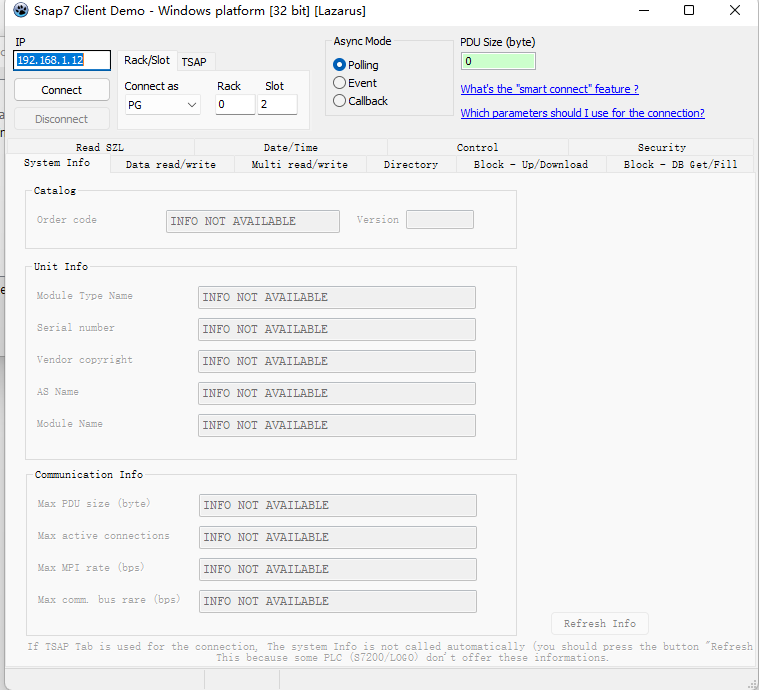
S7协议模拟器使用说明

# client端使用说明

## 启动clientdemo，双击clientdemo.exe启动客户端，如下图所示



**IP说明：**

在上图IP下输入需要连接的server端IP。

**Connect as说明：**

在PLC S7300中PG/OP通讯的意思：  
1、PG就是可连接的最多电脑个数。  
2、OP是触摸屏一类的数。  
3、S7是cpu可以连接的下位机硬件数。  
4、PG默认是1，如果要增加电脑数，需要减小S7，增加PG。

**TSAP说明：**

只要smart200与上位机进行opc的以太网通讯，或是与西门子s71200 、s7300 s7400直接的s7通讯可以设定。

在弹出的窗口中“查找CPU”，在网络中选择要做OPC通信的PLC，紧接着设置本地和远程的TSAP号。  
其中“本地”指的是电脑上S7-200 PC Access SMART，“远程”指的是PLC。  
TSAP是Transport Service Access Point的缩写（运输服务接入点），表示的是连接资源的地址。使用S7-200 SMART CPU时TSAP号只能设置下面的值：

02.00   
02.01   
03.00   
03.01   
使用者也不能设置其他的数值，因为设置的其他数值后，不能选择“确认”按钮完成配置。软件不支持其他数值。

Async mode:通信模式

Polling 轮询模式

Event 事件模式

Callback 回调模式

PDU（协议数据单元）大小

CPU S7 300/400/1200/1500/WinAC - Use Rack/Slot TAB，配置不同的cpu选择后面的rack/slot不同。

"Connect as" is the Connection Type, [PG/OP/S7 Basic].连接类型为这三种。

Each one is good enough.

S7300 : Rack 0 - Slot 2

S7400 : Depends on the hardware configuration (Rack 0 - Slot 3 should be good)

S71200 : Rack 0 - Slot 0

S71500 : Rack 0 - Slot 0

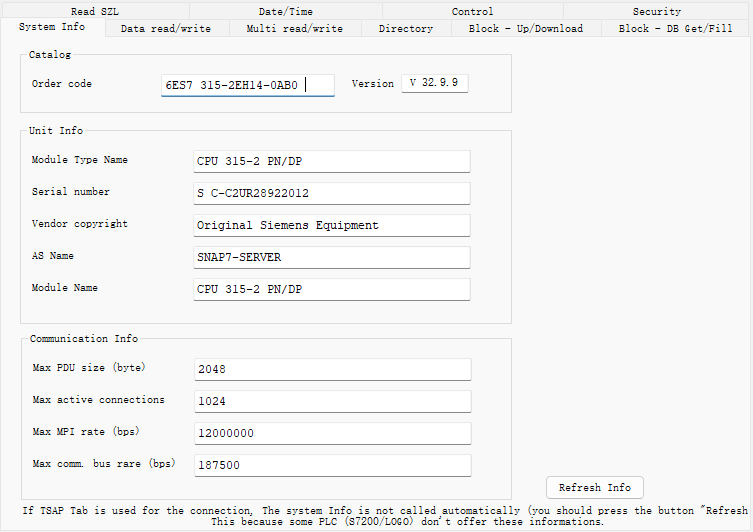
WinAC : Rack 0 - Slot See the Station Configuration.

CPU S7200/LOGO 0BA7/LOGO 8 - Use TSAP TAB

S7200 : LocTSAP 4D.57 - RemTSAP 4D.57 (or 02.00 - 02.00)

LOGO : Depends on Tools->Ethernet Connections of LOGOComfort.

## 系统信息说明



Catalog：目录

Order code：订购代码

Version：版本号

Unit info：单元信息

Module Type Name：CPU型号

Serial number：序列号

Vender copyright：出售版权

As Name：别名

Module Name：模块名称

Communication info：连接信息

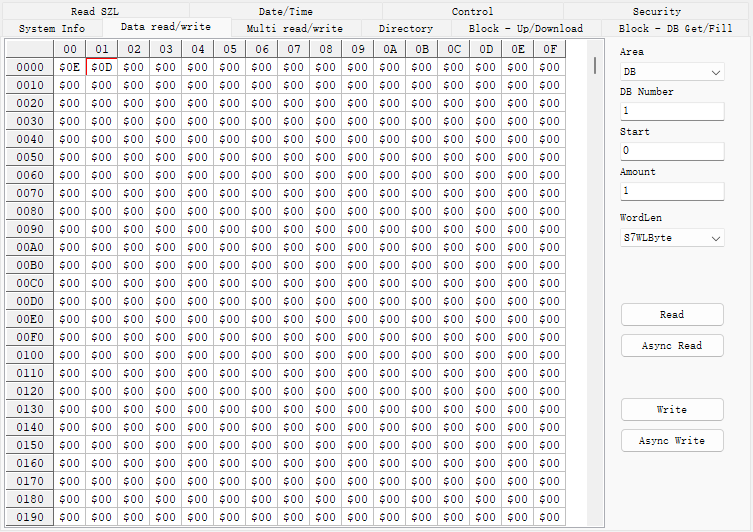
Max PDU size：连接信息最大PDU块。

Max active connection：最大连接数

Max MPI rate(bps)：最大传输速率

Max comm. Bus rare(bps):通信总线最大传输速率

**Data read/write:**



数据读取模块：

Area读取数据的位置，DB Number读取的模块哪一个，和server中的DB 1，DB 2，DB3对应。

Start：开始地址

Amount：数量

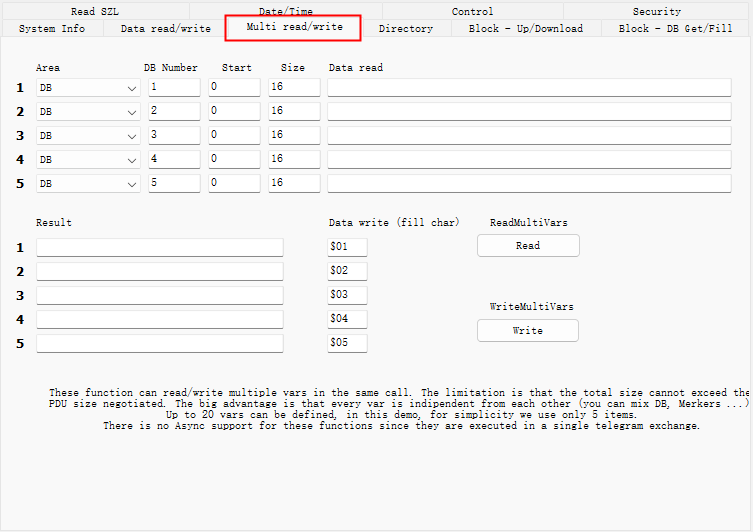
Wordlen:传输的字符类型。

Read：同步读取数据，Async Read：异步读取

Write：同步写入，Async Write：异步写入。

## Multi read/write

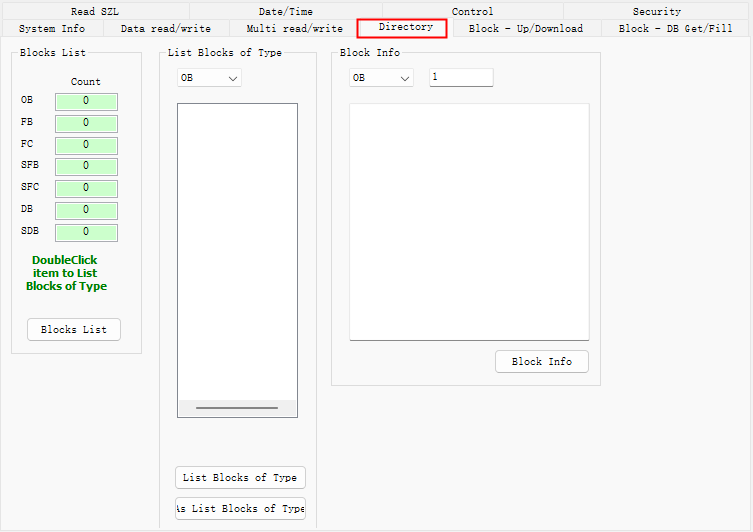
多块数据写入或读取



these function can read/write multiple vars in the same call.the limitation is that the total size cannot exceed the up to 20 vars can be defined, in this demo, for simplicity we use only 5 items. there is no async support for these functions since they are executed in a single telegram exchange.

这些函数可以在同一个调用中读取/写入多个变量。限制是总大小不能超过最多可以定义 20 个变量，在这个演示中，为简单起见，我们只使用 5 个项目。 这些功能没有异步支持，因为它们是在单个电报交换中执行的。

## Directory



程序采用结构化程序，把程序分成多个模块，各模块完成相应的功能。结合起来就能实现一个复杂的控制系统。就像高级语言一样，用子程序实现特定的功能，再通过主程序调用各子程序，从而能实现复杂的程序。

在S7-300/400PLC中写在OB1模块里和程序就是主程序，子程序写在功能(FC)，功能块(FB)。

      ① FC运行是产生临时变量执行结束后数据就丢失-----不具有储存功能

      ② FB运行时需要调用各种参数，于是就产生了背景数据块DB。例如用FB41来作PID控制，则它的PID控制参数就要存在DB里面。FB具有储存功能

      ③ 系统功能块（SFB）和系统功能（SFC）也是相当于子程序，只不过SFB和SFC是集成在S7 CPU中的功能块，用户能直接调用不需自已写程序。

      ④ SFC与FC不具有储存功能,FB和SFB具有储存功能。

      ⑤ OB模块相当于子程序，负责调用其他模块。如果程序简单只需要OB就可以实现。

用西门子plc编程时，可以用到功能块FB和功能FC（FB、FC都是组织块）资料上说FB与FC都可以作为用户编写的子程序，但两者是有一定区别的，在使用时应注意。

     FB--功能块，带背景数据块

     FC--功能，相当于函数

     他们之间的主要区别是：FC使用的是共享数据块，FB使用的是背景数据块。

     举个例子，如果您要对3个参数相同的电机进行控制，那么只需要使用FB编程外加3个背景数据块就可以了，但是，如果您使用FC，那么您需要不断的修改共享数据块，否则会导致数据丢失。FB确保了3个电机的参数互不干扰。

      FB,FC本质都是一样的，都相当于子程序，可以被其他程序调用（也可以调用其他子程序）。他们的最大区别是，FB与DB配合使用，DB中保存着FB使用的数据，即使FB退出后也会一直保留。FC就没有一个永久的数据块来存放数据，只在运行期间会被分配一个临时的数据区。

在实际编程中，是使用FB还是FC，要看实际的需要决定。

      FB与FC没有太大的差别，FB带有背景数据块，而FC没有。所以FB带上不同的数据块，就可以带上不同的参数值。这样就可以用同一FB和不同的背景数据块，被多个对象调用。FC和FB像C中的函数，只不过FB可以生成静态变量，在下次函数调用时数据可以保留，而FC的变量只在调用期内有效，下次调用又重新更换。

      这是一般的理解；FB需要背景数据块，而FC是没有的；参数的传递方式不同，FB的输入输出对应着背景数据块地址，而FC的输入输出是没有实际地址对应的，只有的程序调用时，才会和实际的地址产生对应关系。FB参数传递的是数据，FC参数传递的是数据的地址。

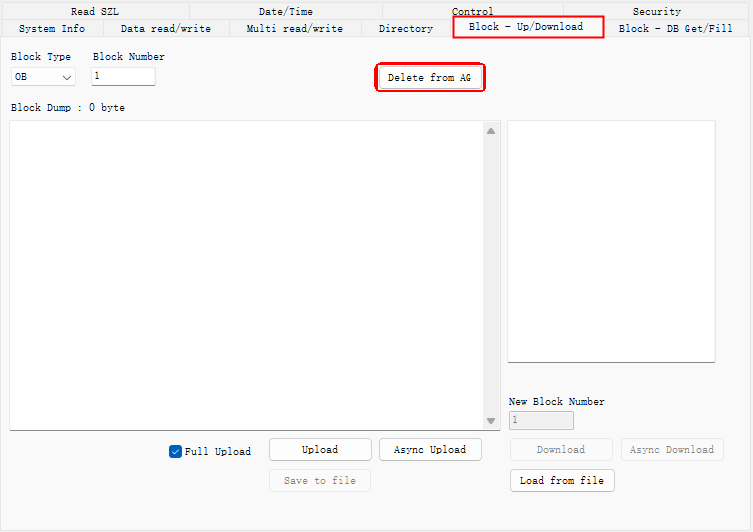
      FB（功能块）的处理方式是围绕着数据块处理数据，他的入口参数和出口参数都是数据块里的数据，以及STAT的数据都是数据块里,入口参数和出口参数、STAT可以认为是静态数据，这些数据不会因为函数消失而逝去，他会一直保存在数据块里。FB里的变量与他的背景数据块是一一对应的，而他的对应并不是一层不变的。

      更确切的说，FB里的变量在调用时将根据AR2的值当作偏移量与背景数据块是一一对应。如果一个FB功能块里没有入口参数、出口参数及STAT数据，他将不需要背景数据块，这时的FB和没有入口出口参数的FC就没有什么区别了，就只能使用临时变量和全局变量了。

      用很多人认为，FB的背景数据块必须由FB生成、FB里的第一个变量对应着背景数据块的第一个变量，还有就是由FB生成的数据块只能作为FB的背景数据块使用。其实这些理解是错误的，FB的背景数据块不一定是通过FB生成的，可以像生成共享数据块一样生成FB的背景数据块。

      换句话说，普通的数据块也可以作为FB的背景数据块，不过这种做法是有一定前提的，就是这个数据块的字节数必须大于等于FB所需的字节数，如果小于FB所需的字节数时，FB访问到超出背景数据块的变量时就会找不到变量的地址，肯定会出错了。FB里的第一个变量对应可以对应数据块字节数减去FB所需背景数据块字节数里的任意位置的变量。

## Block-UP/DownLoad



Block type:模块名称，Block Number：模块编号

Delete from AG：删除数据从网关。AG （Access Gateway接入网关）

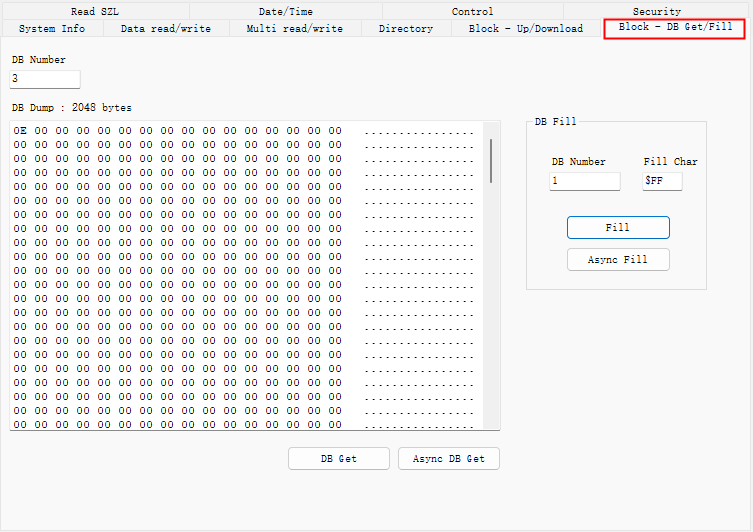
Full Upload：全部上传，Upload：同步上传，Async Upload：异步上传

DownLoad：同步下载，async Download：异步下载

Save to file: 保存到文件

Load from file：加载文件

## Block-DB get/fill



整块输进去DB的数据获取或者上传填充。

DB Number：要获取/填充的数据块的编号。

DB Dump：获取的数据块的大小

DB Get：同步获取数据

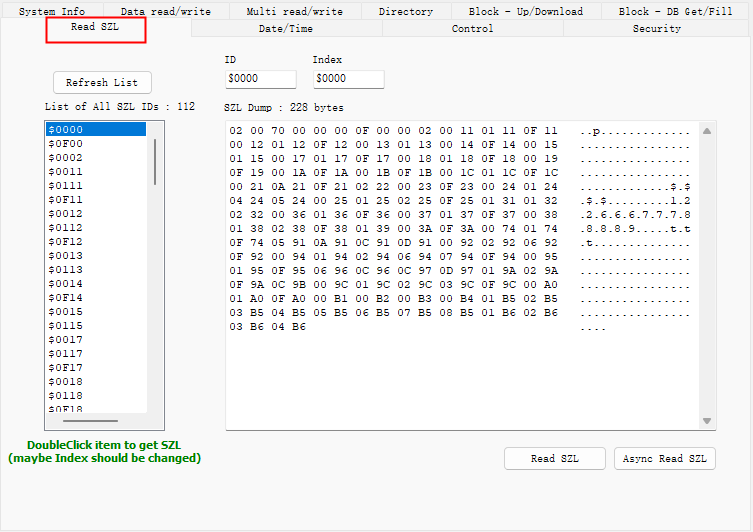
Async DB Get：异步获取数据

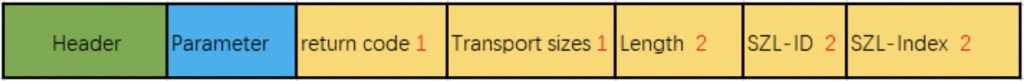
Fill Char:要填充的数据

Fill：同步对server端数据进行填充。

Async Fill：异步对server端数据进行填充。

## Read SZL



读取SZL说明文档： <http://blog.nsfocus.net/s7comm-readszl-0427/>

Refresh List：刷新SZL ID的列表。

List Of All SZL ID是：112——表示SZL的列表，数字位有多少个SZL ID。

ID位SZL的ID号，Index为SZL-index的值。

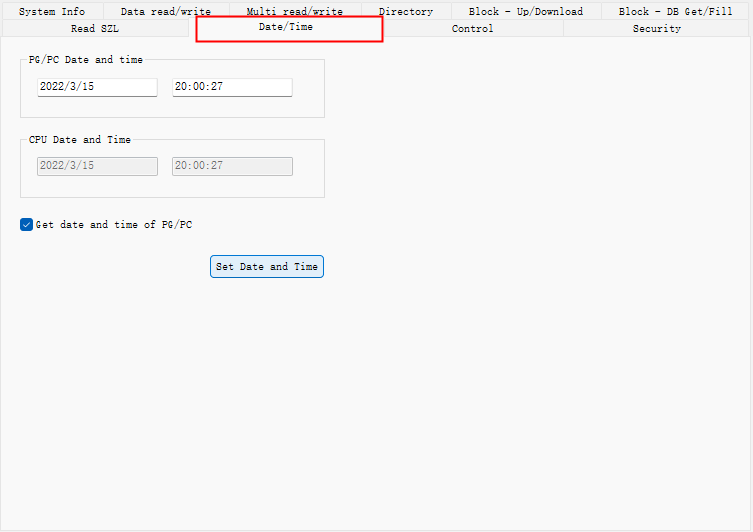
SZL Dump：228 bytes下面的列表中表示当前szl-ID和SZL-Index联合后取出来的值。

在左边的SZL-ID列表中双击ID号，可以获取到这个ID号和Index组合后获取的值。

Read SZL：同步从server端读取SZL中的值。

Async Read SZL：异步读取SZL的值。

## Date/Time



PG，Programmer的编写，编程器，或者是西门子编程电脑

PC，Personal Computer，就是电脑

在西门子软件中的经常出现PG/PC这个字眼，不用怕，其实指的就是自己正在使用的编程电脑。

Set PG/PC Interface，即设置自己所用的电脑的接口，用什么接口与设备去连接。

PG/PC Station，就是配置自己电脑成一个站点。

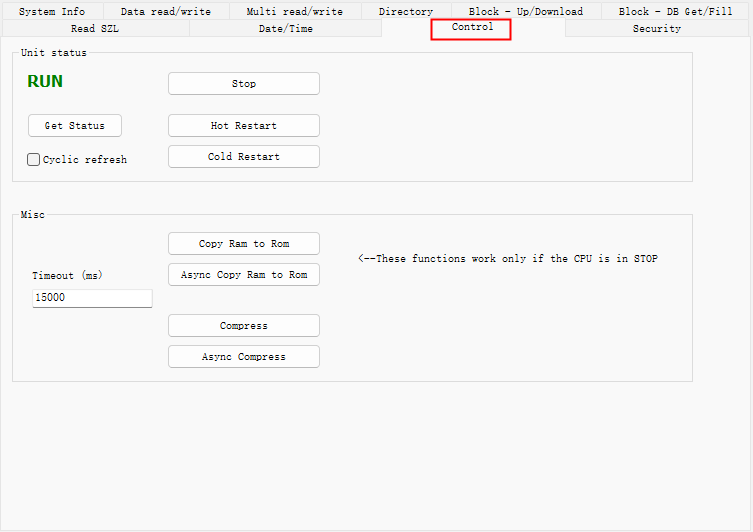
PG/PC date and time:编程电脑上的日期和时间。

CPU Date and Time：CPU的日期和时间。

Get date and time of PG/PC:从编程电脑上获取日期和时间。

Set Date and Time：设置日期时间。

## control



https://blog.csdn.net/weixin\_45263626/article/details/113915337

获取系统的状态

Get status：获取CPU的运行状态。状态位run或者stop.

正常情况下，S7-CPU具有以下操作模式：

●STOP（停止）： CPU 处于“STOP”操作模式时，不执行用户程序。

●STARTUP（启动）：接通 CPU 后，先执行启动程序再执行用户程序。 有“暖启动”、“热启动”和“冷启动”三种启动模式，本文详述。用户可指定S7-CPU上电时的启动类型。

●RUN（运行）：CPU 执行用户程序、更新输入和输出、并处理中断和错误消息。

●HOLD（暂缓）：CPU暂停执行用户程序，适用于设备调试时。

Cyclic refresh:持续刷新获取CPU状态。

Stop:给server端发送停止CPU运行的指令。

Hot Restart：热启动

Cold Restart：冷启动

Copy Ram to Rom: 把闪存的数据拷贝到只读存储器中.同步方式。

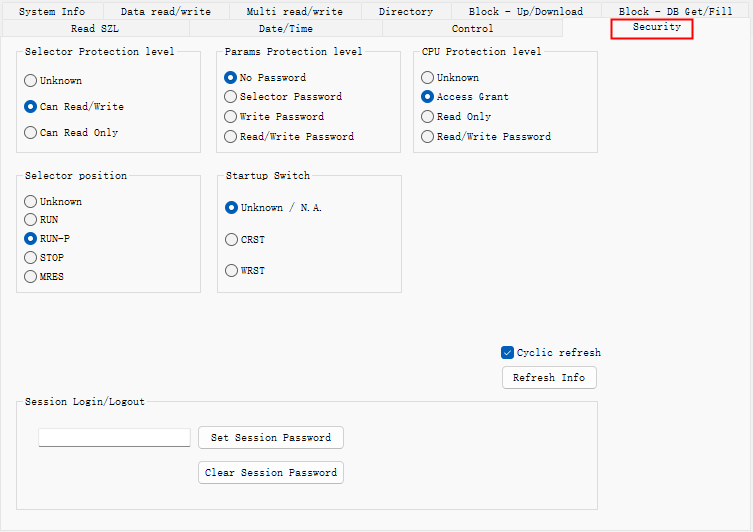
Async Copy Ram to Rom: 把闪存的数据拷贝到只读存储器中.异步方式。

Timeout：超时时间。

Compress:同步进行cpu内存压缩。

Async Compress:异步方式的内存压缩。

## Security



Selector Protestion level:选择防护级别，读写，只读。

Params protection level:参数防护级别，没有密码，选择器密码，写密码，读写密码。

CPU Protection level：CPU防护级别，unknown，Access grant授权访问，Read only只读，read/write password读写密码。