固件更新接口声明

编制部门：研发--软件部

编 制 人：贾亮亮

审　　核：

会　　签：

批　　准：

文件修订履行			
版本	修订内容简述	生效日期	修订部门/修订者
1	新制订	2016-12-05	软件部
2	添加服务器端，差分包生成流程	2016-12-06	软件部
3	添加返回信息说明	2016-12-09	贾亮亮
4	调整升级包下载接口返回字符串	2016-12-21	贾亮亮

说明

1. 本文对固件更新进行设计
2. 本文对固件更新的接口进行声明
3. 本文对接口更新下载进行声明

1 引言

1.1 编写目的

在优必选统一后台开发系统项目的前一阶段，也就是需求分析阶段中，已经将系统用户对本系统的需求做了详细的阐述，这些用户需求已经在上一阶段中对公司开发的需求中，用户的实地调研中获得，并在需求规格说明书中得到详尽得叙述及阐明。

本阶段已在系统的需求分析的基础上，对统一后台管理系统做概要设计。主要解决了实现该系统需求的程序模块设计问题。包括如何把该系统划分成若干个模块、决定各个模块之间的接口、模块之间传递的信息，以及数据结构、模块结构的设计等。本文档主要对素材管理模块做概要设计，在以下的概要设计报告中将对在本阶段中对系统所做的所有概要设计进行详细的说明。

在下一阶段的详细设计中，程序设计员可参考此概要设计报告，在概要设计对统一后台管理系统所做的模块结构设计的基础上，对系统进行详细设计。在以后的软件测试以及软件维护阶段也可参考此说明书，以便于了解在概要设计过程中所完成的各模块设计结构，或在修改时找出在本阶段设计的不足或错误。

1.2 项目背景

本项目是有优必选公司开发的统一后台管理系统，有研发部-公共数据服务平台，负责实际的开发工作。

统一后台管理系统--固件更新模块开发，负责优必选公司统一固件，APP 和其它软件升级使用，现阶段固件更新分为三个重要模块：

1、固件上传管理模块

2、固件更新下载模块

3、**文件服务器模块**

1.3 定义

专业术语

Mysql：系统服务器所使用的数据库管理系统（DBMS）。

SQL: 一种用于访问查询数据库的语言

事务流：数据进入模块后可能有多种路径进行处理。

主键：数据库表中的关键域。值互不相同。

外部主键：数据库表中与其他表主键关联的域。

ROLLBACK: 数据库的错误恢复机制。

Zookeeper：一个分布式的，开放源码的分布式应用程序协调服务。

Dubbo：是一个分布式服务框架,提供高性能和透明化的 RPC 远程服务调用方案

Redis：一个先进的 key-value 存储可用于构建高性能,扩展 Web 应用程序的解决方案。

缩写

系统：若未特别指出，统指统一后台管理系统。

模块：若未特别指出，统指固件更新模块。

SQL: Structured Query Language（结构化查询语言）。

2 任务概述

2.1 目标

统一固件更新系统，前台提供升级文件的上传，提供升级文件下载操作，并统计用户下载信息，提供用户下载升级软件更新数据报告。

2.2 运行环境

固件更新模块将由两部分程序组成：

1、用户上传界面和用户下载接口提供。

2、后端的查询和持久化服务，使用 Dubbo 协议框架实现，实现分布式部署和管理。

服务器部署在 Linux 服务器上，有 Centos6.5 +版本环境下运行，具体部署文件请参考详细设计文档，服务器配置部署文档。

2.3 需求概述

需要提供升级软件上传服务，用户可以创建项目，并且上传升级文件，后台需要根据需求生成差分包，提供用户下载升级使用。

用户下载请求时，需要先请求服务器地址，获得 Token 信息，然后通过 Token 信息，获取下载文件地址，提供用户进行升级使用。

用户下载成功后，需要将安装信息返回给服务端，提供服务数据统计操作。

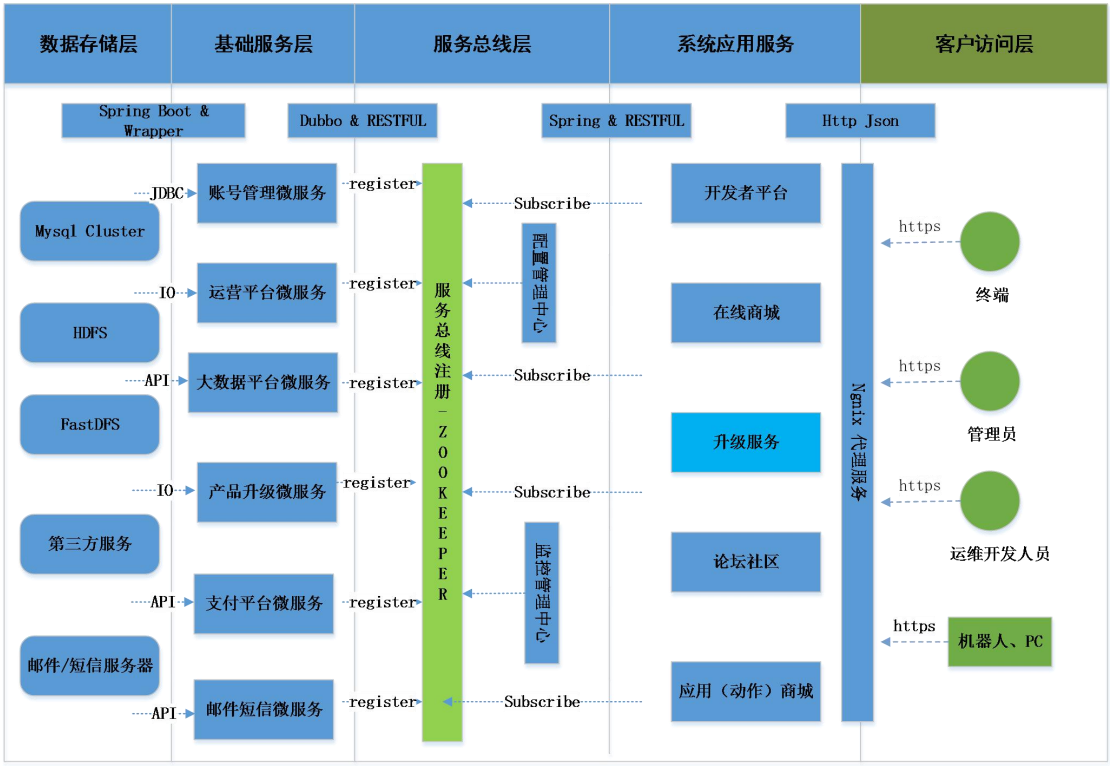
要求系统能有效、快速、安全、可靠和无误的完成上述操作。并要求上传软件的界面简单明了，易于操作，服务器程序利于维护。

2.4 条件与限制

无

3 总体设计

总体框架图如下：



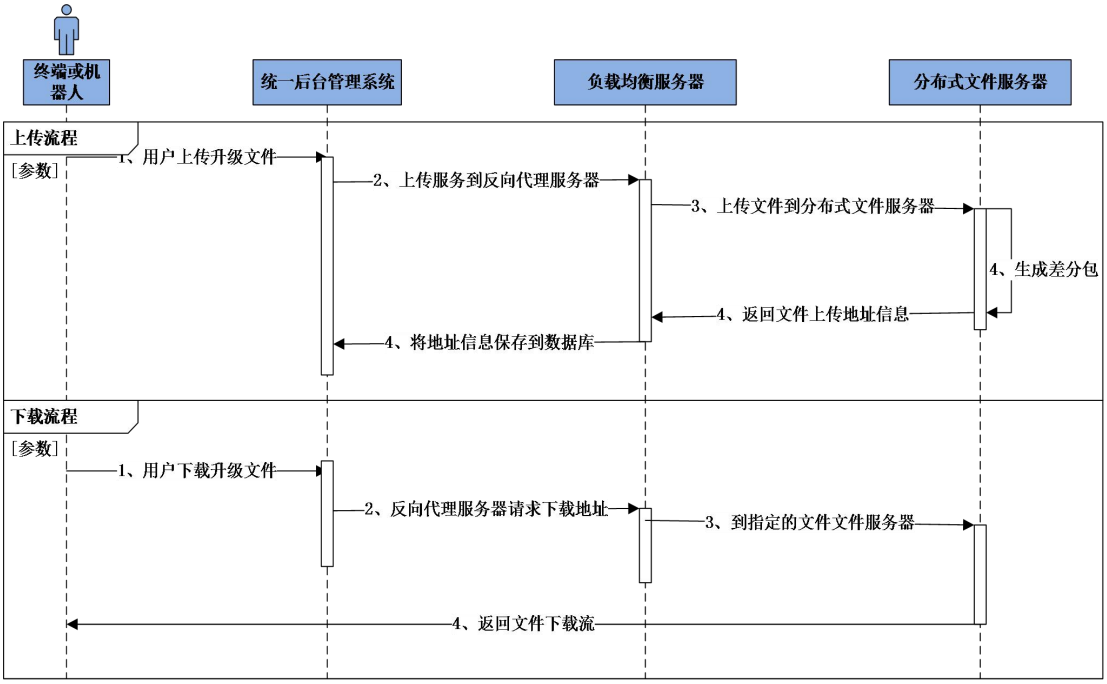
3.1 处理流程

下面将使用（结构化设计）升级软件下载操作。系统可分为两大部分：一、升级软件上传界面操作，二、升级软件下载操作，以下将分别对系统的这两大部分进行流程分析：

服务端软件上传升级软件流程：

管理员用户通过统一后台管理系统，上传升级软件到服务器上，提供用户下载，

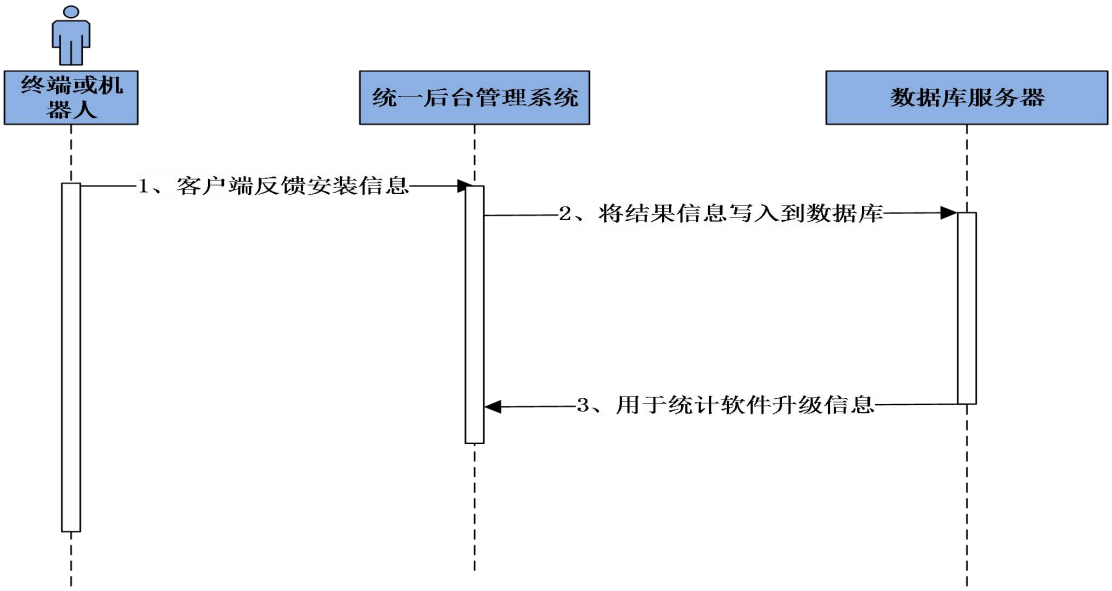
其内部处理流程如下：



下面对升级流程进行功能说明：

1. *用户创建机器人，不同类型的机器人类型，可以单独的创建一个机器人。*
2. *用户在不同机器人下面创建分类。*
3. *用户上传用户升级包到指定机器人下面的分类。*

客户端下载升级软件反馈流程：

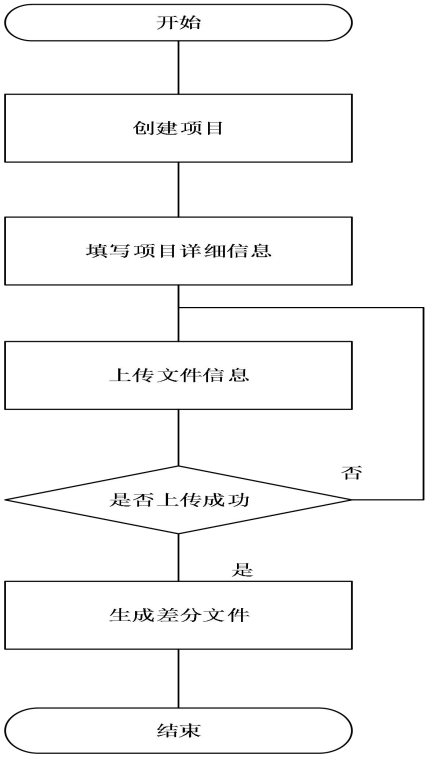


下面对各模块进行功能说明：

1. *终端或客户端通过 Https 协议，进行文件流的下载操作。*
2. *客户端统计下载用户信息，将用户下载信息保存在数据库中。*

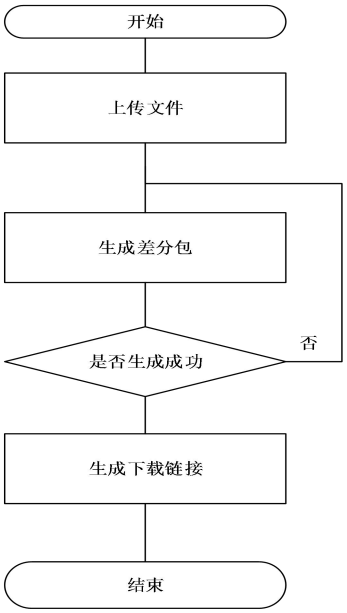
3.2 服务器后台服务模块

此模块提供升级软件的上传操作，用户可以创建不同的项目，进行文件的上传操作，上完毕后，客户端可以通过接口调用，返回指定的升级文件地址，及相应信息，详细的流程图如下：

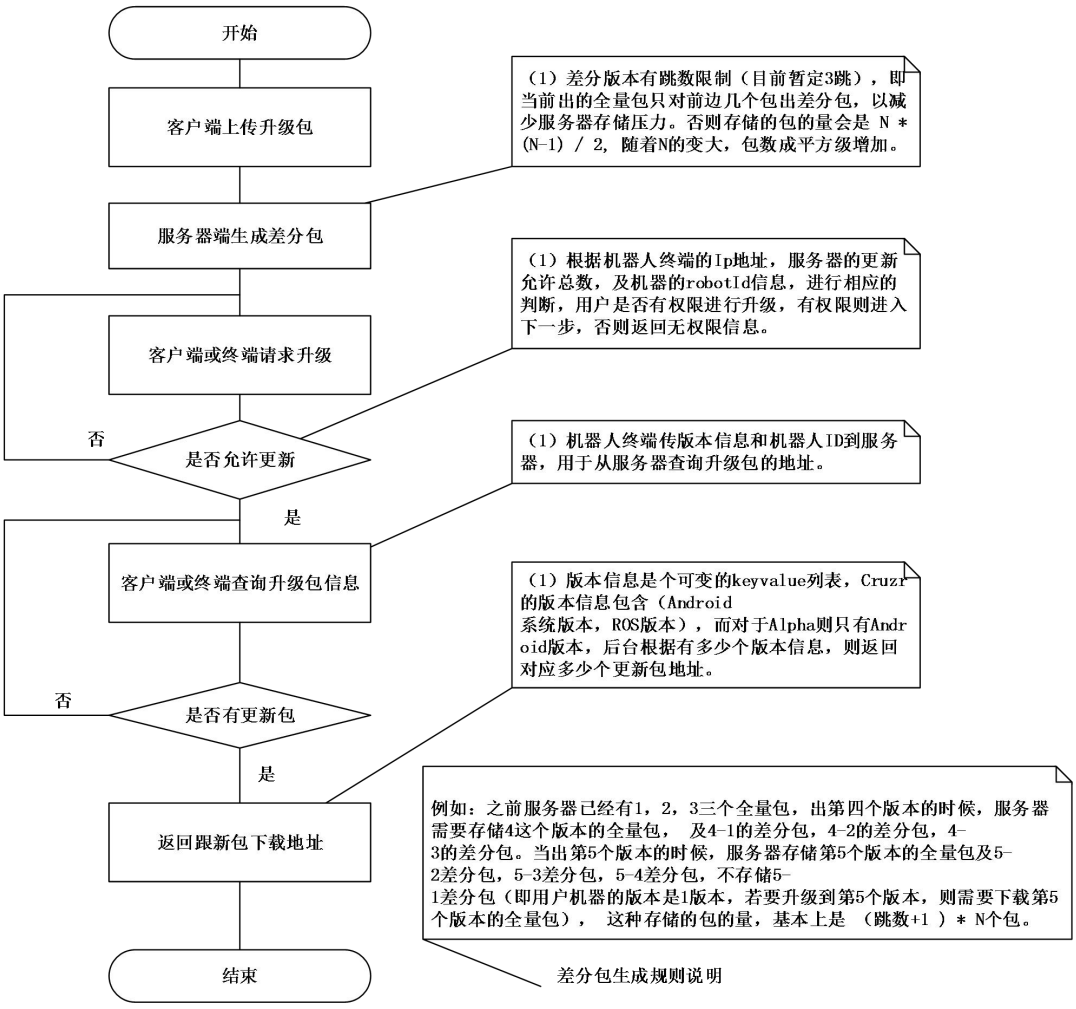


3.3 分布式文件服务器模块

提供文件的上传和软件升级包的差分服务接口，流程图如下所示：



3.4 客户端或终端升级查询服务



接口升级包查询的接口声明如下：

参数名称	是否必须	参数类型	备注
access_token	必须	String	如何获得 Token，请参考接口声明，如何获取 Token
robot_type	必须	String	机器人型号
model	必须	String	机器人终端版本信息，版本如：3-v1.0.1 多个版本例子如： 2-v1.1.1;5-v1.2.1;6-v1.1.1
ip	必须	String	Ip 地址
robot_id	必须	String	机器码（机器唯一标识）

说明信息如下：

（1） 启动下载前，机器人终端传版本信息，Ip 地址信息和机器人 ID 到服务器，用于从服务器查询升级包的地址，

（2）服务端根据终端的 Ip 地址做地域判断是否有更新权限，判断是否到达更新总数，同时判断 RobotId 是否可以进行更新；**服务器端根据用户本身的版本号信息，在服务端查询**

此版本的最新版本信息，如果服务器最新版本跟终端版本相差 3 个版本以内（包括 3 个版本），则返回终端与服务端的版本的所有差分包地址及 MD5 值，如果服务器最新版本跟终端版本相差 3 个版本以上，则直接发送最新升级包的地址和 MD5 值。

（3） 版本信息是个可变的 keyvalue 列表，Cruzr 的版本信息包含（Android 系统版本，ROS 版本），而对于 Alpha 则只有 Android 版本，后台根据有多少个版本信息，则返回对应多少个更新包地址。

（4）差分版本有跳数限制（目前暂定 3 跳），即当前出的全量包只对前边几个包出差分包，以减少服务器存储压力。否则存储的包的量会是 N * (N-1) / 2, 随着 N 的变大，包数成平方级增加。

举例参考：

例如：之前服务器已经有 1，2，3 三个全量包，出第四个版本的时候，服务器需要存储 4 这个版本的全量包， 及 4-1 的差分包，4-2 的差分包，4-3 的差分包。当出第 5 个版本的时候，服务器存储第 5 个版本的全量包及 5-2 差分包，5-3 差分包，5-4 差分包，不存储 5-1 差分包（即用户机器的版本是 1 版本，若要升级到第 5 个版本，则需要下载第 5 个版本的全量包）， 这种存储的包的量，基本上是 （跳数+1) * N 个包。

3.5 功能分配

服务器端主要有三大块：上传升级服务包功能、下载升级服务包功能，分布式图片服务器（提供升级包的差分功能）。分布式文件服务器主要也是由三大功能：接收上传数据、数据下载操作及数据包差分服务部分。服务器程序需与已建立的 Mysql 数据库互连，将信息保存到数据库下，其接口将于下面部分阐述。

4 接口设计

4.1 外部接口

用户界面

请参考：http://10.10.1.48/%E5%9B%BA%E4%BB%B6%E6%9B%B4%E6%96%B0/start.html

获得 access_token 接口信息

方法说明：为了确保请求的合法性，用户访问资源是，必须先申请 access_token 令牌。
HTTPS　GET 方法　　（获得 access_token 信息）
访问例子如下：
https://localhost:8010/oauth/token?client_id=mobile_1&client_secret=secret_1&grant_type=password&username=aa&password=aa

参数说明：

参数名称	是否必须	参数类型	备注
client_id	必须	String	管理员提供 client_id
client_secret	必须	String	管理员提供 client_secret
grant_type	必须	String	“password” 固定字段
username	必须	String	管理员提供 username
password	必须	String	管理员提供 password

返回信息：

{"access_token":"10bb2da80c1a442e99a4d914451e5fbe","token_type":"bearer","refresh_token":"8acf9cd2dbfe4bf88283bcf2a3f6735f","expires_in":11999,"scope":"read write trust"}

返回信息说明：

参数名称	参数类型	备注
access_token	String	获取的 AccessToken
token_type	String	令牌类型”bearer”或”mac”，暂无很明确的说明，通常是 bearer 或省略（可忽略）
refresh_token	String	用于刷新 Access Token 的 Refresh Token
expires_in	String	AccessToken 的有效期，以秒为单位
scope	String	Access Token 最终的访问范围，即用户实际授予的权限列表，用户在授权页面时，有可能会取消掉某些请求的权限，通常只作或只有登录认证的话（可忽略）

版本下载接口

方法说明：用户下载版本信息，验证成功后，返回下载文件地址
HTTPS　GET 方法　　（获得下载地址信息）
访问例子如下：
https://localhost:8010/file/download?access_token=10bb2da80c1a442e99a4d914451e5fbe&robot_type=2&model=2-v1.1.1;5-v1.2.1&ip=192.168.1.4&robot_id=15ae48ecs171faef35fafe5feaf12

参数名称	是否必须	参数类型	备注
access_token	必须	String	上一步，获得 Token
robot_type	必须	String	机器人型号
model	必须	String	更新模块如：3-v1.0.1 多个模块的话： 2-v1.1.1;5-v1.2.1;6-v1.1.1
ip	必须	String	Ip 地址
robot_id	必须	String	机器码（机器唯一标识）

返回结果如下：


```
{
    "data": {
        "upgradeType": "1",
        "times": [
            {
                "time": "1131",
                "model": "andorid"
            },
            {
                "time": "1241",
                "model": "linux"
            }
        ],
        "version": [
            {
                "model": "andorid",
                "md5": "CB39E15DC1F37ACCE3538EC66B091886",
                "url": "http: //10.10.1.14:8080/Alpha2Services-1.1.1.32--17--5mic.patch"
            },
            {
                "model": "linux",
                "md5": "CB39E15DC1F37ACCE3538EC66B091886",
                "url": "http: //10.10.1.14:8080/Alpha2Services-1.1.1.32--17--5mic.patch"
            }
        ]
    },
```

"code": "0",
"msg": "success"
}

返回信息说明：

参数名称	参数类型	备注
code	String	返回的信息码，请参考下面返回码说明
data	String	包含有 version 信息和 time 信息
data:version:model	String	升级的模块名称
data:version:md5	String	升级模块，升级包的 MD5 值
data:version:url	String	升级模块，升级包的 URL 地址
data:times:version	String	指定时间间隔的升级模块
data:times:time	String	指定升级模块的时间间隔
upgradeType	String	升级类型 0:非强制升级 1：强制升级
msg	String	返回提示信息，用于排除错误。

返回码说明：

返回码信息	返回码说明	备注
id	下载版本对应的 id 号码	用于用户升级完成后，反馈时使用
data	返回下载地址路径	
Code:0	成功	
Code:1	创建成功	
Code:2	无此对应版本	
Code:3	机器无权升级	
Code:4	无此语言版本	
Code:5	服务器端错误	

版本升级信息反馈接口

方法说明：用户升级完成后，反馈给服务器状态信息，升级是否成功信息返回。

HTTPS POST 方法 （获得下载地址信息）

访问例子如下：

https://localhost:8010/file/callback?access_token=10bb2da80c1a442e99a4d914451e5fbe&id=23&robot_id=15ae48ecs171faef35fafe5feafew&code=1

参数名称	是否必须	参数类型	备注
access_token	必须	String	上一步，后的的 Token
model	必须	String	模块名称
robot_id	必须	String	机器码，机器唯一标识
code	必须	String	0:无状态 1:成功 2:失败 3:暂未更新

返回结果如下：

{"code":"100","msg":"success"}

返回信息说明：

参数名称	参数类型	备注
code	String	返回的信息码，请参考下面返回码说明
msg	String	返回是否反馈成功标识信息 success　　fail

返回码说明：

返回码信息	返回码说明	备注
data	返回信息	
Code:0	成功	
Code:1	创建成功	
Code:2	无此对应版本	
Code:3	机器无权升级	
Code:4	无此语言版本	
Code:5	服务器端错误	

4.2　内部接口

内部接口方面，各模块之间采用函数调用、参数传递、返回值的方式进行信息传递。具体参数的结构将在下面数据结构设计的内容中说明。接口传递的信息将是以数据结构封装了的数据，以参数传递或返回值的形式在各模块间传输。

5 数据结构设计

5.1　数据库数据结构设计

DBMS 的使用上系统将采用 Mysql Server, 素材管理模块系统主要需要维护 3 张数据表：

1． 机器人信息表

项目信息表保存需要升级机器人的版本号，不同的版本需要建立不同的机器人信息，不同语言版本的机器人，同样需要建立不同的机器人信息。

2． 机器人详情表

机器人升级文件的详细地址，包括机器人升级版本，是否允许升级等操作，并包括可以升级的 ip 地址名单。

3． 升级文件详情表

用于保存升级文件详细地址地址，数据包的差分版本信息等。

5.2 物理数据结构设计

物理数据结构设计主要是设计数据在模块中的表示形式。数据在模块中都是以结构的方式表示。

1. **机器人信息表**

1.	机器人 ID	String
2.	机器人名称	String
3.	分类数	INT
4.	备注	String
5.	创建时间	DateTime

用于创建机器人更新服务项目，同时提供用户查询使用。

2. **机器人详情表**

用于输入上传文件信息，用户更新文件的详情信息。

1.	分类名	String
2.	文件名称	String
3.	最新版本	String
4.	用户限制	String
5.	创建时间	Date/Time

3. **升级文件详情表**

1.	文件 ID	String
2.	文件名称	String
3.	上传时间	Date/Time
4.	修改时间	Date/Time
5.	保存地址	String

用于保存更新文件信息，保存更新文件的地址信息。

数据类型可参照上面所述。

6 运行设计

6.1 运行模块的组合

客户机程序在有输入时启动接收数据模块，通过各模块之间的调用，读入并对输入进行格式化。在接收数据模块得到充分的数据时，将调用网络传输模块，将数据通过网络送到服务器，并等待接收服务器返回的信息。接收到返回信息后随即调用数据输出模块，对信息进行处理，产生相应的输出。

服务器程序的接收网络数据模块必须始终处于活动状态。接收到数据后，调用数据处理/查询模块对数据库进行访问，完成后调用网络发送模块，将信息返回客户端。

6.2 运行控制

运行控制将严格按照各模块间函数调用关系来实现。在各事务中心模块中，需对运行控制进行正确的判断，选择正确的运行控制路径。

在网络传方面，客户机在发送数据后，将等待服务器的确认收到信号，收到后，再次等待服务器发送回答数据，然后对数据进行确认。服务器在接到数据后发送确认信号，在对数据处理、访问数据库后，将返回信息送回客户机，并等待确认。

6.3 运行时间

在软体的需求分析中，对运行时间的要求为必须对作出的操作有较快的反应。网络硬件对运行时间有最大的影响，当网络负载量大时，对操作反应将受到很大的影响。所以将采用高速网络，实现客户机与服务器之间的连接，以减少网络传输上的开销。其次是服务器的性能，这将影响对数据库访问时间即操作时间的长短，影响加大客户机操作的等待时间，所以必须使用高性能的服务器，建议使用高性能处理器。硬件对本系统的速度影响将会大于软件的影响。

7 出错处理设计

7.1 出错输出信息

程序在运行时主要会出现两种错误：1、由于输入信息，或无法满足要求时产生的错误，称为软错误。2、由于其他问题，如网络传输超时等，产生的问题，称为硬错误。

对于软错误，须在用户上传成功判断及输入数据验证模块由数据进行数据分析，判断错误类型，再生成相应的错误提示语句，送到输出模块中。

对与硬错误，可在出错的相应模块中输出简单的出错语句，并将程序重置。返回输入阶段。

出错信息必须给出相应的出错原因，例：

返回码信息	返回码说明	备注
message	返回信息	用于记录返回信息，错误则是错误信息
Code:100	成功	
Code:101	创建成功	
Code:102	无此对应版本	
Code:103	机器无权升级	
Code:104	无此语言版本	
Code:500	服务器端错误	

7.2 出错处理对策

所有的客户机及服务器都必须安装不间断电源以防止停电或电压不稳造成的数据丢失的损失。若真断电时，客户机上将不会有太大的影响，主要是服务器上：在断电后恢复过程可采用 Mysql Server 的日志文件，对其进行 Rollback 处理，对数据进行恢复。

在网络传输方面，可考虑建立一条成本较低的后备网络，以保证当主网络断路时数据的通信。

在硬件方面要选择较可靠、稳定的服务器机种，保证系统运行时的可靠性。

8 安全保密设计

由于数据的传输上需要通过网络传输，为了客户端信息保密，需要在网络的传输过程中使用 Https 协议的方式发布接口协议。

客户端或终端调用接口时，需要使用 Oauth2.0 协议，对客户端进行认证，对于认证通过的客户端，发放 token，客户端或终端可以通过这个 Token 信息访问服务器资源。

由于使用 Https 协议传输，同时使用 Oauth2.0 对用户进行认证，提供系统访问的安全性，防止信息泄露。

9 维护设计

维护方面主要为对服务器上的数据库数据进行维护。可使用 Mysql 数据库维护功能机制。例如，定期为数据库进行 Backup，维护管理数据库死锁问题和维护数据库内数据的一致性等。

同时需要对分布式文件服务器进行管理，提供文件的上传服务和下载服务的正常操作。