

海加SRA纵向加密认证网关Datasheet

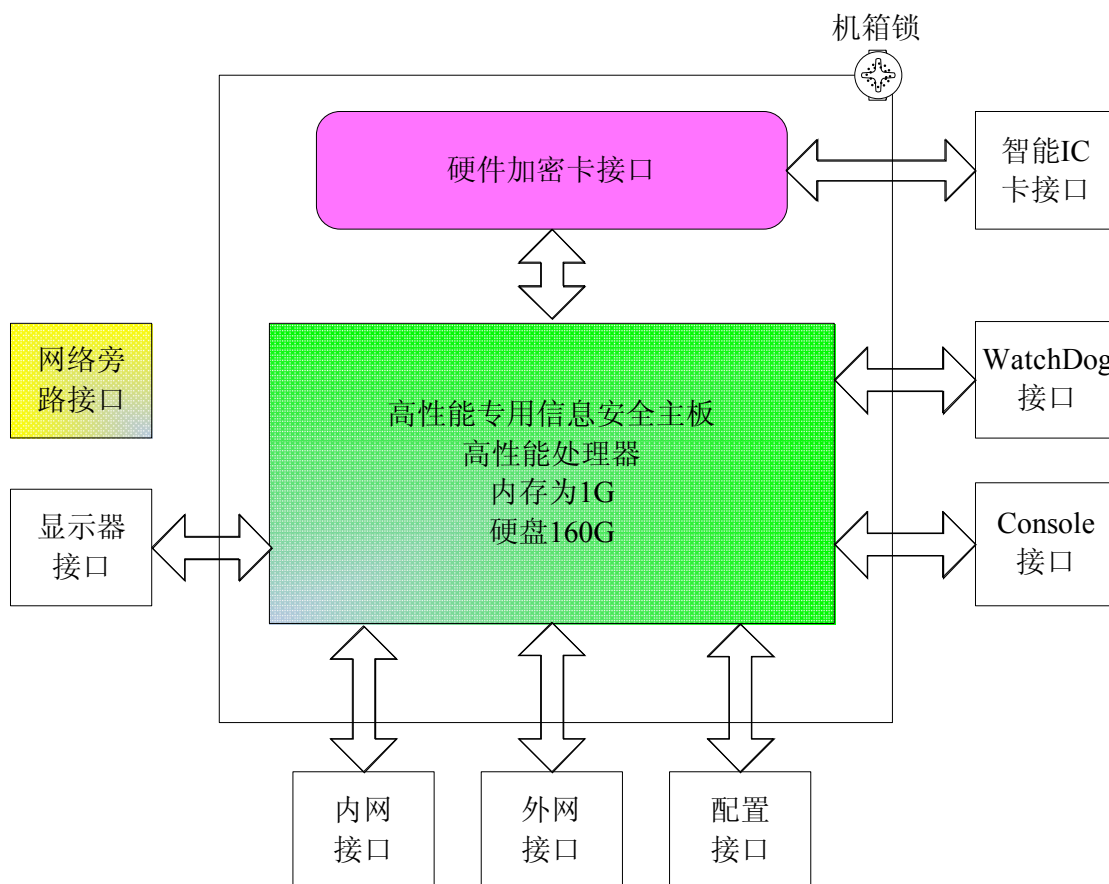
1. 简介

上海海加网络科技有限公司依托自身在网络安全领域的广泛技术积累和应用实践经验，根据电力系统二次安全防护的需要，按照纵向加密认证装置技术要求，自主研发并推出SRA-6.0纵向加密认证网关，用于安全区I/II的广域网边界保护，可为本地安全区I/II提供一个网络屏障，同时为上下级控制系统之间的广域网通信提供认证与加密服务，实现数据传输的机密性、完整性保护。通过长时间的测试，SRA-6.0纵向加密认证网关具有很高的可靠性和稳定性，可以满足用户需要的执行效率。

2. 产品架构

2.1. 硬件体系架构

下图是海加SRA-6.0纵向加密认证网关硬件体系架构：



海加SRA-6.0纵向加密认证网关硬件采用高性能专用信息安全主板，配备有高性能的CPU处理器和1GB的内存，从而保证了系统的高性能和高可靠性。

网关内置集成国家密码办审批的电力系统专用的“SSX06型密码算法芯片”的PCI加密卡，采用电力专有算法，对要求加密的数据进行加解密，保护数据传输过程的安全性和完整性，从硬件级别上保证系统间的数据通讯安全。

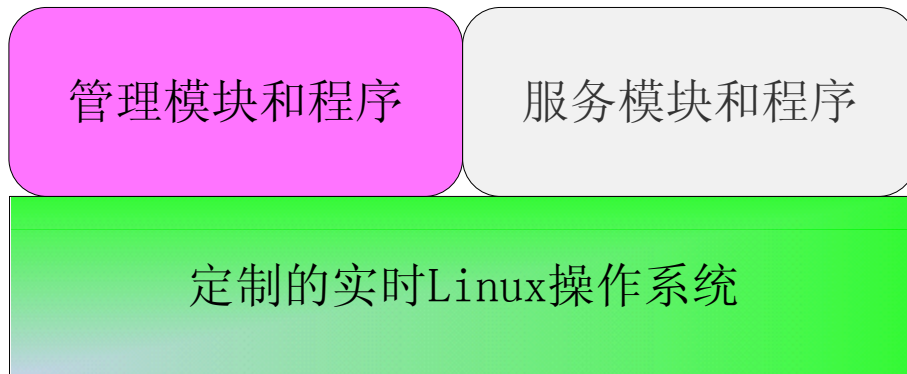
网关采用至少160GB硬盘配置，有能力记录网关产生的海量日志，提高网关的安全性和可用性。网关同时提供四个百兆或者千兆自适应网口的网卡接口和一个百兆配置/心跳网络接口，分别实现不同的功能，保证网络传输的高速度和稳定性，以及保障系统的可管理性。系统内置Watchdog，用以监视系统的运行状态，保证整个硬件电路的安全稳定性和可靠性。

网关采用1U标准机箱，配置双电源，支持上架方式。机箱配有机箱锁，只有通过匹配的专用钥匙，才能开箱，从物理层次上保证设备本身及加密卡的安全。网关机箱外部面板提供状态直观显示装置，直接为用户提供设备状态信息，方便用户随时了解系统运行的状态，及时发现可能遇到的各种问题。

网关配置IC卡接口，随机带有国家电力调度通信中心指定的IC卡生产厂家的IC卡，设备管理人员采用配置的安全介质IC卡实现设备登录，实现人、机、卡三方认证。

2.2. 软件体系架构

下图是海加SRA-6.0纵向加密认证网关软件体系架构：



海加SRA-6.0纵向加密认证网关系统采用经过内核裁减和客户化定制的实时Linux操作系统，所有源码完全受控，保证系统的安全性。通过裁减和客户化定制的实时Linux操作系统，优化了内核和底层服务，保证了系统的性能。

海加SRA-6.0纵向加密认证网关系统提供了良好的管理模块和程序，实现了友善的用户接口和图形化的管理界面。管理员通过图形化的配置界面进行系统维护和设置，不仅简单易用，而且有效防止由于配置复杂性造成安全隐患。系统配置信息包括对装置的设备基本信息的配置和管理、安全性配置和管理、双机热备功能的配置和管理、日志功能的配置和管理、工作模式的配置和管理。

海加SRA-6.0纵向加密认证网关提供了性能优秀及运行稳定和可靠的服务模块和程序，为系统提供各种应用服务，实现了纵向加密认证网关各种功能。

3. 产品功能指标/性能指标

3.1. 功能指标

- 1) 采用国家密码办审批的电力系统专用的“SSX06型密码算法芯片”的PCI加密卡，使用固化在硬件芯片中电力专用加密算法SSX-06对数据进行加密/解密，提供了算法强度及物理安全性；
- 2) 支持标准的加密和验证算法；
- 3) 支持基于数字证书的身份认证，以及支持基于数字证书结合设备MAC和IP地址等设备硬件参数的多因子认证方式；
- 4) 支持X.509数字证书标准，实现与已经投入运行的各个网省电力调度中心的“电力调度证书服务系统”无缝配合，也支持第三方CA中心发放的数字证书；
- 5) 支持详细日志审计功能，加强设备和网络的安全性；
- 6) 具有基于IP/TCP协议和应用端口号的综合报文过滤与访问控制功能；
- 7) 支持透明连接和借用地址模式，不占用网络IP地址资源；
- 8) 纵向加密认证网关接入网络时，无需对网络的架构及配置做任何改动；
- 9) 采用专用的实时安全操作系统内核，提供高安全性和高性能的系统；
- 10) 支持设备系统及软件升级；
- 11) 支持双机热备功能，在其中一台设备出现故障时，自动切换至备机；
- 12) 设备本身具有防御常见网络攻击的功能，包括ARP Attack、Ping Attack、Ping of Death Attack、Smurf Attack、Unreachable Host Attack、Land Attack、Teardrop Attack、Syn Attack等；
- 13) 具有严格的设备管理功能，在对纵向加密认证网关进行管理时，需要“人机卡”的三方认证过程。管理人员必须持有可用于管理的智能IC卡，必须持有可登陆管理的密码，再进行过“人机卡”的三方认证才能登陆纵向加密认证网关模块，进行有效的管理配置；
- 14) 支持纵向加密认证网关能被其对应的管理中心远程监控和管理，支持装置重启、隧道初始化和策略添加等操作，具备安全的可管理性；
- 15) 专用纵向加密认证网关能够实现“电力二次系统安全防护总体方案”中要求的安全防护功能，满足二次系统安全防护要求；
- 16) 海加SRA-6.0纵向加密认证网关在和不同厂家之间的纵向加密认证网关和装置已经能互连互通；
- 17) 已经通过电力系统指定检测机构的电磁兼容性检测。

3.2. 性能指标

SRA-6.0电力专用纵向加密认证网关（增强型）：

- 1) 网络接口：4个千兆网卡接口（其中eth0与eth1、eth2和eth3接口支持自动旁路），1个百兆配置/心跳接口
- 2) 最大并发加密隧道数：2048条
- 3) 1000M LAN环境下，加密隧道建立延迟<1s
- 4) 明文数据包吞吐量：340Mbps（200条安全策略，1024报文长度）
- 5) 密文数据包吞吐量：80Mbps（200条安全策略，1024报文长度）
- 6) 数据包转发延迟：<1ms（50%密文数据包吞吐量）
- 7) 平均无故障时间(MTBF)>100000小时(100%负荷)
- 8) 满负荷数据包丢弃率：0

SRA-6.0电力专用纵向加密认证网关（普通型）：

- 1) 网络接口：4个百兆网卡接口（其中eth0与eth1、eth2和eth3接口支持自动旁路），1个百兆配置/心跳接口
- 2) 最大并发加密隧道数：1024条
- 3) 100M LAN环境下，加密隧道建立延迟<1s
- 4) 明文数据包吞吐量：95Mbps（200条安全策略，1024报文长度）
- 5) 密文数据包吞吐量：25Mbps（200条安全策略，1024报文长度）
- 6) 数据包转发延迟：<1ms（50%密文数据包吞吐量）

- 7) 平均无故障时间(MTBF)>60000小时(100%负荷)
- 8) 满负荷数据包丢弃率: 0

4. 产品优势分析

1) 实现了安全方便的加密认证以及互联互通

海加网络SRA产品支持透明模式、路由模式、防火墙模式、旁路模式四种模式,充分考虑了该装置在部署过程中的不同网络情况的要求,通过认证授权以后,在海加设备之间建立一条安全通道,就可以透明地访问内部的B/S应用和C/S应用。

系统支持完备的安全事件告警机制,当发生非法入侵、装置异常、通信中断或丢失应用数据时,可通过加密认证网关专用的告警接口或网络输出报警信息,日志格式遵循Syslog标准,方便用户统一集中管理。

2) 实现了增强的设备认证和权限管理功能

系统采用数字证书的认证方式认证用户,用户在使用SRA设备时,需要插入IC卡,输入口令才能通过认证,从而大大增强了设备安全性。

集成基于应用的内容过滤和硬件防火墙技术。系统支持对数据报文的源、目的地址、协议域及相应的源、目的端口、标志域等属性进行组合形成不同的包过滤规则,控制进出的信息流向和信息包。

同时系统管理员可以指定访问控制策略,通过给不同的设备以不同的应用系统访问权限,从而控制设备对应用的访问。

3) 实现了专有的数据传输的安全

SRA-6.0系列加密认证网关采用国家密码管理局授权批准的电力专用密码算法自主研发开发高性能电力专用硬件密码单元,该密码单元支持身份鉴别,信息加密,数字签名和密钥生成与保护。

方案通过采用海加网络专有的动态密钥更新技术保证了数据的安全性,即在数据传输过程中,密钥和算法可以根据管理员制定的策略,在一定时间或者一定的数据量之后重新生成,从而使密钥和算法不断动态变化,非法用户即使嗅探了加密数据也只能破解其中一段时间的数据,从而更大程度地提高了数据传输的安全性。

4) 支持应用协议选择性加密

SRA-6.0系列加密认证网关支持对多种电力专用协议IEC104、DL476-92等进行安全解析,对不同功能的报文采取不同的应用策略:对监视和查询报文分别以明通方式通信,而对控制报文以及控制报文的参数进行加密,保证重要实时命令的机密性和完整性。

5) 提供简单高效的维护和管理方式

方案采用安全方便Web界面方式,管理员只要通过海加SRA设备的SRA Manager管理模块就可以管理设备的各项功能,集中实现对网络的安全接入进行加密认证控制。

6) 实现了高可靠运行保障

SRA-6.0系列加密认证网关采用了多种高可靠性保障技术包括的双机热备和主备自动切换技术、硬件自动旁路技术、双电源冗余技术等,使得系统达到99.99%以上的不间断运行水平。从所保护的子网中的通信机到本地接入路由器之间的路径上,任何环节,包括设备或链路出现故障,加密装置都能正确识别,配合实现路径切换。

7) 本地化快速支持响应

针对电力纵向加密认证网关的部署与维护特点，我们在华北电网成立了专门的本地化维护队伍，充分保证了服务的及时性和高质量。我们提供7×24小时技术服务支持，在接到用户的故障申告后，我方将在10分钟内给予响应，自接到用户故障申告4小时内无法远程解决该故障，我方立即派遣技术人员到达现场处理故障，保证在接到申告的24小时内恢复设备运行。

5. 产品安全性分析

海加SRA-6.0电力专用纵向加密认证网关具有多方面的安全性，主要包括下面几个方面：

5.1. 算法及密码的安全性

- 国密办指定的专用算法

SRA-6.0电力专用纵向加密认证网关的核心技术是加密算法，它决定着装置的加密强度，抗攻击能力。SRA-6.0电力专用纵向加密认证网关采用国密办专为电力系统设计的加密算法，算法相关信息高度机密，不向任何单位公开，通过将算法封装在加密算法芯片中提供给用户，确保算法的安全可靠，从根本上保证了装置的加密强度。

- 电力专有的高速数据加密卡

SRA-6.0电力专用纵向加密认证网关的密钥生成、数据加密都是由电力专用高速数据加密卡完成，该加密卡为国调、国密办共同指定的厂家研制开发，对称加密基于专用加密算法芯片，非对称加密遵循国际标准，采用硬件噪声源芯片生成高度随机性的随机数，加密强度高，加密速度快，抗攻击能力强。同时加密卡上的关键密钥数据采用保护算法进行加密，物理上保证密钥不出卡，充分保证密钥的安全性。

- 专有的加密通信协议

SRA-6.0电力专用纵向加密认证网关采用电力系统专有的加密通信协议，该协议为国调专家和国密办联合设计，结合了电力系统的应用及管理特点，提高了效率，保证通信协议安全可靠。

5.2. 传输层的安全性

- 数据包的综合过滤技术

SRA-6.0电力专用纵向加密认证网关作为代理从外网的网络访问包中抽取数据然后通过内网接口转入内网，完成数据中转。在中转过程中，电力专用纵向加密认证网关首先对抽取的数据报文的IP地址、端口号实施综合过滤控制，根据需要进行可信的两个主机间的工作密钥协商及工作密钥交换，在两个主机间建立起一个安全可靠的会话，然后对可以通过上述过滤的报文根据规则确定是禁止通过、直接传输还是加密传输，对需要加密的进行加密，然后对允许通过的报文进行签名后通过内网接口转入内网。有了上述的约束条件，可以保证数据在非安全的通道上安全可靠地传输。

- 状态检测技术

基于电力专用纵向加密认证网关所维护的状态表的内容转发或拒绝数据包的传送，比普通的包过滤有着更好的网络性能和安全性。普通包过滤使用的过滤规则是静态的。而采用状态检测技术的电力专用纵向加密认证网关在运行过程中一直维护着一张状态表，这张表记录了从受保护网络发出的数据包的状态信息，然后电力专用纵向加密认证网关根据状态表内容对返回受保护网络

的数据包的状态信息，然后电力专用纵向加密认证网关根据状态表内容对返回受保护网络的数据包进行分析判断，这样，只有响应受保护网络请求的数据包才被放行。

5.3. 系统层的安全性

- 安全可靠的操作系统

SRA-6.0采用Linux操作系统作为支撑平台，不存在版权问题，并对linux操作系统内核做了大量的裁减和安全性改造，包括关闭系统多余的服务、修改内核核心代码、安装专用密码模块等。

- 高强度的抗攻击能力

通过特殊的硬件结构和加固的操作系统的内核以及电力专用纵向加密认证网关本身没有IP地址，使得电力专用纵向加密认证网关本身的抗攻击能力的强度极高。黑客对设备的攻击无从下手。

- 专有的性能优化技术

电力专用纵向加密认证网关性能的优劣影响到用户的使用也同时影响了系统的安全和稳定性，我们采用了多种性能优化技术，通过采用多加密芯片协同运算、大容量缓存技术等方式，大大改善了电力专用纵向加密认证网关的性能。

5.4. 管理层的安全性

- 实时的状态监视和告警功能

可以通过管理工具监视当前设备中存在的安全通道的状态信息包括：流过的包数量、超时次数、出错重协商次数、密钥协商状态等信息。系统支持完备的安全事件告警机制，当发生非法入侵、装置异常、通信中断或丢失应用数据时，可通过加密认证网关专用的告警接口或网络输出报警信息，也可以实现定制的短信或者邮件输出告警信息。

- 安全便捷的配置管理

网关设备支持通过安全WEB方式实现配置管理，管理员采用国家电力调度通信中心指定的IC卡生产厂家的IC卡，实现“人机卡三方认证”，从而保证安全登录设备来进行配置管理，包括隧道重置、设备重置、添加删除策略等工作，便于用户根据实际网络情况，动态调整设备运行方式、规则配置等信息，并可以进行实时切断运行隧道。

6. 产品电气特性

装置外形：

- 1) 标准1U
- 2) 尺寸(长×宽×高):507×440×44.4毫米
- 3) 重量：12千克

外设接口：1个终端接口(RS232)+1个智能IC卡接口

电源接口：双电源接口（支持热插拔）

电源指标:

- 1) 电压: 220V
- 2) 允许偏差: $-20\% \sim +15\%$ 。
- 3) 纹波系数: 不大于3%。
- 4) 额定频率: 50Hz。
- 5) 平均无故障时间(MTBF) >100000 小时(100%负荷)

工作环境:

- 1) 工作温度: $-10^{\circ} \sim -55^{\circ}$
- 2) 工作湿度: 5~95%, 非冷凝
- 3) 大气压力: 70kPa~106kPa。

抗干扰性:

1) 辐射电磁场抗扰度 :能承受GB/T15153.1中规定的严酷等级为3级(6V/m)的辐射电磁场干扰实验,性能符合GB/T17626.1总则9中“a)”规定的要求。

2) 快速瞬变抗扰度:电源和信号都能承受GB/T15153.1中规定的严酷等级为3级的快速瞬变干扰实验,性能符合GB/T17626.1总则9中“a)”规定的要求。

3) 脉冲群抗扰度装置:能承受GB/T15153.1中规定的严酷等级为3级的1MHz和100kHz的脉冲群干扰实验,性能符合GB/T17626.1总则9中“a)”规定的要求。

4) 静电放电抗扰度:能承受GB/T15153.1中规定的严酷等级为3级的静电放电干扰实验,性能符合GB/T17626.1总则9中“a)”规定的要求。

5) 浪涌(冲击)抗扰度:能承受GB/T15153.1中规定的严酷等级为3级的浪涌(冲击)干扰实验,符合GB/T17626.1总则9中“a)”规定的要求。

6) 机械振动装置:能承受GB/T11287-2000中3.2中规定的严酷等级为1级振动实验,性能符合该标准5中规定的要求。

7) 工频磁场装置:能承受GB/T15153.1中规定的严酷等级为4级的工频磁场干扰实验,性能符合GB/T17626.1总则9中“a)”规定的要求。

8) 介质强度装置:能承受GB/T15153.1中规定的严酷等级为3级的绝缘强度(不小于5M Ω)和耐压强度(电源输入回路不小于1500V)实验,性能符合GB/T17626.1总则9中“a)”规定的要求。

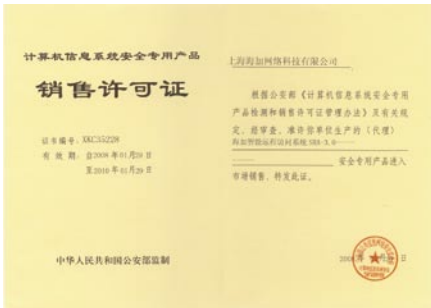
9) 稳定性装置:能承受GB/T13729中3.9规定的稳定性实验。

10) 其他参考标准

- IEC-1000-4-2 (ESD)
- IEC-1000-4-3 (辐射敏感性)
- IEC-1000-4-4 (电快速瞬变)

7. 产品资质

1) 海加SRA公安部销售许可证



2) 商用密码产品生产定点单位



3) 商用密码产品销售许可证



4) 发明专利证书

