| | |
|---|---|
| 编　　制 | 沈胜文 |
| 审　　核 | |
| 批　　准 | |
| 实施责任人 | |

# Amendment history 修改历史记录

| 版本号 | 修改说明 | 修改批准人 | 修改人 | 日期 | 签收人 |
|---|---|---|---|---|---|
| 101 | 创建文档 | | 沈胜文 | 2008-3-21 | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Microunit Technology Co.,Ltd.

| | |
|---|---|
| 编　　制 | 沈胜文 |
| 审　　核 | |
| 批　　准 | |
| 实施责任人 | |

**Table Of Contents 目录**



Microunit Technology Co.,LTD.

# 1. Overview 总述

## 1.1. Background 背景

CRC/MD5是法电项目 MuFTAD 中不可缺少的一部分，它为 MuFTAD 提供文件或分段的完整性校验；

为了保证该部分的独立性，按照扩展库的形式对该程序进行组织和开发，以方便为 MuFTAD 以外的项目提供支持；

## 1.2. Illuminate 说明

**CRC-32实现部分**，该扩展库的实现**不使用**其他外部特殊库，并且采用查表的方式实现；
扩展库必须提供对完整的文件和分段都可以进行校验的功能函数；

**MD5实现部分**，使用 openssl 库提供的 MD5库函数，对一个完整的文件或是分段进行校验；

*[注意]:*
*1、CRC-32校验使用的表达式为:*
$G(X) = X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^{8}+X^{7}+X^{5}+X^{4}+X^{2}+X^{1}+1$

## 1.3. Structure 结构

### 1.3.1. Rules Of Name 命名规则

该扩展库中函数一律使用 Mu_xxx 命名；

### 1.3.2. Library 库

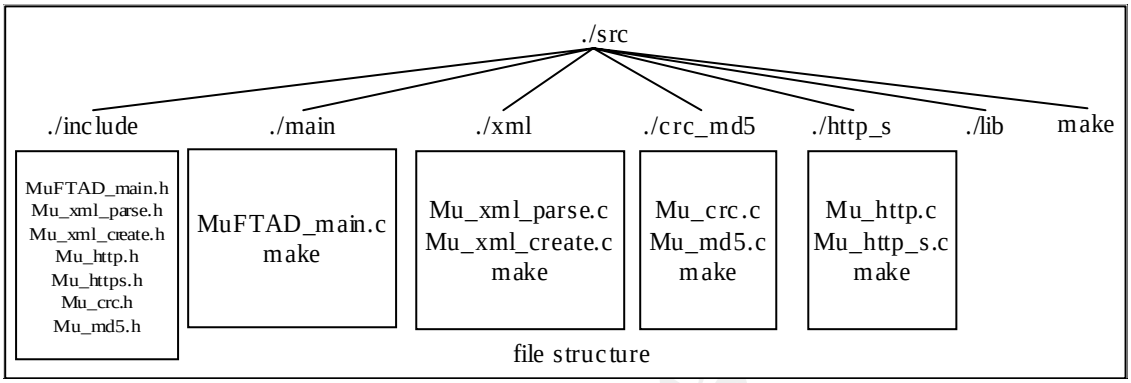
使用 MD5进行校验时，使用 openssl 库提供的库函数完成；

Microunit Technology Co.,LTD.

## 1.3.3. Organize 文件组织

*[注意]:*

*1、此为整个项目的文件组织方式;*




./src/include：文件夹，包含该项目中的所有头文件；

./src/main：文件夹，包含所有按法电《do3c00_SoftProtocol_0.1.0_RC1》流程所开发的程序；

./src/xml：文件夹，包含项目中所需要的 xml 处理库函数源代码；

./src/crc_md5：文件夹，包含项目中所需要的校验函数源代码，包括 CRC 和 MD5校验代码；

./src/http_s：文件夹，包含项目中所需要的与服务器交互的方式，包括 HTTP(s) GET、POST 方式；

s 文件夹，用于存储编译所生成的 xml、http 和 https、crc/md5库。软件编译连接时使用该文件夹下的库；

./src/make：文件，总的编译入口；

*[注意]:*

*1、各对应文件夹下的源文件按需要添加，但是所作修改必须对 makefile 文件作相应的修改，以正确编译;*

## 1.4. Reference 参考文献

AN42-循环冗余检验（CRC）原理与实现1.1.pdf
并行 CRC_32校验码生成算法研究及其实现.pdf
www.openssl.org

Microunit Technology TD.

# 2. Analyse 分析

在 MuFTAD 项目中，需要对二种不同的内容进行 CRC-32/MD5校验：

1、未下载完全的节目。文件是按分段下载的，每当下载完成一个分段，都必须对其完整性进行校验；

2、当所有分段下载完全后，需要对完整的节目进行校验；

*[注意]:*

*1、参考《doc00_SoftProtocol_0.1.1.doc》中说明介绍;*

*2、固件升级时的校验只使用 MD5;*

# 3. Design Of Routines 函数设计

## 3.1. Mu_Crc32

■ **接口**

int Mu_Crc32File(int fd, unsigned int crc32)

■ **说明**

该函数用于校验文件句柄为 fd 的文件的完整性，函数利用文件内的所有字符，并加上 CRC 字段，计算 CRC 值；

若要对文件内的内容进行校验，在调用该函数前，必须确保前期对文件的写操作内容，全部刷新至磁盘；

函数仅仅计算 CRC 值，不对文件内的内容作任何修改，也不会关闭文件句柄，文件句柄的关闭由调用者完成；

■ **输入**

fd：待校验的文件句柄；

crc32：文件的 CRC 余数，加此参数和文件内容一起进行 CRC 校验，以确定文件的完整性；

■ **输出**

校验状态

■ **处理流程**

略

MicroUnit Technology Co.,LTD.

## 3.2. Mu_Crc32Segment

■ **接口**
int Mu_Crc32Segment(int fd, off_t seek, size_t len, unsigned int crc32)

■ **说明**
该函数用于校验文件句柄为 fd 的某一部分的完整性，函数利用文件内的指定部分，加上 CRC 余数，计算 CRC；

在校验前，必须确保对所校验部分的修改全部刷新至磁盘；

函数仅仅计算 CRC 值，不对文件相应部分作任何修改，也不会关闭文件句柄，文件句柄的关闭由调用者完成；

■ **输入**
fd：同3.1.中说明；
seek：用于在文件中定位；
len：指明校验的长度；
crc32：同3.1.中说明；

■ **输出**
校验状态

■ **处理流程**
略

## 3.3. Mu_Md5File

■ **接口**
int Mu_Md5File(int fd, char *md5)

■ **说明**
该函数用于校验文件句柄为 fd 的文件的完整性，函数利用 openssl 提供的函数库，计算文件的 md5散列值，然后与参数 md5比较；

在校验前，必须确保对文件的所有修改均刷新至磁盘；

函数仅仅计算文件的 MD5值，并与调用者提供的 MD5散列值比较。但是该函数不会关闭使用的文件句柄；

Microunit Technology Co,LTD.

- **输入**
  fd：同3.1.中说明
  md5：调用者提供的 MD5散列值；

- **输出**
  校验状态值

- **处理流程**
  略

### 3.4. Mu_Md5Segment

- **接口**
  int Mu_Md5Segment(int fd, off_t seek, size_t len, char *md5)

- **说明**
  同3.2.中说明

- **输入**
  同3.2.和3.3.中说明

- **输出**
  同3.3. 中说明

- **处理流程**
  略

# 4. 运行环境

## 4.1. 设备

达芬奇数字平台 TMS320DM6446 双核 ARM9+DM64X SRAM(8M)、FLASH（256M）、NAND flash (2G)存储。

## 4.2. 支持软件

在安装了 openssl 库的 Linux 内核主机上均可运行。

Microunit Technology Co,LTD.

## 4.3. 接口

本库针对不同的需要提供不同的操作函数，具体的调用由用户完成；

## 4.4. 控制

略

Microunit Technology Co,LTD.