Assignment 3

丁霄汉 131250207

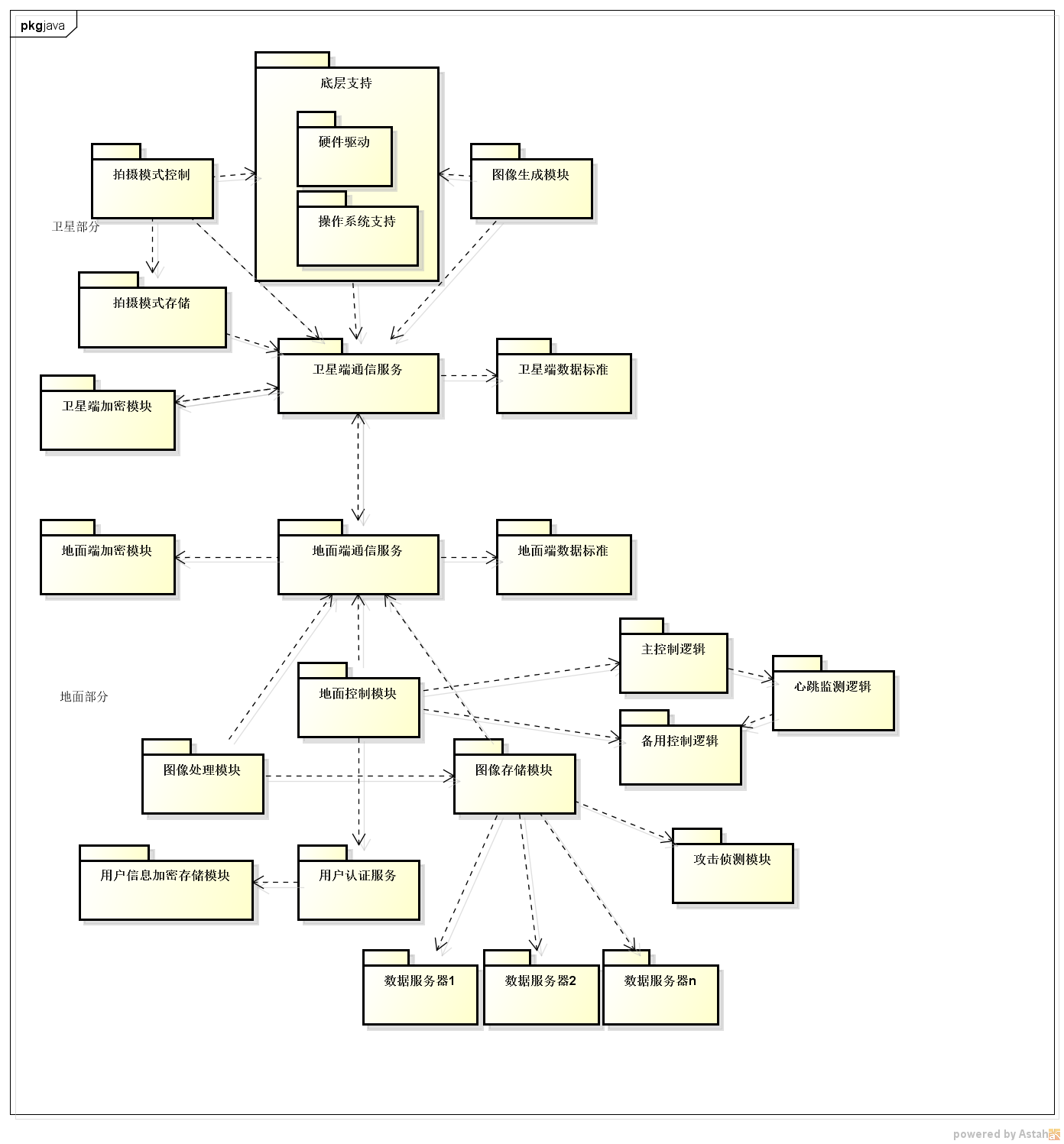
陈云龙 131250181

曾婧 131250159

梁思宇 131250129

## 架构概述

此处呈现的模块视图，比第二次作业中的多了一些部分。



在第二次作业中，由于篇幅所限，删除了一些架构决策和考量因素才勉强没有超出12页的限制。在此呈现的模块视图，除了第二次作业中的全部内容外，还包括：

1. 我们为提高系统可用性而做出的设计决策：地面控制逻辑设置备份模块，通过心跳（heartbeat）监测主控逻辑是否正常运行，如果出现故障，则切换至备用控制逻辑。探测器端模块不作备份，主要是考虑航天用元件的低性能高可靠性的特性。后文有详述。

2. 为提高系统性能而做出的设计决策：图像处理模块需要经常读写存储在服务器上的图像数据，考虑到航天拍摄的照片尺幅巨大，图像处理需要进行大量运算，所以应该采取必要措施保证图像数据足够的存储容量和读写速率。我们决定采用分布式数据服务器，由图像存储模块对外提供统一接口。

## 非功能需求场景和效用树

|  |  |  |
| --- | --- | --- |
| 质量属性 | 属性精化 | 场景 |
| 可修改性 |  | A1:开发者更新加密标准，在1人月内完成（H，H）  A2:开发者更新某些系统模块的功能，修改预算未超过总预算的10%，其他无关的系统功能未受影响（H，H） |
| 可移植性 |  | A3:开发者将系统从现有操作系统和硬件平台上移植到其他操作系统和硬件平台，移植工作在一周内完成，修改代码量不超过10%，移植后系统所有功能都能正常运行（M，L） |
| 安全性 | 用户身份验证  攻击侦测  通信加密  用户数据加密 | A4:某用户未通过身份验证试图向探测器发送控制指令和访问图像数据，被系统拒绝访问（H，H）  A5:系统受到恶意攻击，系统侦测到攻击后，图像存储模块拒绝一切外界访问，直到确认安全（H，M）  A6:地面和探测器之间通信信号被截获，截获者无法破译加密后的通信信息（H，H）  A7:用户数据被窃取，窃取者无法破译加密后的用户密码等敏感信息（H，L） |
| 可用性 | 故障监测  功能备份  故障重启 | A8:系统某部分发生故障，丧失正常功能，系统在5min内检测到故障源（M，L）  A9:地面控制模块发生故障，系统在1s内发现故障并切换至备用控制逻辑，恢复正常功能。（H，H）  A10其他部分发生故障，若不能恢复，在5min内通过重启恢复正常功能 |
| 互操作性 |  | A11:探测器向地面传回图像数据，根据需要传输至其他工作站或分布式服务器进行处理和存储，不需要经过数据格式转换（M，M） |
| 性能 | 图像生成时间  通信速率  地面数据服务器性能 | A12:系统根据拍摄指令执行完拍摄动作，采集到数据后，在1s内生成原始图像  A13:某用户完成拍摄任务并接收回传的图像，接收图像速率不低于2Mbps  A14：用户处理图像时通过数据服务器读写图像，服务器能够提供200TB的存储容量，且为图像处理模块提供不低于64Mbps的读写速率 |
| 易用性 |  | A15:在本行业具有两年以上的经验的新员工，通过为期一周的培训熟练后掌握此系统的核心功能（M，L） |
| 可维护性 |  | A16:系统所使用的数据库的厂商发布了一个新版本，在一周内部署到所有数据服务器上（H，M） |

## 敏感点和权衡点

#### 敏感点

|  |  |  |
| --- | --- | --- |
| S1 | 模块分离 | 将数据标准模块独立出来，以应对数据标准的潜在变更，影响了可修改性(正面)，因此是**可修改性的敏感点**。硬件驱动模块、操作系统支持模块分离，提高可移植性，是**可移植性的敏感点**同时使安全保障的元素模块容易变更，提高了安全性，是**安全性的敏感点**。 |
| S2 | 增强内聚 | 将底层支持模块分成硬件驱动和操作系统支持模块，以应对硬件和操作系统的升级，是**可修改性的敏感点**，同时有利于移植到其他硬件和操作系统平台上，是**可移植性的敏感点**。 |
| S3 | 延迟绑定 | 分离出数据标准模块，专门维护数据标准，是**可修改性的敏感点**。同时，有利于数据标准的更新和统一，是**互操作性的敏感点**。 |
| S4 | 未使用中间件平台 | 使用中间件能够提高可移植性，是**可移植性的敏感点**。但是影响了系统性能（负面），因此是**性能的敏感点**。 |
| S5 | 用户认证 | 以加密方式存储用户资料，用户向探测器发布控制指令必须经过身份认证。是**安全性的敏感点**。 |
| S6 | 通信加密 | 对地面和探测器之间的通信进行加密，是**安全性的敏感点**。 |
| S7 | 用户数据加密 | 用户密码等敏感信息加密存储，是**安全性的敏感点**。 |
| S8 | 攻击发生时收回数据访问权限 | 增加攻击侦测模块，当侦测到攻击发生时，图像存储模块将会拒绝一切访问直至确认安全，是**安全性的敏感点（正面）**。但是即便是不足为患的攻击也会影响正常用户的访问操作，是**可用性的敏感点（负面）**。 |
| S9 | 未采用检验哈希值验证数据完整性 | 验证数据完整性有利于系统部件之间、不同系统之间的数据交互，能提高互操作性，是**互操作性的敏感点（正面）**，但是会影响性能，是**性能的敏感点（负面）** |
| S10 | 地面控制逻辑采用心跳监测和备份模块 | 有利于迅速发现控制模块故障并通过启用备用模块恢复正常功能，是**可用性的敏感点（正面）**，但是会增加额外负担，是**性能的敏感点（负面）** |
| S11 | 探测器端未采用心跳监测和备份模块 | 避免引入额外负担，但是探测器端故障只能通过重启解决，是**可用性的敏感点（负面），性能的敏感点（正面）** |
| S12 | 分布式数据服务器 | 分布式数据服务器的性价比显著优于单台商业中型机和大型机，能够提供较为优质的数据服务，是**性能的敏感点（正面）**。但是由于数据分散存储，技术门槛较高，对维护工作，特别是数据完整性、一致性的维护提出了较高的要求，是**可维护性的敏感点（负面）** |

#### 权衡点

|  |  |  |
| --- | --- | --- |
| T1 | 未使用中间件平台 | 降低了可移植性，避免性能损失，是**可移植性和性能的权衡点** |
| T2 | 攻击发生时收回数据访问权限 | 避免敏感数据外泄，提高了安全性，降低了可用性，是**安全性和可用性的权衡点** |
| T3 | 未采用哈希值验证数据完整性 | 放弃对数据完整性的进一步确认，降低了互操作性，提高了性能，是**互操作性和性能的权衡点** |
| T4 | 地面控制逻辑采用心跳监测和备份模块 | 有利于故障的迅速发现和快速恢复，提高了可用性，降低了性能，是**可用性和性能的权衡点** |
| T5 | 探测器端未采用心跳监测和备份模块 | 避免引入性能负担，但是故障只能通过重启解决，提高了性能，降低了可用性，是**可用性和性能的权衡点** |
| T6 | 分布式数据服务器 | 性价比高，以相同成本提供更佳的容量和读写速率，但是维护工作技术门槛高，是**性能和可维护性的权衡点** |

## 风险和非风险

#### 风险

|  |  |  |
| --- | --- | --- |
| R1 | 未使用中间件平台 | 可能导致可移植性不够好，当有移植到新硬件平台和操作系统的需要时，移植成本超出预算或不能按时交付 |
| R2 | 攻击发生时收回数据访问权限 | 可能导致可用性不够好，如果系统经常遇到并不严重的攻击，即便不会影响数据安全，也会影响正常用户的访问操作 |
| R3 | 未采用检验哈希值验证数据完整性 | 可能导致互操作性不够好，如果通信协议不能正确工作，或通信环境过于恶劣，或受到严重干扰，会导致数据丢失 |
| R4 | 地面控制逻辑采用心跳监测和备份模块 | 可能造成地面部分性能负担，影响系统整体性能。 |
| R5 | 探测器端未采用心跳监测和备份模块 | 可能影响系统可用性，当探测器端出现故障时需要重启解决，浪费宝贵的探测器端计算资源 |
| R6 | 分布式数据服务器 | 分布式数据服务器技术门槛高，提高人力成本。如果维护不当，数据的完整性和一致性可能出现问题。 |

#### 非风险

|  |  |  |
| --- | --- | --- |
| N1 | 模块分离 | 成熟的设计原则，显著利于增强可修改性、可移植性 |
| N2 | 增强内聚 | 同上 |
| N3 | 延迟绑定 | 有利于增强可修改性。由于本项目中延迟绑定的是数据标准模块，有利于标准变更，也提高了互操作性 |
| N4 | 用户认证 | 多用户系统和涉密系统的标准配置 |
| N5 | 用户数据加密 | 同上 |
| N6 | 通信加密 | 涉密系统和需要长距离通信系统为保证安全性采取的必要设计 |

## ATAM分析

#### 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A3** | 开发者将系统从现有操作系统和硬件平台上移植到其他操作系统和硬件平台 | | | |
| **质量属性** | 可移植性 | | | |
| **环境** | 开发环境 | | | |
| **刺激** | 操作系统变更和硬件升级 | | | |
| **响应** | 移植工作在一周内完成，修改代码量不超过10%，移植后系统所有功能都能正常运行 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 模块分离 | S1 |  |  | N1 |
| 增强内聚 | S2 |  |  | N2 |
| 未使用中间件平台 | S4 | T1 | R1 |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **理由说明** | 模块分离和增强内聚是成熟的设计原则，无需多言。  对于本项目而言，航天器上的计算资源宝贵，性能不容浪费，所以不使用中间件平台。由于航天器所使用的电子元件以稳定性为第一位，更新换代慢，可移植性的适当牺牲、移植工作超出预算和工期的合理风险是可以接受的。 | | | |
| **相关架构图** |  | | | |

#### 2.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A5** | 系统受到恶意攻击，系统侦测到攻击后，图像存储模块拒绝一切外界访问，直到确认安全 | | | |
| **质量属性** | 安全性 | | | |
| **环境** | 运行时 | | | |
| **刺激** | 外部攻击 | | | |
| **响应** | 系统侦测到攻击后，图像存储模块拒绝一切外界访问，直到确认安全 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 用户认证 | S5 |  |  | N4 |
| 攻击发生时收回数据访问权限 | S8 | T2 | R2 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **理由说明** | 本项目涉及航天拍摄，可能包括机密信息，所以安全性尤为重要。  对于多用户系统而言，设置用户认证机制是成熟的应对策略。  攻击者若不能通过用户认证，可能使用各种方式对系统发动攻击。为安全起见，当侦测到攻击发生时拒绝外界访问图像数据，这样可以确保图像数据不外泄。虽然也可能影响正常用户的访问操作，但是这种风险是可以接受的，而泄密的风险是不可接受的。 | | | |
| **相关架构图** |  | | | |

#### 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A6** | 地面和探测器之间通信信号被截获，截获者无法破译加密后的通信信息 | | | |
| **质量属性** | 安全性 | | | |
| **环境** | 运行时 | | | |
| **刺激** | 不法分子截获通信信号 | | | |
| **响应** | 通信信息经过加密，截获者无法破译 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 模块分离 | S1 |  |  | N1 |
| 延迟绑定 | S3 |  |  | N3 |
| 通信加密 | S6 |  |  | N6 |
|  |  |  |  |  |
|  |  |  |  |  |
| **理由说明** | 对于本项目而言，需要通过电磁波实现天地之间通讯，而电磁波的物理特性决定了通信内容容易被截获，而且原发送方和接收方对截获的发生一无所知。所以，对通信内容的加密是必不可少的。  将地面端和探测器端加密模块独立出来，而且加密算法和密钥等信息不是写死在程序里的，易于变更，减少变更代价。  加密算法和密钥容易变更，减小了被破译的可能性，有利于提高安全性。 | | | |
| **相关架构图** |  | | | |

#### 4.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A9** | 地面控制模块发生故障，系统在1s内发现故障并切换至备用控制逻辑，恢复正常功能。 | | | |
| **质量属性** | 可用性 | | | |
| **环境** | 运行时 | | | |
| **刺激** | 地面控制模块故障 | | | |
| **响应** | 系统在1s内发现故障并切换至备用控制逻辑，恢复正常功能 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 模块分离 | S1 |  |  | R1 |
| 心跳 | S10 | T4 | R4 |  |
| 功能备份 | S10 | T4 | R4 |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **理由说明** | 由于航天器上的计算资源宝贵，地面控制部分故障导致探测器长时间无法正常工作是不能接受的。而且航天器上使用的计算机最重视稳定性，普遍特征是低性能高可靠性，地面部分的性能远强于探测器部分，系统的性能瓶颈一定是在探测器端的，在地面控制部分引入功能备份和心跳机制不会对系统的整体性能造成显著影响，因此这种风险是可以接受的。另一方面，如果在探测器端也引入功能备份的话，以本来就低的性能为代价提高本来就很高的可靠性，是得不偿失的。 | | | |
| **相关架构图** |  | | | |

#### 5.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A11** | 探测器向地面传回图像数据，根据需要传输至其他工作站或分布式服务器进行处理和存储，不需要经过数据格式转换 | | | |
| **质量属性** | 互操作性 | | | |
| **环境** | 运行时 | | | |
| **刺激** | 系统向其他系统传输数据 | | | |
| **响应** | 数据根据需要传输至其他工作站或分布式服务器进行处理和存储，不需要经过数据格式转换 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 模块分离 | S1 |  |  | N1 |
| 延迟绑定 | S3 |  |  | N3 |
| 未采用检验哈希值验证数据完整性 | S3 | T3 | R3 |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **理由说明** | 将数据通信标准单独分离出来，而不是写死在程序里，提高了可修改性。  主流通信协议包括对数据完整性的确认机制。如果通信协议不能正确工作，或通信环境过于恶劣，或受到严重干扰，会导致数据丢失，这种风险是确实存在的。但是，如果通过哈希值验证完整性的话，探测器端回传图像数据就要首先计算哈希值，而由于航天照片尺幅巨大，图像数据往往是很大的，会给航天器端造成较大的性能负担，得不偿失。 | | | |
| **相关架构图** |  | | | |

#### 6.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **场景：A14** | 用户处理图像时通过数据服务器读写图像，服务器提供200TB的存储容量，且为图像处理模块提供不低于64Mbps的读写速率 | | | |
| **质量属性** | 性能 | | | |
| **环境** | 运行时 | | | |
| **刺激** | 用户处理图像 | | | |
| **响应** | 服务器提供200TB的存储容量，且为图像处理模块提供不低于64Mbps的读写速率 | | | |
| **架构决策** | **敏感点** | **权衡点** | **风险** | **非风险** |
| 分布式数据服务器 | S12 | T6 | R6 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **理由说明** | 相比于单台商用中型机和大型机，分布式服务器性价比更高，相同成本下能够提供大的存储容量和更高的读写速率，但是维护工作技术门槛较高，需要有专门的分布式系统从业经验的技术人员维护。由于航天照片数据量巨大，图像处理需要大量运算和较高的读写速率，本系统对高性能数据服务的需求是现实存在的，节约预算、追求高性价比的需要也是现实存在的。随着分布式技术的发展成熟，相关人才越来越多，经验越来越丰富，人力成本、数据一致性和完整性的风险是可以接受的。 | | | |
| **相关架构图** |  | | | |

## 个人小结

#### 丁霄汉 131250207

#### 陈云龙 131250181

#### 曾婧 131250159

#### 梁思宇 131250129