构](#_Toc7163764) [8](#_Toc7163764)

[4.3.2](#_Toc7163765) [性能软件架构](#_Toc7163765) [8](#_Toc7163765)

[4.4](#_Toc7163766) [信息架构](#_Toc7163766) [8](#_Toc7163766)

[4.4.1](#_Toc7163767) [记录管理](#_Toc7163767) [8](#_Toc7163767)

[4.5](#_Toc7163768) [内部通信架构](#_Toc7163768) [8](#_Toc7163768)

[4.6](#_Toc7163769) [安全架构](#_Toc7163769) [9](#_Toc7163769)

[4.7](#_Toc7163770) [性能](#_Toc7163770) [9](#_Toc7163770)

[4.8](#_Toc7163771) [系统架构图](#_Toc7163771) [9](#_Toc7163771)

[5.](#_Toc7163772) [系统设计](#_Toc7163772) [10](#_Toc7163772)

[5.1](#_Toc7163773) [业务要求](#_Toc7163773) [10](#_Toc7163773)

[5.2](#_Toc7163774) [数据库设计](#_Toc7163774) [10](#_Toc7163774)

[5.2.1](#_Toc7163775) [数据对象和结果数据结构](#_Toc7163775) [10](#_Toc7163775)

[5.2.2](#_Toc7163776) [文件和数据库结构](#_Toc7163776) [10](#_Toc7163776)

[5.3](#_Toc7163777) [数据转换](#_Toc7163777) [11](#_Toc7163777)

[5.4](#_Toc7163778) [用户机读界面](#_Toc7163778) [11](#_Toc7163778)

[5.4.1](#_Toc7163779) [输入](#_Toc7163779) [11](#_Toc7163779)

[5.4.2](#_Toc7163780) [输出](#_Toc7163780) [12](#_Toc7163780)

[5.5](#_Toc7163781) [用户界面设计](#_Toc7163781) [12](#_Toc7163781)

[5.5.1](#_Toc7163782)  [508 条款合规性](#_Toc7163782) [12](#_Toc7163782)

[6.](#_Toc7163783) [操作场景](#_Toc7163783) [13](#_Toc7163783)

[七、](#_Toc7163784) [详细设计](#_Toc7163784) [14](#_Toc7163784)

[7.1](#_Toc7163785) [硬件详细设计](#_Toc7163785) [14](#_Toc7163785)

[7.2](#_Toc7163786) [软件详细设计](#_Toc7163786) [14](#_Toc7163786)

[7.3](#_Toc7163787) [安全详细设计](#_Toc7163787) [15](#_Toc7163787)

[7.4](#_Toc7163788) [性能详细设计](#_Toc7163788) [16](#_Toc7163788)

[7.5](#_Toc7163789) [内部通信详细设计](#_Toc7163789) [16](#_Toc7163789)

[8.](#_Toc7163790) [系统完整性控制](#_Toc7163790) [17](#_Toc7163790)

[九、](#_Toc7163791) [对外接口](#_Toc7163791) [18](#_Toc7163791)

[9.1](#_Toc7163792) [界面架构](#_Toc7163792) [18](#_Toc7163792)

[9.2](#_Toc7163793) [接口详细设计](#_Toc7163793) [18](#_Toc7163793)

[附录 A：变更记录](#_Toc7163794) [19](#_Toc7163794)

[附录 B：缩写词](#_Toc7163795) [20](#_Toc7163795)

[附录 C：词汇表](#_Toc7163796) [21](#_Toc7163796)

[附录 D：参考文档](#_Toc7163797) [22](#_Toc7163797)

[附录 E：批准](#_Toc7163798) [23](#_Toc7163798)

[附录 F：附加附录](#_Toc7163799) [24](#_Toc7163799)

[附录 G：作者须知/模板说明](#_Toc7163800) [25](#_Toc7163800)

图列表

**未找到图表条目。**

表格列表

[表 1 - 变更记录](#_Toc7163739) [19](#_Toc7163739)

[表 2 - 缩写词](#_Toc7163740) [20](#_Toc7163740)

[表 3 - 词汇表](#_Toc7163741) [21](#_Toc7163741)

[表 4 - 参考文件](#_Toc7163742) [22](#_Toc7163742)

[表 5 - 认证](#_Toc7163743) [23](#_Toc7163743)

## 介绍

说明：为系统设计文档 (SDD) 适用的现有和/或拟议的自动化系统或情况提供识别信息（例如，开发项目、现有系统或情况以及拟议的系统或情况的全名和首字母缩写词）情况，如适用），以及文件的预期演变。还描述与使用本文档相关的任何安全或隐私注意事项。

系统设计文档(SDD) 描述了需求文档中记录的功能性和非功能性需求、高级技术设计概念/备选方案文档中记录的初步面向用户的功能设计以及逻辑数据模型中记录的初步数据设计(LDM) 转换为构建系统的更多技术系统设计规范。 SDD 记录了高级系统设计和低级详细设计规范。

SDD 描述了设计目标和考虑因素，提供了系统架构的高级概述，并描述了与系统相关的数据设计，以及人机界面和操作场景。高级系统设计进一步分解为每个系统组件的低级详细设计规范，包括硬件、内部通信、软件、系统完整性控制和外部接口。高级系统设计作为初步设计审查(PDR) 的主要输入。低级详细设计作为详细设计审查(DDR) 的输入。

### SDD的目的

说明：提供 SDD 的用途。本文档应根据特定项目的需要进行裁剪。

SDD 记录并跟踪有效定义体系结构和系统设计所需的必要信息，以便为开发团队提供有关要开发的系统体系结构的指导。根据信息技术(IT) 项目的特定情况和用于开发系统的系统开发方法，设计文档在系统开发生命周期中以增量方式和迭代方式生成。它的目标读者是项目经理、项目团队和开发团队。本文档的某些部分，例如用户界面(UI)，可能会与客户/用户以及需要对 UI 进行输入/批准的其他利益相关者共享。

## 一般概述和设计指南/方法

本节描述了在设计和实施系统时用作指南的原则和策略。

### 总体概述

说明： 简要介绍系统上下文和基本设计方法或组织。简要概述系统和软件架构以及设计目标。包括先前在高级技术设计概念/备选方案和/或要求文档中提供的系统和子系统的高级上下文图，必要时更新以反映根据最新信息或理解。如果高级上下文图已更新，请确定所做的更改及其原因。

### 假设/约束/风险

#### 假设

说明：描述有关系统、软件及其使用的任何假设或依赖性。这些可能涉及以下问题：相关软件或硬件、操作系统、最终用户特征以及可能和/或可能发生的功能变化。

#### 约束条件

说明：描述对系统硬件、软件和/或通信的设计有重大影响的任何全局限制或约束，并描述相关影响。此类限制可能由以下任何一项施加（列表并不详尽）：

* 硬件或软件环境
* 最终用户环境
* 资源的可用性或波动性
* 符合标准
* 互操作性要求
* 接口/协议要求
* 许可要求
* 数据存储库和分发要求
* 安全要求（或其他此类规定）
* 内存或其他容量限制
* 性能要求
* 网络通讯
* 验证和确认要求（测试）
* 解决质量目标的其他方法
* 需求文档中描述的其他需求

#### 风险

说明：描述与系统设计和建议的缓解策略相关的任何风险。

### 与联邦企业架构保持一致

说明：描述与 FEA 的对齐。

## 设计注意事项

说明：描述在尝试设计完整的设计解决方案之前需要解决或解决的问题。

### 目标和准则

说明：描述主导或体现系统及其软件设计的任何目标、指南、原则或优先级。此类目标的示例可能是：强调速度与内存使用；或者像现有产品一样工作、看起来或“感觉”。指南包括编码指南和约定。对于每个这样的目标或指南，请描述其可取性的原因，除非它是显而易见的。描述没有全面架构影响的任何设计策略和/或策略（意味着它们不会显着影响系统的整体组织及其高层结构），但仍然会影响接口和/或实现的细节系统的各个方面（例如，选择使用哪个特定产品）。

### 开发方法和突发事件

说明：简要描述用于系统和软件设计的方法或方法（例如，结构化、面向对象、原型、J2EE、UML、XML 等）。如果采用或改编了一种或多种正式/公布的方法，则包括对这些方法的更详细描述的参考。如果认真考虑了几种方法，则应提及每种方法，并简要解释为什么使用或不使用全部或部分方法。描述在系统和软件的设计中可能出现的任何可能改变开发方向的突发事件。可能性包括缺乏与外部机构的接口协议或在准备 SDD 时架构不稳定。解决任何可能的解决方法或替代计划。

### 架构策略

说明：描述影响系统整体组织及其高层结构的任何设计决策和/或策略。这些策略应该提供对系统架构中使用的关键抽象和机制的洞察。描述每个决策和/或策略（可能指先前陈述的设计目标和原则）所采用的推理，以及如何平衡或权衡任何设计目标或优先级。

描述与 CMS 企业架构 (EA) 和标准的合规性。具体确定与 CMS EA 和标准的任何偏差，并提供支持偏差的理由。在描述设计决策时，讨论考虑过的任何其他重要备选方案，以及拒绝它们的原因（以及接受最终选择的备选方案的原因）。有时使用“模式格式”来描述策略可能是最有效的。

设计决策的示例可能涉及（但不限于）以下内容：

* 使用特定类型的产品（编程语言、数据库、库、商业现成 (COTS) 产品等）
* 重用现有软件组件来实现系统的各个部分/功能
* 扩展或增强软件的未来计划
* 用户界面范例（或系统输入和输出模型）
* 硬件和/或软件接口范例
* 错误检测和恢复
* 内存管理策略
* 外部数据库和/或数据存储管理和持久性
* 分布式数据或网络控制
* 通用控制方法
* 并发和同步
* 沟通机制
* 其他资源管理

### 性能工程

指示：

使用需求文档中定义的性能需求，提供详细的解释，描述性能需求是如何融入系统设计的。有关定义性能要求的指南，请参阅 CMS 性能测试计划和结果模板的第 2.0 节。

开始准备生产负载模型，为性能测试做准备。请参阅 CMS 性能测试计划和结果模板的第 2.1.1 节，以获取有关负载模型构建的指南。

性能要求是影响系统设计的一个因素。

性能要求是在系统上处理的特定工作负载的定义的可伸缩性或响应性期望。

## 系统架构与架构设计

说明：描述系统架构，应用程序如何与其他应用程序交互。不一定是应用程序本身如何工作，而是如何在应用程序之间正确传递适当的数据。概述系统的功能和职责是如何划分的，然后分配给子系统或组件。不要在本节中详细介绍各个组件本身。 SDD 的后续部分将提供详细的组件说明。这里的主要目的是大致了解系统是如何分解的以及为什么分解，以及各个部分如何协同工作以提供所需的功能。

在最顶层，描述软件必须承担的主要职责以及系统（或系统的一部分）必须扮演的各种角色。描述系统如何分解成它的组件/子系统（确定每个顶级组件/子系统和分配给它的角色/职责）。描述更高级别的组件如何相互协作以实现所需的结果。为选择这种特定的系统分解提供某种理由（也许讨论其他提议的分解以及它们被拒绝的原因）。

尽可能使用设计模式，无论是描述架构的各个部分（以模式格式），还是引用使用它们的架构元素。提供选择特定算法或编程习惯用法（或设计模式）以实现部分系统功能的基本原理。

本节概述了系统的系统结构和硬件架构设计。

### 逻辑视图

说明：插入任何相关的逻辑视图或提供对它们存储位置的引用。

### 硬件架构

说明：描述整个系统的硬件和组织，说明处理系统是分布式还是集中式。确定所有硬件组件的类型、数量和位置，包括演示、应用程序和数据服务器以及任何外围设备（例如，负载平衡器、SSL 加速器、交换机、防火墙），并简要说明每个项目和显示连接性的图表组件之间以及所需的防火墙、端口和使用的网络频带（例如，管理频带）。包括处理器容量、内存、在线存储和辅助存储的资源估计。

#### 安全硬件架构

说明：描述支持系统安全和隐私的硬件组件和配置。指定用于 (1) 身份验证的体系结构，以在允许访问系统之前验证用户身份，包括使用 IACS/EUA 或其他类型的身份审查和身份验证系统；(2) 授权用户在登录后执行功能活动系统，(3) 支持业务风险和信息性质的加密协议，以及 (4) 日志记录和审计设计，如果需要的话。设计应基于指定的系统安全级别，并针对威胁和漏洞提供充分的保护。

#### 性能硬件架构

说明：描述支持系统性能和可靠性的硬件组件和配置。识别单点故障，如果相关，描述高可用性设计（例如，集群）。

### 软件架构

说明：描述支持系统所需的所有软件，每个软件组件所针对的硬件组件，并指定所有软件系统的物理位置。列出诸如逻辑组件（例如，表示层中的 JSP、应用层中的 JNDI、数据层中的 EJB 和 JDBC）、数据库平台、计算机语言、编译器、实用程序、操作系统、通信软件、编程计算机辅助软件工程工具等事物、商用现成 (COTS) 软件、开源框架等，并简要说明每个项目的功能和任何识别信息，例如制造商、版本号、所需许可证的数量和类型等，作为适当的。识别所有计算机软件配置项 (CSCI)、计算机软件组件 (CSC) 和应用程序编程接口 (API)，包括每个项的名称、类型、用途和功能；这些元素的接口、消息传递和协议；软件架构设计的基本原理。包括作为函数、子例程或类的软件模块。使用功能层次图、结构化组织图（例如，结构图）或面向对象的图，将各种细分级别显示到最低级别。图表上的所有特征都应该有参考编号和名称。

包括扩展和增强对功能分解的理解的叙述。如有必要，描述一个组件是如何进一步划分为子组件的，以及子组件之间的关系和交互。根据需要进行尽可能多的级别/子部分的讨论，以便提供对整个系统或子系统的高级理解，将详细信息包含在 SDD 的后续部分中。包括符合适当标准（例如，Yourdon-Demarco 约定）的数据流图，并提供与逻辑过程和数据流相关的物理过程和数据流分解为原始过程级别（描述每个输入如何处理/转换为结果输出）。如果在该开发工作开始之前系统的某些部分已经存在，则只描述旧部分和新部分之间的关系和交互。修改或增强的预先存在的部分仅需描述到足以提供对正在进行的更改的性质的充分理解所必需的程度。

#### 安全软件架构

说明：描述支持系统安全和隐私的软件组件和配置。指定用于 (1) 身份验证的体系结构，以在允许访问系统之前验证用户身份，包括使用 IACS/EUA 或其他类型的身份审查和身份验证系统；(2) 授权用户在登录后执行功能活动系统，(3) 支持业务风险和信息性质的加密协议，以及 (4) 日志记录和审计设计，如果需要的话。设计应基于指定的系统安全级别，并针对威胁和漏洞提供充分的保护。

#### 性能软件架构

说明：描述支持系统性能和可靠性的软件组件和配置。识别单点故障，如果相关，描述高可用性设计（例如，集群）。

### 信息架构

说明：描述将存储在系统中的信息（例如受益人信息、索赔数据等） 识别是否有任何信息是个人身份信息 (PII)、个人身份信息 (IIF) 或个人健康信息 (PHI) ).

#### 记录管理

国家档案和记录管理局(NARA)发布的联邦法规在 36联邦法规(CFR) - 子章 B - 记录管理中有所概述。企业主必须联系战略运营和监管事务办公室(OSORA) 以启动记录管理流程。

##### 数据

识别提供给系统的所有数据（以及数据格式——纸质、手动输入、电子数据）以及谁/什么提供数据。

##### 手动/电子输入

提供有关手动/电子输入在输入主文件/数据库并经过验证后会发生什么情况的说明。

##### 主文件

提供系统/数据库中维护的数据的详细描述。

### 内部通讯架构

说明：提供系统通信网络的详细描述，指出正在实施的通信体系结构（例如，令牌环、以太网等）以及系统组件如何链接。描述任何局域网或广域网和总线。包括必要设备的描述（例如，集线器、路由器、电缆、发射器、防火墙、端口等）。提供描述系统和子系统组件之间的通信流的图表。包括在每个平台上安装和执行每个应用程序所需的通信网络容量（LAN 和 WAN）的资源估计。

### 安全架构

说明：插入任何相关的安全架构文档，包括完整性控制，或提供它们存储位置的参考。

### 表现

说明：插入任何性能文件或提供它们存储位置的参考。

### 系统架构图

说明：使用上述硬件、软件、通信和信息设计，从表示、应用程序和数据区域方面描述系统的整体集成结构。

图应显示“待生产系统”的架构，即架构设计必须映射到目标生产环境。

图表必须反映系统架构的准确性和清晰度。

图必须反映完整系统的上下文，即更详细的软件组件、内部/外部接口及其底层基础设施等，而不仅仅是与审查中的设计有关。

## 系统设计

### 业务需求

说明：插入任何相关的项目业务需求或提供它们存储位置的参考。

### 数据库设计

说明：描述与系统相关的所有数据库管理系统 (DBMS) 文件和非 DBMS 文件的设计。提供全面的数据字典，显示数据元素名称、类型、长度、来源、验证规则、维护（创建、读取、更新、删除 (CRUD) 功能）、数据存储、输出、别名和描述。数据设计信息可以包含在附录中或记录在单独的数据库设计文档 (DDD) 中，视情况而定，将在此处引用。 DDD 模板可从位于https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/的 CMS Integrated IT Investment & System Life Cycle Framework 网站获得下载/ [DatabaseDesignDocument](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/DatabaseDesignDocument.docx) .docx 。

#### 数据对象和结果数据结构

说明：对于每个功能数据对象，指定将用于存储和处理数据的数据结构。描述作为系统主要部分的任何数据结构，包括在组件之间传递的主要数据结构。列出所有函数和函数参数。对于函数，在描述中给出函数输入和输出名称。酌情参考分解图。

#### 文件和数据库结构

说明：使用逻辑数据模型 (LDM)，创建描述系统架构设置中的数据存储和操作的物理数据模型。描述文件结构及其位置。如果适用，解释数据在所选 DBMS 中的结构。酌情参考单独的 DDD。对于网络，详细说明数据的具体分布。请注意由于软件或硬件要求而对 LDM 进行的任何更改。

##### 数据库管理系统文件

说明：提供DBMS文件的详细设计。通常，此信息应记录在单独的 DDD 中，并应在本节中引用。 DDD 模板可从位于https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/的 CMS Integrated IT Investment & System Life Cycle Framework 网站获得下载/ [DatabaseDesignDocument](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/DatabaseDesignDocument.docx) .docx 。

##### 非数据库管理系统文件

说明：提供所有非 DBMS 文件的详细描述，并包括每个文件用途的叙述性描述，以标识文件是否用于输入、输出或两者，以及文件是否为临时文件。还提供了哪些模块读取和写入文件以及包含文件结构的指示（请参阅数据字典）。适当时，文件结构信息应包括以下内容：

* 记录结构、记录键或索引以及记录中引用的数据元素
* 记录长度（固定或最大可变长度）和分块因子
* 访问方法（例如，索引顺序、虚拟顺序、随机访问等）
* 估计文件大小或文件中的数据量，包括文件访问方法产生的开销
* 文件更新频率的定义（如果文件是基于在线交易的系统的一部分，请提供每单位时间的估计交易数量，以及这些交易的统计平均值、模式和分布。）
* 备份和恢复规范

### 数据转换

说明：插入描述任何必要数据转换的任何文档或提供它们存储位置的参考。

### 用户机读界面

说明：提供与系统关联的每个用户类别或角色的描述。用户类别由用户与建议的系统或情况交互的方式来区分。区分用户类别的因素包括共同职责、技能水平、工作活动以及与系统交互的模式。在此上下文中，用户是与所建议系统交互的任何人，包括操作用户、数据输入人员、系统操作员、操作支持人员、系统维护人员和培训人员。对于每个用户类别，提供预期用户总数、最大并发用户数和外部用户数的估计值。

#### 输入

说明：提供用户/操作员用于向系统提供信息的输入媒体的描述。显示到高级数据流的映射（例如，数据输入屏幕、光学字符阅读器、条形扫描仪等）。如果合适，可以参考数据设计部分提供的输入记录类型、文件结构和数据库结构。包括数据元素定义，或参考数据字典。提供所有输入数据屏幕或图形用户界面 (GUI)（例如，窗口）的布局。定义与每个屏幕或 GUI 关联的所有数据元素，或引用数据字典。为数据元素提供编辑标准，包括特定值、值范围、强制/可选、字母数字值和长度。还解决了数据输入控制问题，以防止绕过编辑。讨论与用户/操作员输入相关的杂项消息，包括（但不限于）以下内容：

* 表格副本（如果输入数据是通过键入或扫描的方式从打印表格中输入数据的）
* 任何访问限制或安全注意事项的描述
* 每个交易名称、代码和定义，如果系统是基于交易的处理系统
* 如果系统受隐私法保护，则将隐私法声明纳入屏幕流程
* 描述符合《康复法》第 508 条的无障碍条款

#### 产出

说明：描述与用户/操作员相关的系统输出设计。显示到高级数据流的映射。系统输出包括报表、数据展示界面和图形界面、查询结果等，可参考数据设计部分描述的输出文件。如果合适，应提供以下内容：

* 识别报告和数据显示屏幕的代码和名称
* 报告和屏幕内容的描述（提供每个布局的图形表示并定义与布局相关的所有数据元素或引用数据字典）
* 输出目的的描述，包括主要用户的识别
* 报告分发要求（如果有）（包括定期报告的频率）
* 任何访问限制或安全注意事项的描述

### 用户界面设计

说明：插入任何用户界面设计文档或提供它们存储位置的参考。

#### 第 508 条合规

说明：描述您的用户界面设计中的可访问性注意事项，并插入您的第 508 节合规性相关文档或提供它们存储位置的参考。

## 操作场景

说明：从用户的角度描述系统的一般功能，并通过操作场景提供系统的执行或操作流程，这些操作场景提供有关所提议的系统应如何操作以及如何与用户及其外部交互的逐步描述在给定的一组环境下的接口。这些场景通过描述它们如何交互将系统的所有部分、用户和其他实体联系在一起，也可以用来描述系统不应该做什么。

应针对所有操作模式、交易和为建议系统确定的所有用户类别描述操作场景。对于每个事务，提供大小（如果可变，则使用最大值）和频率（例如，每个会话的平均数）的估计值。确定是否存在任何交易高峰期，并包括对这些时期频率的估计。每个场景都应酌情包括事件、动作、刺激、信息和交互，以提供对拟议系统的操作方面的全面理解。

场景可以用几种不同的方式呈现：1) 对于建议系统的每个主要处理功能，或 2) 基于线程，其中每个场景遵循建议系统中的一种事务类型，或 3) 遵循信息流通过系统针对每个用户能力，遵循控制流，或关注系统中的对象和事件。指定的场景数量和详细程度将与项目的感知风险和关键程度成正比。

## 详细设计

说明：提供系统开发团队实际构建和集成硬件组件、编码和集成软件组件以及将硬件和软件部分互连成功能产品所需的信息。此外，解决将单独的 COTS 包组合到单个系统中的详细过程。

### 硬件详细设计

说明：提供有关每个单独硬件组件的足够详细信息，以正确构建和/或采购系统的所有硬件（或集成 COTS 项目）。如果组件很多或者组件文档很多，请将其放在附录中。如有必要，添加额外的图表和信息以充分描述每个组件及其功能。应遵循行业标准组件规范实践。对于 COTS 组件，确定特定的供应商和适当的项目名称和型号。在详细的组件设计中包括以下信息（如适用）：

* 每个组件的电源输入要求
* 信号阻抗和逻辑状态
* 连接器规格（串行/并行、11 针、公/母等）
* 内存和/或存储空间规格
* 处理器要求（速度和功能）
* 描绘硬件项目（例如，服务器、I/O 设备、监视器、打印机等）数量以及组件相互之间的相对位置的图形表示
* 电缆类型和长度
* 用户界面（按钮、拨动开关等）
* 硬盘/软驱/光驱规格
* 显示器分辨率

### 软件详细设计

为解决以下软件服务属性的每个系统软件服务提供详细描述。本节中出现的大部分信息应包含在每个组件、子系统、模块和子例程的源代码的标题/序言和注释部分中。如果是这样，本节可能主要包括对带注释的图表和源代码的引用或摘录。在任何设计审查中都应提供任何参考图表或源代码摘录。

* 服务标识符 - 软件服务的唯一标识符和/或名称
* 分类 - 服务的种类（例如，应用程序、数据服务等）
* 定义——服务的特定目的和语义
* 需求 - 服务满足的特定功能或非功能需求
* 内部数据结构 - 服务的内部数据结构
* 约束 - 服务的任何相关、假设、限制或约束（这应包括对时间、存储或服务状态的约束，并且可能包括与服务交互的规则（包括前置条件、后置条件、不变量、其他对输入或输出值和本地或全局值、数据格式和数据访问、同步、异常等的约束））
* 组合 - 对作为服务一部分的子服务的用途和含义的描述
* 用户/交互 - 服务与其他服务协作的描述（哪些其他服务使用此实体？此实体使用哪些其他服务（包括此服务可能对系统其他部分产生的任何副作用）？这包括交互方法，以及交互本身。面向对象的设计应该包括对任何已知或预期的子类、超类和元类的描述）
* 处理 - 准确描述服务如何执行履行其职责所必需的职责（这应包括对所使用的任何算法的描述；更改或状态；相关的时间或空间复杂性；并发性；创建、初始化和清理的方法; 和处理异常情况）
* 接口/导出 - 服务提供的一组服务（资源、数据类型、常量、子例程和异常）（应提供每个此类元素的精确定义或声明，以及描述值含义的注释或注释，参数等；对于所描述的每个服务元素，在其讨论中包括或提供对其重要软件服务属性（组件标识符、分类、语言、SLOC 估计、定义、职责、要求、内部数据结构、约束）的描述的参考、组成、使用/交互、资源、处理和接口/导出））
* 报告设计和集成 - 如果内置，请提供有关数据流量和容量的详细信息

### 安全详细设计

说明：为每个单独的安全硬件组件提供包含详细信息的图形表示。根据需要指定以下项目的设计。

* 验证
* 授权
* 记录和审计
* 加密
* 网络端口使用
* 入侵检测和预防（特别是托管在非 CMS 数据中心时

设计应基于指定的系统安全级别，并针对威胁和漏洞提供充分的保护。

### 性能详细设计

说明：为每个单独的性能和可靠性硬件组件提供包含以下项目的详细信息的图形表示：

* 容量和体积要求/估计
* 业绩预期
* 可用性要求
* 满足容量需求的性能设计
* 满足可用性要求的可靠性设计
* 备份、恢复和存档设计

识别单点故障，如果相关，描述高可用性设计（例如，集群）。

### 内部通讯详细设计

说明：如果系统包括多个组件，则可能需要内部通信来交换信息、提供命令或支持输入/输出功能。提供有关通信设计的足够详细信息，以正确构建和/或采购系统的通信组件。在详细的组件设计中酌情包括以下信息：

* 每个区域网络中要包含的服务器和客户端的数量
* 总线时序要求和总线控制规范
* 组件间交换数据的格式
* 组件之间连接的图形表示，显示数据流的方向（如果适用）以及组件之间的大致距离（信息应提供足够的详细信息以支持采购硬件以在给定位置完成安装）
* 局域网拓扑

## 系统完整性控制

说明：为以下最低级别的控制和任何适当或必要的附加控制提供设计规范：

* 内部安全将关键数据项的访问限制为用户/操作员所需的那些访问类型
* 满足运营和管理报告的控制、报告和保留期要求的审计程序
* 应用程序审计跟踪以动态审计对指定关键数据的检索访问
* 用于或请求用于验证数据字段的标准表
* 关键数据的添加、删除或更新的验证过程
* 能够通过用户标识、网络终端标识、日期、时间、访问或更改的数据来识别所有审计信息。

## 外部接口

说明：描述与不在所设计系统范围内的外部系统存在的任何接口，无论其他系统是否由 CMS 或其他实体管理。描述正在设计的系统与每个其他系统和/或子系统之间的电子接口，强调正在设计的系统的观点。如果有一个或两个以上的外部系统，或者如果接口不简单，则应准备一个或多个单独的接口控制文档 (ICD) 并在此处引用。如果适用，确定存在多少个 ICD 以及它们是什么。 ICD 模板可从位于[https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/的 CMS Integrated IT Investment & System Life Cycle Framework 网站获得下载/InterfaceControlDocument.docx](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/InterfaceControlDocument.docx) 。

### 界面架构

说明：描述正在开发的系统与其他系统之间的接口（例如，批量传输、查询等），指出接口系统的位置。包括正在实施的接口架构（例如，广域网、网关等）和接口机制（例如，MQ、Gentran 等）。如果需要远程连接，请确定访问方法。提供描述该系统与每个其他系统之间的通信路径的图表，该图表应映射到系统概述部分中提供的上下文图表。图形表示应描述系统之间的连接，显示数据流的方向。使用小节或单独的 ICD 来独立寻址每个接口。

### 接口详细设计

说明：对于与设计系统接口的每个外部系统，描述信息交换和管理接口的规则。提供有关接口的足够详细信息，以便通过接口正确格式化、传输和/或接收数据。通常，此信息应记录在单独的 ICD 中，并应在本节中引用。 ICD 模板可从位于[https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads的 CMS Integrated IT Investment & System Life Cycle Framework 网站获得/InterfaceControlDocument.docx](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/InterfaceControlDocument.docx) 。

附录 A：变更记录

说明：提供有关如何控制和跟踪 SDD 的开发和分发的信息。使用下表提供版本号、版本日期、版本作者/所有者以及创建修订版本的原因的简要说明。

表1 - 变更记录

| 版本号 | 日期 | 作者/所有者 | 变更说明 |
| --- | --- | --- | --- |
| <XX> | <月/日/年> | 内容管理系统 | <变更说明> |
| <XX> | <月/日/年> | 内容管理系统 | <变更说明> |
| <XX> | <月/日/年> | 内容管理系统 | <变更说明> |

附录 B：缩略语

说明：提供文档中使用的首字母缩略词和相关直译的列表。使用如下所示的表格格式按字母顺序列出首字母缩略词。

表2 - 缩写词

| 首字母缩略词 | 字面翻译 |
| --- | --- |
| <首字母缩略词> | <直译> |
| <首字母缩略词> | <直译> |
| <首字母缩略词> | <直译> |

附录 C：词汇表

说明：为文档读者可能不熟悉的文档中使用的术语提供清晰简洁的定义。术语应按字母顺序列出。

表3 - 词汇表

| 学期 | 首字母缩略词 | 定义 |
| --- | --- | --- |
| <术语> | <首字母缩略词> | <定义> |
| <术语> | <首字母缩略词> | <定义> |
| <术语> | <首字母缩略词> | <定义> |

附录 D：参考文件

说明：总结本文档与其他相关文档的关系。为用于达成和/或在本文件中引用的所有文件提供识别信息（例如，相关和/或配套文件、先决条件文件、相关技术文件等）。

表4 - 参考文件

| 文档名称 | 文档位置和/或 URL | 发行日期 |
| --- | --- | --- |
| <文档名称> | <文档位置和/或 URL> | <月/日/年> |
| <文档名称> | <文档位置和/或 URL> | <月/日/年> |
| <文档名称> | <文档位置和/或 URL> | <月/日/年> |

附录 E：批准

下面的签名者承认他们已经审查了 SDD 并同意本文件中提供的信息。对本 SDD 的更改将与下列签署人或其指定代表协调并由其批准。

说明：列出需要签名的个人。此类人员的示例包括企业主、项目经理（如果确定）和任何适当的利益相关者。根据需要添加额外的签名行。

表5 - 认证

| 文件批准人 | 批准日期 |
| --- | --- |
| 姓名：<姓名>，<职务> - <公司> | 日期 |
| 姓名：<姓名>，<职务> - <公司> | 日期 |
| 姓名：<姓名>，<职务> - <公司> | 日期 |
| 姓名：<姓名>，<职务> - <公司> | 日期 |

附录 F：附加附录

说明：利用额外的附录来简化文档的使用和维护。建议的附录包括（但不限于）：

* 软件架构图 - 提供功能层次图、结构化组织图或面向对象的图表，这些图显示了软件架构的各种细分级别，一直到最低级别。
* 数据字典——提供所有流程、数据流、数据元素和数据存储的定义。
* 需求可追溯性矩阵 - 证明系统和软件架构设计对需求文档中记录的功能性和非功能性需求的向后追踪性。
* CMS 第 508 条产品评估 - 证明符合或不符合 1973 年康复法案第 508 条规定的可访问性标准，该法案于 2001 年 6 月 20 日修订生效 本附录的模板可在 https://www.cms.gov[获得/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/Sect508ProdAssessment.docx](https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/XLC/Downloads/Sect508ProdAssessment.docx) 。

附录 G：作者须知/模板说明

本文档是为给定投资或项目创建 SDD 的模板。最终文件应以可电子搜索的格式提交。 SDD 应独立存在，并为读者/审阅者（包括可能不熟悉 CMS 项目和投资的 CMS 以外的审阅者）解释所有元素并拼写首字母缩略词。

此模板包括说明、样板文本和字段。开发人员应注意：

* 每个部分都提供说明或描述该部分中包含的内容的意图、假设和上下文。在整个模板中，说明文本以蓝色斜体字显示。
* 每个部分的说明文字应替换为特定投资的特定信息。
* 一些文本和表格作为措辞和格式的样板示例提供，可以酌情使用或修改。

使用此模板时，请按照下列步骤操作：

1. 表格标题和说明将左对齐放置在表格上方。
2. 根据您的特定投资，酌情修改任何样板文本。
3. 不要删除任何标题。如果标题不适用于投资，请在标题下填写“不适用”。
4. 所有文件必须符合第 508 节的要求。
5. 图标题和说明将左对齐放置在图下方。所有图形都必须有一个相关联的标签，为第 508 节合规性提供适当的替代文本。
6. 在完成文档的初稿之前，删除此“作者注释/模板说明”页面和所有作者说明。