SIEMENS贵州省安顺市西门子（授权）中国总代理-西门子西南地区一级总代理商

产品名称	SIEMENS贵州省安顺市西门子（授权）中国总代理-西门子西南地区一级总代理商
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	变频器:西门子代理商 触摸屏:西门子一级代理 伺服电机:西门子一级总代理
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房（仅限办公）（注册地址）
联系电话	18126392341 15267534595

产品详情

1.研究背景

???PLC???
?????????????????????

2019 BlackHat USA?????????Sara Bitan?????PLC???????S7Comm-Plus??????????????ADLab??????????????S7-1500???????????

2.西门子PLC协议

???PLC??S7-200?S7-300?S7-400?S7-1200??S7-1500??????S7-200/300/400??PLC????????????S7comm?????S7-1200/1500??PLC?????S7Comm-Plus???????

S7Comm-Plus???S7comm??????????????????????????????????TIA?PLC?????????4????

?1?TCP Connection

?2?COTP Connection

?3?S7Comm-Plus Connection????????????

?4?S7Comm-Plus Function????????

?1 S7Comm-Plus??????

????????????????????2????????????

?2 ??????

?1?TIA?PLC??M1?????????

?2?PLC????TIA?????M2?M2??PLC????????ServerSessionChallenge???20????

?3 M2?????

?3?TIA??M2????PLC??M3?M3???SecurityKeyEncryptedKey(?4??????)????Magic???0xfee1dead???180???SecurityKeyEncryptedKey???3????????(?4??????)?

?4 M3?????

?4?PLC??M3??????????????????TIA??M4????

??????????TIA?PLC?????????????????????IntergrityPart?????5???PLC??
????????????IntergrityPart?????????????????

?5 stop??????