

低压用电信息采集安全研究与系统解决方案

用电信息采集系统需要承载实时、准实时业务及管理信息业务，系统中数据采集、指令发送与控制过程中所使用的电力用户信息、电量信息及用电类型信息等是电力企业的重要机密，其非法使用和丢失将带造成严重后果。传统的数据通信安全防护策略和安全防护技术已经不能满足智能电网用电信息采集系统数据通信安全的需求。对低压用电信息采集系统的安全现状进行了分析，并根据分析结果，分别从系统自身通信安全和运维系统安全出发，提出了对应的解决方案。

齐火箭 徐海宾 王嘉宏 杨红欣/国网冀北电力有限公司张家口供电公司



齐火箭/高级工程师

低压用电信息采集系统目前的安全问题主要存在两个方面。一是自身的通信安全；二是负责运维工作的运维系统安全。

目前业界的宽带PLC集抄产品在低压配电台区中节点间的通信数据普遍采用明文传输的方式，这将给通信双方都带来潜在的安全隐患。身份合法性：数据明文传输，无法令头端和终端相互认证对方身份的合法性，存在仿造并替换某一台区内PLC抄表模块或电表来实现恶意目的的巨大风险。数据保密性：数据明文传输，导致通信双方无法抵抗重放、同形等恶意攻击方式，对载波抄表、费控的数据安全带来了巨大威胁。数据完整性：数据明文传输，第三方攻击者可以很容易地删减、修改通信报文的内容，从而扰乱通信双方的正常业务功能。

在低压用电信息采集系统中，运维工作按照以下方式进行：运维工作人员持有一个安装有运维软件的终端设备，该终端设备可能是PAD、PC或其他形

式。运维终端通过Wi-Fi或网线连接抄控宝，再进一步通过PLC连接到集中器或者直接通过网口或串口连接到集中器，如图1所示。当运维终端连接上集中器后，便可以开始一系列的运维工作。

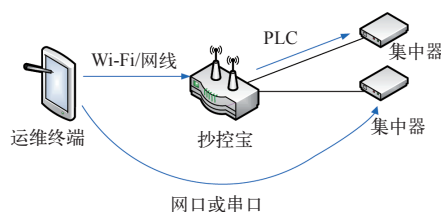


图1 运维终端连接集中器进行运维工作

整个运维过程存在如下安全隐患：

身份合法性：任何人都能通过运维终端连接到集中器进行调试，若无关人员连接集中器，便可以查看台区信息，设置参数，造成信息泄露，甚至破坏台区环境；权限等级划分：连接集中器后的操作未作限制，导致任何操作人员都可以设置网络参数，查看集中器日志信息等，运维人员应当被赋予不同权限，仅允许进行权限允许的操作；日志记录与责任跟踪：运维人员对台区进行的操作未被记录，尤其是一些对台区安全可能产生影响的敏感操作应该被记录，可用于在问题发生时进行责任跟踪等。

智能电网低压用电信息采集系统的保密通信

随着智能电网业务的普及，低压用电信息采集系统所面临的各节点间身份合法性鉴权、节点间通信数据保密性以及数据完整性问题亟待解决。提出一种智能电网低压用电信息采集系统的保密通信机制，针对系统中各节点间的身份

关键词/Keywords

用电信息采集系统 ·
信息安全 ·
数据传输安全 ·
访问控制 ·

份进行鉴权从而确认各节点间的身份合法性；鉴权成功后自动进行后续通信的加密算法及密钥协商，保障系统正常业务工作时的数据保密性；在入网和正常业务通信时分别采用数字签名和解密后CRC判决，从而保障通信数据的完整性。

1. 系统中各通信节点间的鉴权机制

该系统中的节点间合法身份鉴权机制采用非对称加密算法RSA作为基础。由模块厂家建立接入网络的CA证书服务器，分别生成密钥对：针对STA的公钥（PubSTA）、私钥（PriSTA）及CCO的公钥（PubCCO）、私钥（PriCCO）。根据RSA非对称加密算法的原理生成密钥对。用于身份合法性鉴权的RSA的密钥对（公钥、私钥）在工厂模块加工的出厂工装检测阶段进行分发。密钥分发流程如图2所示。

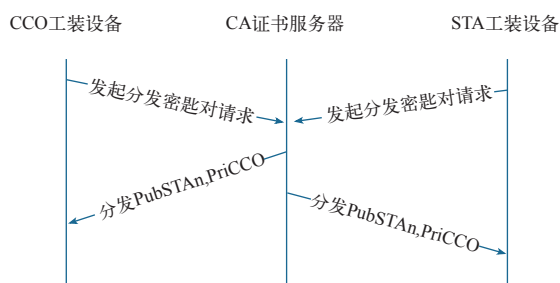


图2 密钥分发流程

在CCO/STA的密钥对完成分发后，CCO/STA模块将各自收到的两个密钥中的私钥写入芯片的eFuse ROM中，该ROM为一次性熔断式ROM，且限制芯片外部读取；公钥则存入片外的FLASH中即可。密码的存储量对于每个STA模块的情况，只需存储PubCCO和一个PriSTA，数量很少；对于CCO的情况，则除了PriCCO存入eFuse ROM中之外，还需存储 n 个STA的PubSTA，其中 n 的个数为一个台区的终端个数。由于这 n 个STA的公钥存储于CCO的FLASH中，因而对存储量要求不高。

由于低压配电台区的头端CCO与终端STA组网后形成的网络为树状结构，每个STA在入网时都需要向CCO发起入网请求。定义入网流程如图3所示。

2. 系统各节点间通信的数据保密性的保障

当STA与CCO相互完成了身份合法性鉴权后，

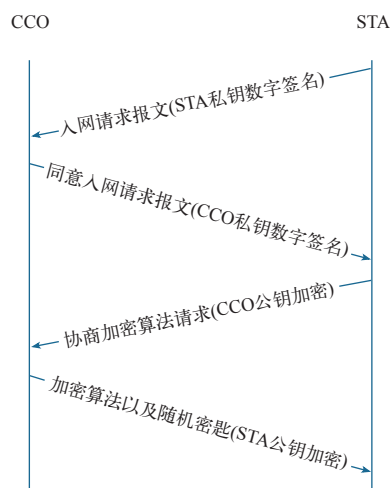


图3 集抄模块身份合法性鉴权流程

由STA发出经过CCO公钥RSA加密的通信加密算法和密钥协商请求，该请求中还包括了STA所支持的加密算法；CCO收到该报文后通过CCO私钥RSA解密，从而开始启动后续业务通信所用的加密算法和密钥协商动作。

(1) 保密通信加密算法协商

CCO通过统计所有STA所支持的加密算法的并集 U ，从而由 U 中按照随机的方式选定一个加密算法用于后续的业务功能时的保密通信。加密算法集合包括AES加密、3-DES加密和DES加密。

(2) 加密密钥的协商

CCO根据STA的可用加密算法的并集 U ，随机的选择1个加密算法，则对应的密钥长度是已知的，再根据该密钥长度，随机生成1个密钥，通过加密算法和密钥协商应答报文的原始数据。该数据经过STA RSA算法的私钥加密，应答给对应STA即完成了加密密钥和加密算法协商动作。对于该业务通信所采用的加密算法和密钥，全部写入芯片的只写寄存器中，无法再从芯片中读出，避免泄密的风险。

(3) 密钥的更替

为了更好地保证数据通信的保密性，因而，CCO在每隔24 h后，自动重新从STA支持的加密算法的并集 U 中随机选择一种加密算法，并对应的生成一个密钥，形成密钥更替通知报文的原始数据，再使用原有的对称加密算法和密钥经过加

密，分发给各个STA，并即刻生效。

对于由于信道异常未收到密钥更替报文的STA站点，在信道恢复正常后则使用原有加密算法和密钥无法进行正常业务通信，最终会离网，并重新进行入网请求的身份合法性鉴权流程，从而重新获得业务通信的加密算法及密钥，恢复业务通信功能。

3. 系统通信数据完整性的保障

从上文的身份合法性鉴权以及数据保密性保障两个章节可以得知，在身份合法性鉴权阶段，CCO和STA发出的报文都分别对报文原始数据进行了MD5的数字摘要，并使用自身的私钥对该摘要进行了数字签名，从而令接收方确认发送方的身份是合法的。由于接收方也会对接收到的原始数据进行数字摘要，并与解签名的原始数字摘要进行比对，因而，在此处可以保障身份合法性鉴权阶段的数据完整性。

在业务数据保密通信阶段，使用对称加密算法和对应密钥解密后的报文会经过CRC校验，从而确认数据的完整性，也可确认该阶段的数据完整性获得了保障。

基于云端的运维系统安全防护

针对上文提出的运维系统存在的安全隐患，提出一个基于云端的低压集采电力运维系统解决方案。它由3个主要部分构成，即运维终端设备、集中器和云端。它们之间的关系如图4所示。

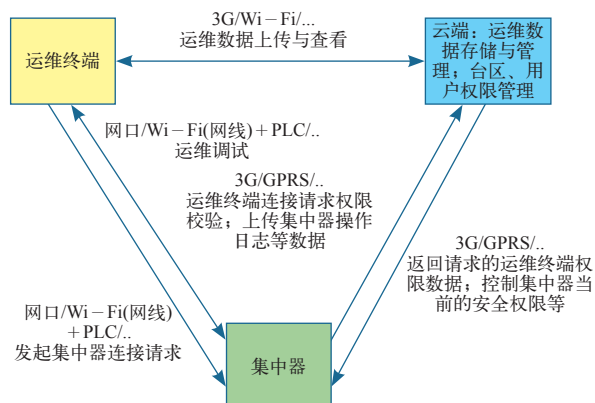


图4 基于云端的低压集采电力运维系统

从图4中可以看到，云端是存储用户数据和台区信息的后台服务器。其校验用户是否具有连接该集中器的权限，并将校验结果返回给集中器，集中器再根据该结果决定是否允许用户连接。当用户连接集中器成功后，方能进行运维调试工作。

在整个运维系统中，云端发挥着重大作用。它除了为用户连接集中器过程中进行权限鉴定外，还能够存储和分析用户的运维数据，上传用户操作日志，甚至能够远程设置各集中器的一些安全权限等。在这个系统中，用户只能在通过云端的权限认证后，方能连接集中器进行运维工作，很大程度上保护了台区的安全。除非有外部原因导致账号泄露，否则无关人员是无法连接集中器进行查看和设置操作的。即使有这种情况发生，通过云端存储的集中器操作日志也能够看到相关历史操作信息。

下面从运维终端连接集中器鉴权实现、云端集中器安全等级设置与危险监听、运维过程操作日志存储与分析、数据的加密传输与存储4个方面详细描述该运维系统的实现。

1. 运维终端连接集中器鉴权实现

在实现运维终端连接集中器鉴权以前，需要做一些准备工作，包括云端功能模块管理与安全防护、用户账户的注册与认证、用户权限的管理等。

(1) 云端功能模块管理与安全防护

集中器通过GPRS等网络向主站服务器上报告采集数据。因此，运维系统云端服务器的部署可参照采集系统主站服务器的部署方式。甚至如果条件允许，云端服务完全可以作为主站系统服务器上的一个子功能模块运行，专门提供运维服务，管理运维数据。运维服务器的部署完全不影响原集中器与主站之间的数据通信。

本方案重点关注的是云端的功能模块管理与安全防护。要实现运维终端连接集中器鉴权，云端必须包含以下功能：用户管理、集中器管理、权限管理。此外，为了实现日志存储和运维数据存储，其还应当包含日志管理和运维数据管理。如图5所示。

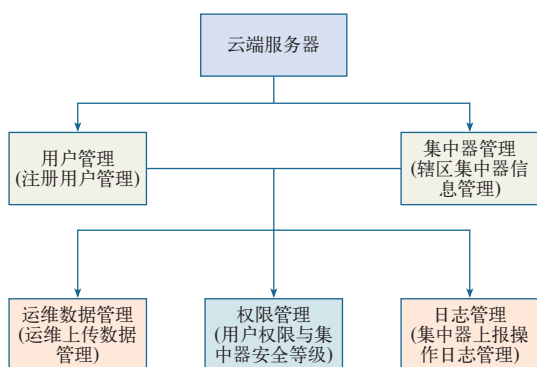


图5 云端服务器功能模块划分

云端需要足够安全。一旦云端安全系数不够，信息泄露，整个运维系统的安全也将受到威胁。

(2) 用户注册与实名认证

用户在连接集中器时，需要输入账号和密码。该账号需要用户在云端提供的申请页面进行申请，并且在管理员审批通过之后方能使用。用户申请账号必须进行实名。此外，用户可以同时进行集中器权限的申请，集中器权限包含了用户可以连接的集中器及在该集中器的操作权限。

(3) 用户权限管理与集中器操作权限控制

尽管允许用户连接到集中器，但并非所有用户都能进行相同的操作。例如，有的用户仅能查看台区信息，不能进行修改操作；有的用户可以对台区环境进行修改设置，但不能查看集中器内的日志信息等。用户对集中器的操作权限可以在云端服务器提供的页面进行申请，或由管理员下发。用户所具有的权限示例如表1所示。

表1 用户操作权限代码示例

用户操作权限代码	说明
AU00	在该集中器上本账号冻结，没有连接权限
AU01	用户具有最高权限，可以进行任何操作
AU02	用户仅具有查看台区信息权限，无法进行设置操作
AU03	用户具有查看台区信息和设置台区参数的权限，但无法查看集中器内操作日志
...	更多的权限设置

(4) 用户连接集中器流程

当用户注册并具有集中器相关权限后，便可以开始使用终端设备连接集中器进行运维调试

了。用户连接集中器流程图和时序图分别如图6、图7所示。

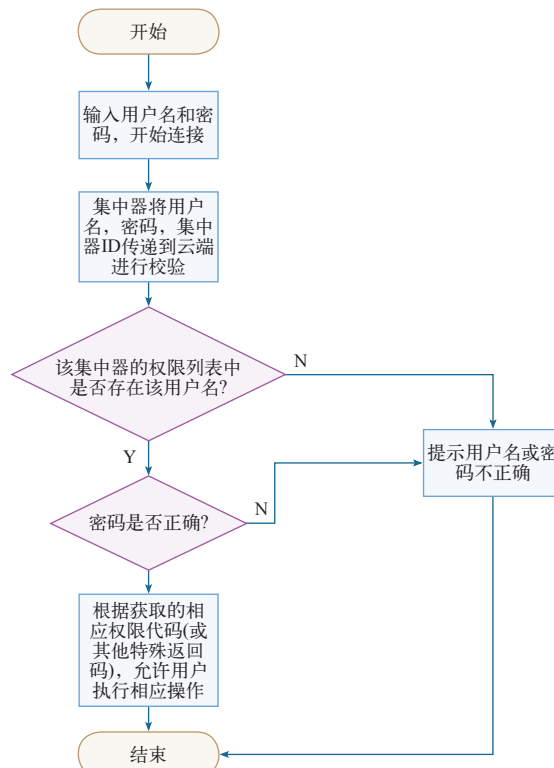


图6 运维终端连接集中器流程图

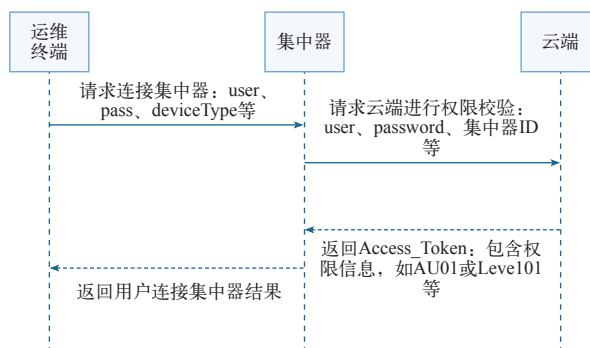


图7 运维终端连接集中器时序图

2. 云端集中器安全等级设置与危险监听

既然云端可以同集中器通信，在必要时刻，它也可以对集中器进行一些特殊操作，如进行安全等级设置与危险监听。该功能尤其在用户账号发生泄露等可能危及台区信息安全的情况下非常有效。

集中器安全等级设置。在云端后台集中器管理模块，可以对集中器设置特殊安全等级，默认为无任何设置。比如让其不能被运维终端连接，

不能进行设置操作，不能查看日志信息等。

危险监听是一种事件上报机制，其使用频率较低，但在保护运维系统安全中也发挥着其独特的作用。其用在一些特殊情形下，例如当某台区某段时间总是出现异常设置操作，但账号所有人并未去该台区进行过调试，且未发现集中器自身存在异常时，就可以启用危险监听功能。

3. 运维过程操作日志存储与分析

云端的日志管理模块负责存储集中器在运维过程中主动上报的操作日志信息，这些日志信息可能是一些设置或修改操作，并不是用户的所有操作都会记录到日志，具体哪些操作会被记录可以根据需求制定。

日志管理模块下日志信息分文件夹存放，每个文件夹对应一个集中器，每个集中器下按日期归档了每天上报的运维日志信息。每条日志信息记录的信息包括：操作类型—操作人员—操作时间—操作设备信息。

4. 数据的加密传输与存储

由于解决方案的各个关键点都存在集中器与云端之间的数据传输。如果不采取任何保护措施，网络数据在传输过程中可能被截取、篡改，进一步造成信息泄露，危及台区安全。因此，保证数据传输的机密性、完整性、不可抵赖性、访问控制性、身份可靠性等显得异常重要。

目前成熟的网络传输数据加密技术分为两个系统：对称加密和非对称加密。对称加密中具有代表性的是DES算法和AES算法，由于DES密钥长度较短，已经不适合当今网络对数据加密安全性的要求，逐渐被AES取代；非对称加密中最著名的是RSA算法。

考虑到在集中器与云端的网络传输中，AES和RSA各有优缺点，比如AES的加解密速度明显优于RSA，而RSA的密钥管理却又优于AES。所以，可以根据实际需求，结合AES和RSA，实现更符合业务逻辑的数据传输加解密算法。一种AES和RSA相结合的加解密方案示例如图8所示。

如图8所示，该方案加解密流程如下：接收方创建RSA密钥对，将RSA公钥发送到发送方，同时

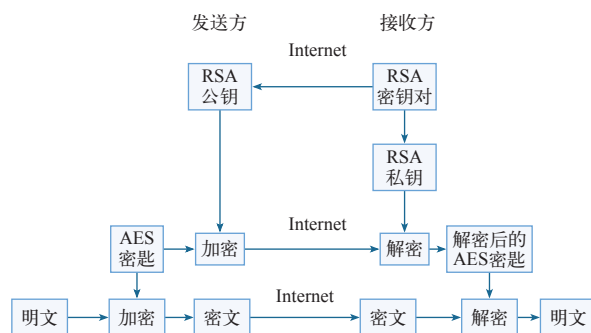


图8 AES和RSA相结合方案示例

保存RSA私钥。发送方创建AES密钥，并用该密钥加密明文，同时用RSA公钥加密AES密钥，最后把加密后的AES密钥和密文一起发送到接收方。接收方调用保存的RSA私钥对加密后的AES密钥进行解密，得到AES密钥，再用该AES密钥解密密文得到明文。

除了数据的传输需要进行加解密处理外，云端服务器的敏感数据（如用户信息、集中器信息等）的存储也有必要进行相应的加密处理，确保存储的数据不会轻易泄露。同时有必要基于云端建立灾备系统，防止意外情况造成数据的丢失。

5. 可行性分析及基于License的过渡方案

该基于云端的运维系统和目前的运维方式相比，确实在安全性上有了很大的提升，并且其数据存储、分析能力也是目前的运维系统所不具备的。要实现该方案需要满足两个条件：有强大的云端（后台服务器）作支撑；在现有集中器的基础上，建立起集中器与云端运维服务器的通信机制。虽然要实现这两点，技术上是不存在壁垒的，但由于涉及面较广，且需要到对传统集中器进行部分改造（和运维云端交互），需要投入较大精力去完成。

鉴于目前运维系统的安全问题确实迫在眉睫，在此提出一种无须云端服务参与的解决方案：基于License的安全运维方案。虽然该方案不如基于云端的安全方案功能强大，但其实现简单，且能在一定程度上保护台区的信息安全，可以作为一个从当前到实现基于云端的运维系统之间的一个过渡方案。该方案的实现要点主要有以

下几项。

1) 建立运维软件的License授权机制与权限划分机制：只有被与设备对应的License授权的设备方能运行运维软件。该机制在于将运维软件绑定到指定终端设备上运行，且不同的License权限可以使终端用户具有不同的操作权限，设备标识符可以是其MAC地址等唯一标识。虽然定制运维终端设备也能够将运维软件绑定到指定终端运行，但其成本较高，且软件分发不够灵活。

2) 集中器连接密码设置与修改：可以为集中器设置连接密码，密码仅告知相关运维人员，且高权限的终端用户可以对其进行修改。一定程度上加强了连接安全性。

3) 集中器操作日志记录：可以将用户操作产生的日志信息存储在集中器内，虽然由于集中器空间有限，日志信息的存储也将是有限的。

4) 运维软件的加固与防破解机制：为了防止运维软件被破解，从而泄露license授权机制等重要信息，运维软件的加固保护显得尤其重要。例如，软件的加壳与代码混淆等技术都应该被应用到运维软件中。

需要说明的是，基于云端的运维平台毕竟是当前的一个发展趋势，其带来的运维效率的提高与安全性的保障不是当前运维方式及上述过渡方案所能比拟的。甚至将来大多数的台区运维操作都可以在云端进行。

结束语

针对低压用电信息采集系统中的信息安全

现状，提出了一个系统的安全解决方案。该解决方案对系统自身的通信机制进行优化，提出了保密通信机制，解决了电力线上数据明文传输可能造成数据泄露等问题；同时从运维系统的安全出发，提出了基于云端的运维系统安全防护方案，并对其可行性进行了分析，解决了运维过程中的信息安全和台区安全问题。

参考文献

- [1] 陈玉慧, 蒋元晨. 打造电网特色的信息运维综合管理系统 [J]. 电力信息化, 2011, 9 (2) : 165-169.
- [2] 王喜贺. 电力调度自动化网络安全与实现 [D]. 济南: 山东大学, 2009.
- [3] 李劲. 遵循等级化保护的电力调度数据网安全防护 [J]. 广西电力, 2008, 31 (4) : 23-25.
- [4] 沐连顺, 崔立忠, 安宁. 电力系统云计算中心的研究与实践 [J]. 电网技术, 2011, 35 (6) : 170-175.
- [5] 宋磊, 罗其亮, 罗毅, 等. 电力系统实时数据通信加密方案 [J]. 电力系统自动化, 2004, 28 (14) : 76-81.
- [6] 张乐星. 基于RSA和高级数据加密标准的网络数据加密方案 [J]. 科技通报, 2005, 21 (2) : 198-200.
- [7] 李立新, 谢巧云, 袁荣昌, 等. 电网调度云灾备系统优化分析与设计 [J]. 电力系统自动化, 2012, 36 (23) : 82-86.

(收稿日期: 2015-02-10) **EA**

.....

欢迎订阅 欢迎投稿 欢迎刊登广告