终端控制器 Toolkits 调试协议

文件状态: [ ] 草稿 [√] 正式发布 [ ] 正在修改	项目名称:			
	项目编号:			
	文件标识:	**终端控制器 Toolkits 调试协议**		
	当前版本:	**V1.0**		
	编　　制:		**日期:**	**2021-03-26**
	标 准 化:		日期:	
	审　　核:		日期:	
	批　　准:		日期:	

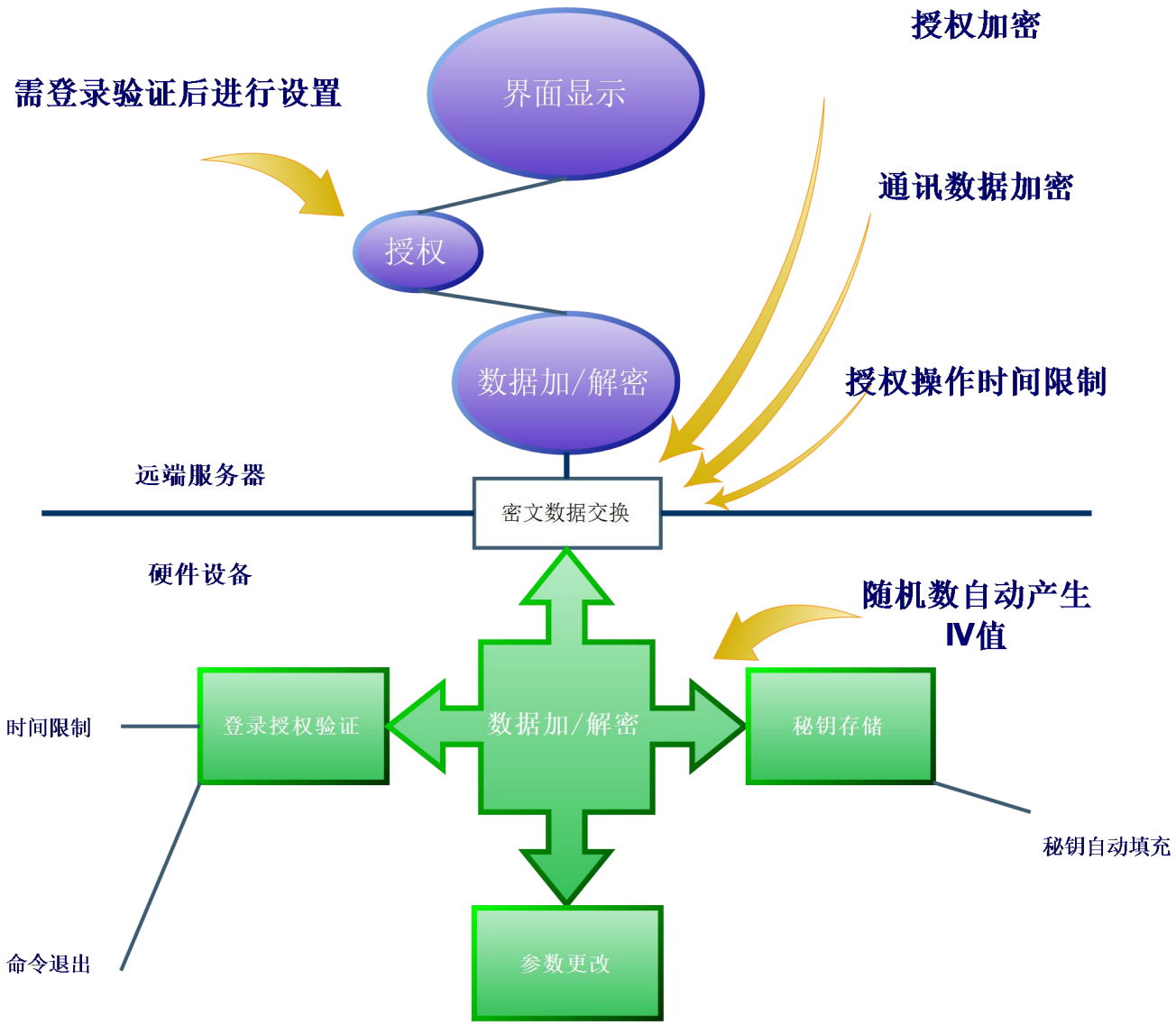
版本历史

版本/状态	作者	参与者	起止日期	备注
V1.0				1、满足对接 toolkits 软件的通用控制器协议； 2、满足华为红线管理要求。

目录

一、协议介绍

本协议适应于上海三思生产的控制器和调试软件 Toolkits 之间的通信，协议兼容各类通信接口。



二、协议说明

2.1 传输说明

除非另有说明，否则协议帧中所有数据均以 16 进制表示，在多字节传输时遵循高字节在前，低字节在后的顺序进行通讯传输。

2.2 字节格式

除非另有说明，否则协议帧中所有字节都是无符号的。

2.3 R 码表

编码	描述
0x00	操作成功
0x01	操作失败
0x02	无效命令码
0x03	操作超时
0x04	无效参数

2.4 校验码算法

16 位 CRC 检验算法的 C 语言实现

```
unsigned short gen_crc(const unsigned char *buffer, int buffer_length)
{
	unsigned char c, treat, bcrc;
	unsigned short wcrc = 0;
	int i, j;
	for (i = 0; i < buffer_length; i++)
	{
		c = buffer[i];
		for (j = 0; j < 8; j++)
		{
			treat = c & 0x80;
			c <<= 1;
			bcrc = (wcrc >> 8) & 0x80;
			wcrc <<= 1;
			if (treat != bcrc)
				wcrc ^= 0x1021;
		}
	}
	return wcrc;
}
```

三、数据帧格式

帧主要由三部分组成：帧头、帧数据和帧尾。每帧由帧起始符、有效长度、加密参数、保密信息密文、校验码及帧结束符等 6 个部分组成。

帧起始符	有效长度	加密参数	保密信息密文	校验码	结束符
1Byte	2Byte	19Byte	NByte	2Byte	1Byte
0xA5	XX XX	XX……XX	XX……XX	XX	0x5A

- 帧起始符：表示一帧数据的开始，其值为 0xA5。
- 有效长度：有效长度=加密参数字节数+保密信息密文字节数。
- 加密参数：加密模式(1 字节)+有效明文长度(2 字节)+IV(16 字节)。**加密模式分为固定加密模式(0x00)和用户加密模式(0x01)。**
  固定加密模式：采用固定秘钥对数据进行加密，且此模式仅对授权命令有效；
  用户加密模式：采用指用户秘钥对数据进行加密。
- 保密信息密文：保密信息密文解密后，得到信息由“有效明文+填充数据”组成。对于 AES256 加密算法，加密参数字段中的“有效明文长度”指明了“有效明文”的长度。
- 校验码： 采用 CRC16 的校验方式对从帧起始符到数据域内的所有数据的校验，算法见校检码章节。
- 结束符： 结束符为 0x5A。

四、保密信息密文

保密信息密文是指有效明文加填充字节加密后的数据。加密前数据组成如下：

有效明文			填充数据
命令码	应答码	有效参数	填充数据
1Byte	1Byte	NByte	NByte

- 命令码：同一种命令码，回复命令码是请求命令码与 0x80 相或运算后获得。例如授权请求命令码为 0x01，则授权请求回复命令码为 0x01 | 0x80；
- 应答码：设备对操作命令的确认，范围在 0~0xFE。0xFF 表示该帧是个操作帧，具体见“R 码表”
- 数据参数：根据具体的命令码有所不同。具体可参照如下各命令码详解；
- 为满足 AES256 加密，长度必须为 16 的整数倍，即命令码+响应码+数据参数不足 16 的倍数，以 0 补全；

4.1 授权

功能：服务器请求设备端授权
发送：服务器->设备

命令码	应答码	数据参数
0x01	0xFF	用户秘钥(32Byte)

回复：设备->服务器

命令码	应答码	数据参数
0x81	R	无

4.2 修改用户秘钥

功能：服务器发送修改用户秘钥指令码给设备，用以修改用户秘钥。
发送：服务器->设备

命令码	应答码	数据参数
0x03	0xFF	新用户秘钥(32Byte)

回复：设备->服务器

命令码	应答码	数据参数
0x83	R	无

说明：

- 用户秘钥修改后需重新获取授权。

4.3 寄存器操作

4.3.1 服务器对设备寄存器读操作

发送：服务器->设备

命令码	应答码	数据参数			
0x04	0xFF	寄存器 1 地址	寄存器 2 地址	.....	寄存器 N 地址
		2Byte	2Byte	2Byte*N	2Byte

回复：设备->服务器

命令码	应答码	数据参数								
0x84	R	寄存器数据 1				寄存器数据 N-1	寄存器数据 N			
		地址	状态码	长度	数据	.....	地址	状态码	长度	数据
		2Byte	1Byte	1Byte	N Byte		2Byte	1Byte	1Byte	N Byte

说明：

- 状态码字段：0 表示操作成功，1 表示操作失败，长度字段为 0，数据为空；
- 多寄存器读操作时，需考虑设备传输数据长度的能力，可参考附录一通用寄存器“帧数据容量”数值；

4.3.2 服务器对设备寄存器写操作

发送：服务器->设备

命令码	应答码	数据参数						
0x05	0xFF	寄存器 1			寄存器 2	寄存器 N		
		地址	长度	数据	.....	地址	长度	数据
		2Byte	1Byte	N Byte		2Byte	1Byte	N Byte

回复：设备->服务器

命令码	应答码	数据参数					
0x85	R	寄存器 1		寄存器 2		寄存器 3	
		地址	状态码	地址	状态码	地址	状态码

说明：

- 状态码字段：0 表示操作成功，1 表示操作失败，2 表示寄存器不支持；
- 多寄存器写操作时，需考虑设备传输数据长度的能力，可参考附录一通用寄存器“帧数据容量”数值；

4.4 文件操作

4.4.1 获取文件列表

返送：服务器->设备

命令码	应答码	数据参数	
0x06	0xFF	序列号	

回复：设备->服务器

命令码	应答码	数据参数	
0x86	R	序列号	n 条文件列表信息（分包传输，≤64Bytes）

每条文件列表信息格式如下：

文件 ID	文件名称长度	文件名称	文件最大长度	文件操作类型	保留
1Byte	1Byte	不定长 ASCII 码（≤32Bytes）	4Bytes	1Byte	1Byte

说明：

- 文件 ID：文件的唯一标识符；
- 文件操作类型字段：0 表示只读文件，1 表示只写文件(如升级文件和配置文件等)，2 表示可读写文件；
- 序列号从 0 开始递增，每包序号加 1，当传输内容小于 64Byte 时，表示传输结束；

4.4.2 发送下载文件信息

返送：服务器->设备

命令码	应答码	数据参数		
0x07	0xFF	文件 ID	唯一码	文件长度
		1 Byte	2 Byte	4 Byte

回复：设备->服务器

命令码	应答码	数据参数		
0x87	R	文件 ID	唯一码	帧数据容量
		1 Byte	2 Byte	2 Byte

说明：

- 文件 ID：文件的唯一标识符；
- 唯一码： 整个升级文件 CRC16 校验码；
- 文件长度：整个文件的长度；
- 帧数据容量，设备每包传输数据长度的上限，可参考附录一通用寄存器“帧数据容量”数值；

4.4.3 下载文件数据

返送：服务器->设备

命令码	应答码	数据参数
0x08	0xFF	文件 ID(1 Byte) + 文件地址偏移(4 Byte) + 数据包内容

说明：

- 文件 ID：文件的唯一标识符；
- 文件地址偏移： 传输文件的偏移地址；
- 数据包内容：不定长，可根据整包长度计算出数据内容长度；

回复：设备->服务器

命令码	应答码	数据参数
0x88	R	文件 ID(1 Byte) + 文件地址偏移(4 Byte) + 数据包长度(2 Byte)

说明：

- 文件 ID：文件的唯一标识符；
- 文件地址偏移： 传输文件的偏移地址；
- 数据包长度：返回数据包长度，可用于验证数据传输的可靠性；

注：

下载升级文件时，当某包文件地址偏移+数据包长度大于等于文件长度时，则设备认为传输结束，设备端回复后可能会自动重启。

4.4.4 查询上传文件信息

发送：服务器->设备

命令码	应答码	数据参数
0x09	0xFF	文件 ID(1 Byte)

回复：设备->服务器

命令码	应答码	数据参数			
0x89	R	文件 ID	唯一码	文件长度	帧数据容量
		1 Byte	2 Byte	4 Byte	2 Byte

说明：

- 文件 ID：文件的唯一标识符；
- 唯一码： 整个升级文件 CRC16 校验码；
- 文件件长度：整个文件的长度；
- 帧数据容量，设备每包传输数据长度的上限，可参考附录一通用寄存器“帧数据容量”数值；

4.4.5 获取上传文件数据

发送：服务器->设备

命令码	应答码	数据参数
0x0a	0xFF	文件 ID(1 Byte) + 文件地址偏移(4 Byte) + 数据包长度(2 Byte)

说明：

- 文件 ID：文件的唯一标识符；
- 文件地址偏移： 传输文件的偏移地址；
- 数据包长度：返回数据包长度，可用于验证数据传输的可靠性；

回复：设备->服务器

命令码	应答码	数据参数
0x8a	R	文件 ID(1 Byte) + 文件地址偏移(4 Byte) + 数据包内容

说明：

- 文件 ID：文件的唯一标识符；
- 文件地址偏移： 传输文件的偏移地址；
- 数据包内容：不定长，可根据整包长度计算出数据内容长度；

注：上传升级文件时，当某包文件地址偏移+数据包长度大于等于文件长度时，则认为传输结束。

附录一 通用寄存器对照表

寄存器地址	名称	长度	单位	操作类型	数据说明
0x0000	设备名称	不定长 ≤32Byte		只读	
0x0001	设备类型	2Byte		只读	LC600： 0x0001 LC1000：0x0002 XES220：0x0003 LC502： 0x0004
0x0002	设备厂商信息	不定长 ≤32Byte		只读	
0x0003	设备 MAC	8Byte		只读	
0x0004	产品序列号	不定长 ≤32Byte		只读	
0x0005	硬件版本号	4Byte	硬件版本号	只读	高位在前，低位在后， 如：0x10000001 表示为 1.0.0.1
	软件版本号	4Byte	软件版本号	只读	高位在前，低位在后， 如：0x10000001 表示为 1.0.0.1
0x0006	设备状态	1Byte			0x00：正常 0x01：运行异常
0x0007	系统时间-年月日时分秒	6Byte	系统时间-年月日时分秒	读写	控制器本地时间，格式为年月日时分秒，数据为 BCD 码；其中年份是基于 2000 年的偏移，如字段年为 0x20，表示为 2020 年；
0x0008	复位操作寄存器	1Byte		读写	0x00 表示复位，0x01 表示复位设备
0x0009	复位信息寄存器	1Byte		只读	0x01：软件复位 0x02：硬件复位 0x03：异常复位
0x000A	恢复出厂设置寄	1Byte		读写	0x00 表示无需操作，0x01 表示清除统计数据
0x000B	清除统计数据	1Byte		读写	0x00 表示无需操作，0x01 表示清除统计数据
0x000C	帧数据容量	1Byte		只读	设备每包传输数据长度的上限
0x000D	上电后运行时间	4Byte		只读	上电之后的设备运行时间
.....	总工作时间	4Byte		只读	设备总工作时间
0x0FFF				保留	

附录二 LC502 专用寄存器对照表

寄存器地址	名称	长度	单位	操作类型	数据说明
0x1000	本机 IP 地址	4Byte		可读写	高字节在前，低字节在后，如 0xC0A80102 表示为 192.168.1.2
0x1001	本机掩码地址	4Byte		可读写	同 IP 地址格式
0x1002	本机网关地址	4Byte		可读写	同 IP 地址格式
0x1003	本机 UDP 端口号	2Byte		可读写	17222
0x1004	X9 TCP 端口号	2Byte		可读写	4080
0x1005	AR502H 服务器地址	4Byte		可读写	同 IP 地址格式
0x1006	AR502H UDP 端口号	2Byte		可读写	17222
0x1007	Toolkits UDP 端口号	2Byte		可读写	3434
0x1008	RS485_1 波特率	2Byte		可读写	
0x1009	RS485_2 波特率	2Byte		可读写	
0x100a	RS485_3 波特率	2Byte		可读写	
0x100b	HPLC 波特率	2Byte		可读写	
0x100c	设备状态寄存器	4Byte		只读	0x01 表示 PLC 上线，0x02 表示 UDP 上线，0x03 表示未知上线，0x04 表示离线
0x100d	通道 1 调光寄存器	2Byte		可读写	高字节 0x01 开灯，0x00 关灯，低字节表示亮度值(0~100)
0x100e	通道 1 电流	2Byte	0.1ma	只读	
0x100f	通道 1 电压	2Byte	10mv	只读	
0x1010	通道 1 功率因数	2Byte	0.001	只读	有效值为 0~1000，单位为 0.001，对应实际功率因数为 0~1.000
0x1011	通道 1 电压频率	2Byte	0.01Hz	只读	电压频率有效值为 4000~7000，单位为 0.01Hz，对应实际电压频率为 40.00~70.00Hz，FFFFH 为不支持
0x1012	通道 1 有功功率	2Byte	0.01W	只读	
0x1013	通道 1 总消耗电量	4Byte	0.01 度	只读	单位是 0.01 度，0xFFFFFFFF 表示不支持
0x1014	通道 1 总亮灯时间	4Byte	Min	只读	单位是分钟，最大支持 8171 年的亮灯总时间记录，0xFFFFFFFF 表示不支持。
0x1015	通道 1 漏电流	2Byte	0.1ma	只读	
0x1016	通道 1 组播号	8Byte		只读	以 Bit 为单位，1 表示属于这个组，0 表示不属于，故设备最多可同时属于 64 个组
0x1017				保留	
0x1018				保留	
0x1019				保留	
0x101a	通道 2 调光寄存器	2Byte		可读写	高字节 0x01 开灯，0x00 关灯，低字节表示亮度值(0~100)
0x101b	通道 2 电流	2Byte	0.1ma	只读	

0x101c	通道 2 电压	2Byte	10mv	只读	
0x101d	通道 2 功率因数	2Byte	0.001	只读	有效值为 0~1000，单位为 0.001，对应实际功率因数为 0~1.000
0x101f	通道 2 电压频率	2Byte	0.01Hz	只读	电压频率有效值为 4000~7000，单位为 0.01Hz，对应实际电压频率为 40.00~70.00Hz，FFFFH 为不支持
0x1020	通道 2 有功功率	2Byte	0.01W	只读	
0x1021	通道 2 总消耗电量	4Byte	0.01 度	只读	单位是 0.01 度，0xFFFFFFFF 表示不支持
0x1022	通道 2 总亮灯时间	4Byte	分钟	只读	单位是分钟，最大支持 8171 年的亮灯总时间记录，0xFFFFFFFF 表示不支持。
0x1023	通道 2 漏电流	2Byte	0.1ma	只读	
0x1024	通道 2 组号	8Byte		只读	以 Bit 为单位，1 表示属于这个组，0 表示不属于，故设备最多可同时属于 64 个组
0x1025				保留	
0x1026				保留	
0x1027				保留	
0x1028	4 路 DI 寄存器	1Byte		只读	从 bit[0-3]依次表示 DI1-DI4,1 表示开，0 表示关
0x1029	2 路 DO 寄存器	1Byte		可读写	从 bit[0-1]依次表示 DO1-DO2，
0x102a	RDM 状态寄存器	1Byte		只读	1 表示 LINKON,0 表示 LINKOFF
0x102b	RDM 温度传感器	2Byte	0.1℃	只读	最高位为 0 表示正温;为 1 表示负温,需进行补码运算,单位为 0.1℃
0x102c	RDM 湿度传感器	2Byte	0.1%Rh	只读	范围为 0-99.9%,单位为 0.1%Rh
0x102d	PM2.5 寄存器	2Byte		只读	范围为 0-1000,单位为 1
0x102e	气压	2Byte	1hPa	只读	大气压值,范围为 300-1100hPa,单位为 1hPa
0x102f	噪音	2Byte	0.1dB	只读	噪声值,范围为 30~130dB,单位为 0.1dB
0x1030	风速传感器	2Byte	0.1 米/秒	只读	风速值,范围为 0-600,单位为 0.1 米/秒
0x1031	风向传感器	2Byte		只读	风向值,范围为 0-3600,单位为 0.1°
0x1032	RS-WS 温湿度状态	2Byte		只读	1 表示 LINKON,0 表示 LINKOFF
0x1033	RS-WS 温度传感器	2Byte	0.1℃	只读	最高位为 0 表示正温;为 1 表示负温,需进行补码运算,单位为 0.1℃
0x1034	RS-WS 湿度传感器	2Byte	0.1%Rh	只读	湿度值,范围为 0-99.9%,单位为 0.1%Rh
0x1035	红外传感器状态	1Byte		只读	1 表示 LINKON,0 表示 LINKOFF

0x1036	红外传感器触发	2Byte		只读	触发：FFFFH; 未触发：0000H; 上电前 30s 热稳定时间，00A5H
.....	.....			保留	
0x10ff	保留			保留	