南通地区西门子模块代理

产品名称	南通地区西门子模块代理
公司名称	浔之漫智控技术（上海）有限公司
价格	.00/件
规格参数	
公司地址	上海市松江区广富林路4855弄88号3楼
联系电话	158****1992 158****1992

产品详情

南通地区西门子模块代理

在 PLC 程序内部要对相应的信号进行比较、运算时，常需将该信号转换成实际物理值（对应于传感器的量程）。而经程序运算后得到的结果要先转换成与实际工程量对应的整形数，再经模拟量输出模板转换成电压、电流信号去控制现场执行机构。这样就需要在程序中调用功能块完成量程转换。

如一个压力调节回路中，压力变送器输出4-20mADC信号到SM331模拟量输入模板，SM331模板将该信号转换成0-27648的整形数，然后在程序中要调用FC105将该值转换成0-10.0（MPa）的工程量（实数），经PID运算后得到的结果仍为实数，要用FC106转换为对应阀门开度0-的整形数0-27648后，经SM332模拟量输出模板输出4-20mADC信号到调节阀的执行机构。

1、S7-300/400 PLC模拟量输入/输出模板

1.1 需要使用的模板

使用西门子S7-300/400 PLC进行模拟量输入/输出需要使用的模板：

S7-300系列PLC：SM331
系列模拟量输入模板；SM332系列模拟量输出模板；SM334/335系列模拟量输入/输出模板。

S7-400 系列 PLC：SM431 系列模拟量输入模板；SM432 模拟量输出模板

1.2 涉及的信号类型

电压，电流，温度，电阻。

2、STEP 7中模拟量输入/输出的编程

2.1 FC1

05/FC106库文件位置

在编程界面下，在Program elements中的 Libraries下的Standard Library下的 TI-S7 Converting Blocks中就可以找到，见下图：

注意：请不要使用S5-S7 Converting Blocks下的 FC105,
FC106，该路径下的功能是用于S5输入输出模板的，在S7 输入输出模板上无法使用。

2.2 FC105/FC106功能描述

在编程界面下选中该功能块，按一下计算机键盘上的F1功能键，即可打开关于该功能块的在线帮助，包括该功能块的功能，管脚参数定义、例子程序等。建议用户使用 STEP 7
在线帮助，可以提供全面的编程帮助。

FC105/FC106 功能描述在编程界面下选中该功能块，按一下计算机键盘上的 F1 功能键，即可打开关于该功能块的在线帮助，包括该功能块的功能，管脚参数定义、例子程序等。建议用户使用STEP 7在线帮助，可以提供全面的编程帮助。

2.2.1 FC105 功能描述

SCALE（ FC105 ）功能将一个整形数INTEGER（ IN）转换成上限、下限之间的实际的工程值(LO_LIM and HI_LIM) ，结果写到OUT。公式如下：

OUT = [((FLOAT (IN) – K1)/(K2 – K1)) * (HI_LIM – LO_LIM)] + LO_LIM

常数K1和K2的值取决于输入值（ IN）是双极性BIPOLAR 还是单极性UNIPOLAR 。

双极性 BIPOLAR ：即输入的整形数为 – 27648到27648 ，此时K1 = – 27648.0， K2 =+27648.0

单极性UNIPOLAR ：即输入的整形数为0到27648，此时 K1 = 0.0 ， K2 = +27648.0

如果输入的整形数大于K2 ，输出 (OUT) 限位到HI_LIM,
并返回错误代码。如果输入的整形数小于K1，输出限位到LO_LIM ，并返回错误代码。

反向定标的实现是通过定义LO_LIM > HI_LIM
来实现的。反向定标后的输出值随着输入值的增大而减小。

2.2.2 FC106功能描述

UNSCALE（ FC106 ） 功能将一个实数 REAL (IN) 转换成上限、下限之间的实际的工程值

(LO_LIM and HI_LIM)，数据类型为整形数。结果写到OUT 。公式如下：

OUT = [((IN – LO_LIM)/(HI_LIM – LO_LIM)) * (K2 – K1)] + K1

常数K1 和K2 的值取决于输入值（IN）是双极性BIPOLAR 还是单极性UNIPOLAR 。? 双极性BIPOLAR ：即输出的整形数为 – 27648到27648，此时K1= – 27648.0， K2 =+27648.0

单极性UNIPOLAR ：即输出的整形数为0到27648 ，此时K1 = 0.0 ， K2 = +27648.0

如果输入值在下限LO_LIM 和上限HI_LIM 的范围以外，输出 (OUT)

限位到与其相近的上限或下限值（视其单极性UNIPOLAR 或双极性BIPOLAR 而定），并返回错误代码。

西门子2018年5月15日发布安全公告通知客户，其部分 SIMATIC S7-400 CPU
受严重的拒绝服务（DoS）漏洞影响，该漏洞编号为CVE-2018-4850，CVSS（V3.0）评分7.5分。

SIMATICS7-400

SIMATIC S7-400 是西门子旗下的可编程逻辑控制器（PLC），专门用于工业环境中的过程控制。该产品广泛应用在汽车、机械设备制造、建筑设计、钢铁、发电配电、化工、仓储、食品和制药行业。西门子的PLC产品在我国也有着广泛的应用。

漏洞原理

漏洞原因在于受影响的 CPU 未正确验证 S7 通信数据包，从而允许远程攻击者触发 DoS
条件，可致系统进入并保持 DEFECT 模式，必须手动重启才能恢复。

攻击者成功利用该漏洞的前提是能够将特质的 S7 恶意通信数据包发送至 CPU
的通信接口，包括以太网、PROFIBUS
和多点接口（MPI）。值得注意的是，攻击者无需用户交互或获取特权就能利用该漏洞。

西门子指出，该漏洞可能会造成 CPU 的核心功能出现拒绝服务状态，从而影响系统的可用性。截至安全公告发布之时，西门子称未发现公开已知的利用案例。

影响范围

受影响的产品及版本为：

SIMATIC S7-400 (incl. F) CPU 硬件版本4.0及以下所有版本；

SIMATIC S7-400 (incl. F) CPU硬件版本5.0：所有5.2版本以下的所有固件版本；

SIMATIC S7-400H CPU硬件版本4.5及以下所有版本。

建议受影响的用户分别更新到硬件版本5.0、5.2和6.0。西门子表示，受影响的 SIMATIC S7-400 CPU
硬件版本已停产或已被淘汰。西门子建议客户升级到新版本或采用其提供的应对举措。

鉴于 DoS 漏洞会对工业环境造成严重的风险，建议组织机构尽快更新。

缓解建议

1. SIMATIC S7-400（含F）CPU模块硬件版本在

v4.0及以下版本

2. SIMATIC S7-400（含F）CPU模块硬件版本低于v5.0或

所有固件版本低于v5.2

3. SIMATIC S7-400H CPU模块硬件版本在v4.5及以下版本

补充建议

1.避免将控制设备或操作站暴露在互联网中，应用隔离设备确保外界无法从互联网直接访问工业设备。

2.远程设备与控制系统间部署工业网闸，并确保工业控制系统与办公信息网络完全分离。

3.操作站部署主机防护系统，避免其成为网络攻击的中转跳板。

4.必须进行远程访问时，请使用安全方法，例如使用虚拟专用网络（VPN），并同时确保VPN自身的安全性。