Smart Grid 智能电网, 2018, 8(5), 361-366
Published Online October 2018 in Hans. http://www.hanspub.org/journal/sg
https://doi.org/10.12677/sg.2018.85040

Hans汉斯

Application of Security Label in Power Grid Asset Management

Zhenqiang Su, Xin Xia, Yubo Wang, Zhenjiang Pang

Beijing Smartchip Microelectronics Technology Company Limited, Beijing
Email: suzhenqiang@sgitg.sgcc.com.cn

Received: Aug. 21st, 2018; accepted: Sep. 19th, 2018; published: Sep. 26th, 2018

Abstract

This paper analyses the current situation of power grid asset management, finding that it is necessary to use RFID tag with security functions to help power companies complete the safety management of power grid equipment. From the more advanced anti-counterfeiting means, more effective inspection means and more convenient information entry, the management security level of the power grid assets is promoted, the counterfeiting labels of the external personnel are eliminated, the artificial error in the inspection process are avoided, the automatic information entry is realized, and the labor cost is reduced.

Keywords

RFID Label, Security Function, Anti-Counterfeiting

安全标签在电网资产管理中的应用

苏振强，夏　信，王于波，庞振江

北京智芯微电子科技有限公司，北京
Email: suzhenqiang@sgitg.sgcc.com.cn

收稿日期：2018年8月21日；录用日期：2018年9月19日；发布日期：2018年9月26日

摘　要

本文通过分析电网资产管理现状，发现为协助电力公司完成电网设备的安全管理，需要使用带有安全功能的RFID标签。从更先进的防伪手段、更有效的检查手段、更便捷的信息录入方面，提升电网资产的管理安全等级，杜绝外部人员伪造标签、避免巡检过程中人为出错、实现自动信息录入，降低人工成本。

文章引用: 苏振强, 夏信, 王于波, 庞振江. 安全标签在电网资产管理中的应用[J]. 智能电网, 2018, 8(5): 361-366.
DOI: 10.12677/sg.2018.85040

关键词

RFID标签，安全功能，防伪

1. 电网资产管理现状[1]

电网资产主要由输电线路、变电设备、配电线路及设备、用电计量设备、通讯线路及设备、自动化控制设备及仪器仪表、发电及供热设备、水工机械设备、制造及检修维护设备、生产管理用工器具、运输设备、房屋、建筑等组成。具有资产分散、使用部分多、使用地点范围大、数量多、金额大、技术更新快、生命周期长等特点。

在《固定资产管理办法》中明确要求要经常对资产进行清查盘点，每年至少全面盘点一次，保证账、卡、物相符，但是事实上由于资产数量大、分布广，现场情况复杂，很难做到定期盘点，且缺少准确高效的管理办法和手段。目前存在如下的问题：

1) 条码易破损：部分地市采用条码、二维码管理，但是由于其易损易破坏，因此一旦条码磨损将无法查询设备信息，给资产信息的查询和管理带来很大困难。

2) 无法存储、更新和高效获取数据：目前仅记录资产编号，不能提供更多关键信息支撑，无法实现各环节的资产数据存储和及时更新，例如运维检修环节的巡检结果及设备故障履历等。存在设备溯源、维护记录等信息无法在现场高效获取并及时更新的问题。

3) 无法防伪：条码及普通标识容易仿制，对于高价值或关键资产存在被恶意更换，以次充好的风险，不能做到有效资产监管，造成资产流失或信息安全风险甚至给重要系统带来安全威胁。如偷换计量仪器仪表灯。

4) 缺少协调沟通：各职能部门职责分工过于明确，缺少协调沟通，资产管理过程未流畅衔接。电网资产的建设管理、运维管理与价值管理分属不同的部门，建设部门只负责工程建设，重建设轻结算；运维管理部门则重运维轻管理，注重设备的技改大修投入。因资产变动频繁、各部门沟通不畅且资产价值变动工作本身较为麻烦等问题造成的价值变动管理工作较差。

2. RFID 标签技术特点

以应用广泛的 ISO/IEC18000-6C 协议的传统 RFID 标签为例，标签内存储 8 字节 access password 访问密码，一标签一密码，实现标签不能被仿制，非法设备不能对标签信息进行读取和篡改。对于防开启的重要信息安全设备，使用易碎防转移设计的标签，配合日常巡检工作，做到设备被非法破坏、转移后能及时发现，保证设备的安全使用。

RFID 标签具备大存储容量，可记录资产 ID、管理人、资产寿命、厂家信息、部件类别、检修记录等管理方需要的关键信息。因此可在仓储、运维、检修、报废等各阶段实现管理方与设备信息的互动，实现信息的实施更新。同时根据应用进行分区分权限的管理，防止数据被篡改，保证实物资产信息与后台信息的一致性，资产流转的可追溯性、资产责任人的准确性。

RFID 标签具备普通 RFID 标签的群读性、穿透性，可实现批量入库、盘点等环节的快速识别，同时

省去了开箱、装箱等流程来获取资产信息，为管理效率的提升提供了条件。

3. 安全 RFID 标签应用体系设计

3.1. 安全 RFID 标签安全机制

传统 RFID 标签通过 8 位的 access password 密码及 lock 锁定指令控制标签的访问权限，通过 8 位的 kill password 密码获取永久禁用标签的权限。在通过 access password 口令验证后，可修改标签数据或通过发送 lock 指令锁定标签的不同数据区，使其无法读、写，影响标签的正常使用；更严重的是在通过 access password、kill password 口令验证后，可通过发送 kill 指令，永久禁用标签。且传统 RFID 标签无法对读写设备进行身份鉴别，只要拥有正确的 access password、kill password，使用任何设备都可对标签进行恶意破坏[2]。

安全 RFID 标签安全机制上除具备普通 RFID 标签的 access password、kill password 及 lock 指令外，还支持国产 SM7 加密算法，对数据的保护及读取设备的身份鉴别安全性有了极大的提高。SM7 算法是一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。SM7 的算法目前没有公开发布。

标签访问权限控制说明：

- 标签与读写器实现双向身份鉴别：标签的身份鉴别采用 SM7 国家密码算法加密的三重身份认证机制(身份鉴别所需要的加解密运算只能在读写器的安全模块及标签芯片的安全区域内进行，从而消除 Mifare 1 卡在身份鉴别过程中所发生的密钥泄漏的安全隐患)，鉴别过程如图 1 所示。
- 读写器与中间件的双向身份鉴别：读写器与中间件的双向身份鉴别采用基于 PKI 密码技术的 SSL 协议身份认证机制，保证读写器与中间件身份的合法性，从而使攻击者无法通过伪造合法身份侵入应用系统实施攻击。
- 标签、读写器访问控制权限：对具有不同安全需求的信息及访问控制权限设置不同的密钥，使具有不同密钥的操作者具有不同的信息读取区域及不同的写入操作权限，以保证标签、读写器所存储信息在面临非法访问、数据篡改、恶意破坏等安全威胁时，攻击者不能进行相关读、写、修改、创建、删除等操作，从而保证敏感信息的安全。

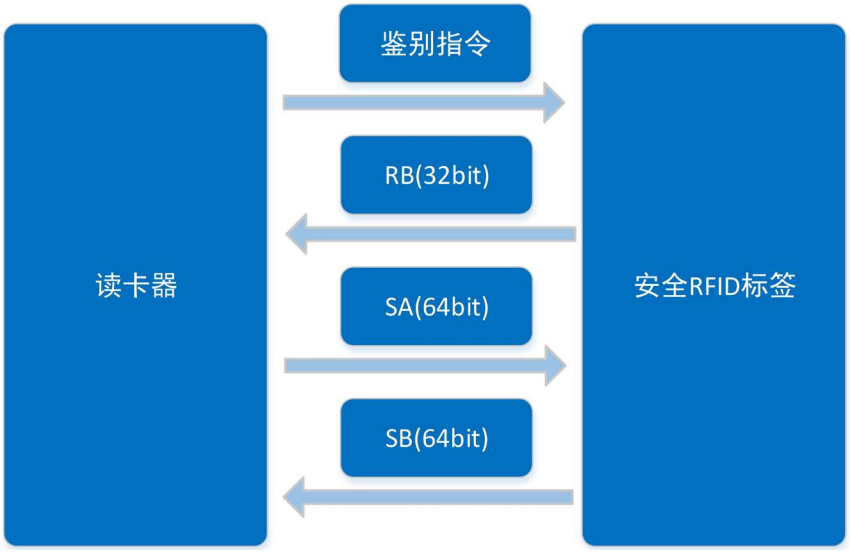

Figure 1. Identification process
图 1. 鉴别过程

3.2. 安全 RFID 标签应用体系

安全 RFID 标签应用体系分为密钥管理部门、芯片生产、设备生产、后台系统、现场五部分，如图 2 所示。

1) 密钥管理系统一级部署在密钥管理机构[3]，全国统一密钥，各网省/部门等标签使用部门通用，一套测试密钥，多套正式密钥。密钥通过密码机形式传递、发放，其分为三类：主密码机、生产密码机、主站密码机，如图 3 所示：

主密码机：发行生产密码机、主站密码机。

生产密码机：用于发行标签、桌面读写器/掌机安全芯片。

主站密码机：标签业务系统使用(需要部署到主站)，用于标签的密钥更新和手持机/读卡器的认证。

2) 芯片生产、设备生产部分完成安全芯片、安全 RFID 标签、掌机等硬件密钥的灌装及数据写入。其中安全芯片安装到手持机或固定式读写器中，协助读写器完成与安全 RFID 标签的读写操作，主要功能是完成与安全 RFID 标签的三重认证。安全芯片采用具有 SM1、SM2 和 SM7 算法的芯片。

3) 后台系统部分在传统业务系统增加密码机，实现对身份认证、下载密钥、标签认证、应用数据传输保护的功能。

4) 现场应用部分通过使用带有安全芯片的掌机、读写器完成安全 RFID 标签认证、密钥更新、应用数据读写操作。认证密钥下载时需要通过会话协商产生会话密钥，下载任务内容包含标签 EPC 数据、标签密钥密文(通过会话密钥加密标签密钥明文生成)。下载任务存储在掌机内，执行业务时，通过读取标签的 EPC 数据，查找对应的任务数据，发送给安全芯片，安全芯片解密得到标签密钥明文，对标签进行认证，认证通过后，执行业务数据写入操作。如图 4 所示。

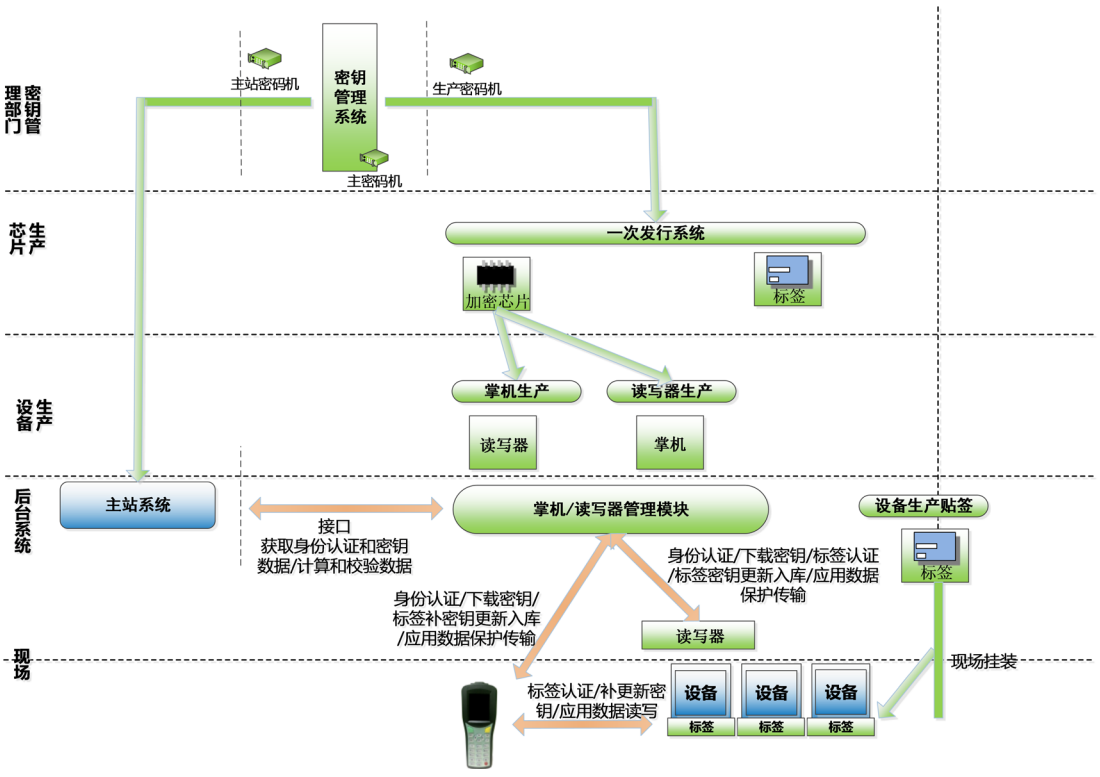

Figure 2. Security RFID tag application framework
图 2. 安全 RFID 标签应用框架

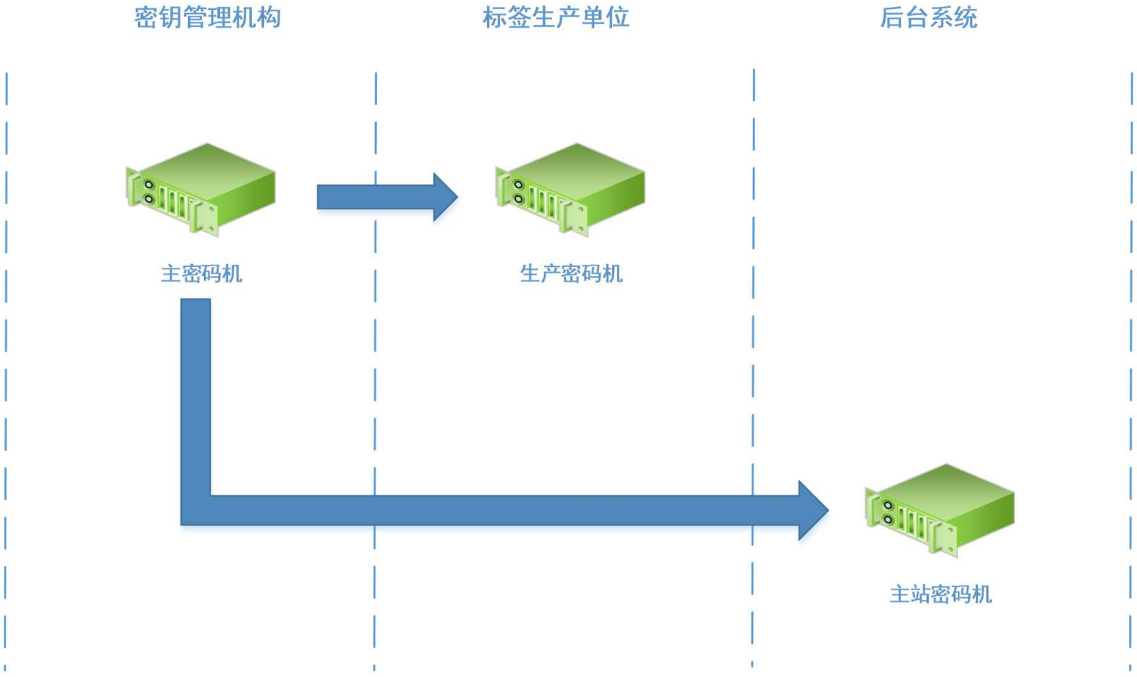

Figure 3. Use diagram of cipher machine
图 3. 密码机使用关系图

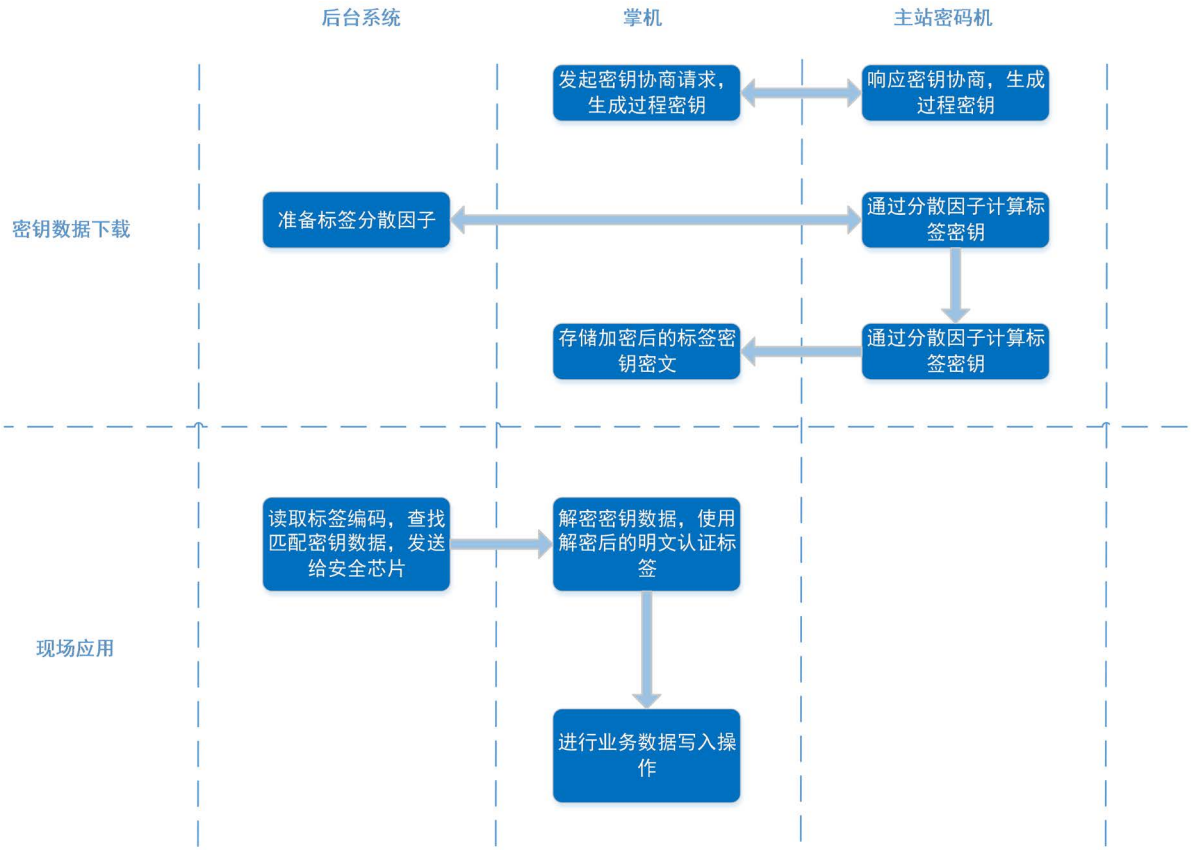

Figure 4. Application process
图 4. 应用流程

4. 结论

在智能电网建设中，信息化、自动化和互动化将成为主旋律。基于 RFID 技术，移动终端等技术，实现电网设备的集中检定、集中仓储、统一配送、统一监督，最终达到“自动化检定、智能化仓储、物流化配送”。安全 RFID 标签较传统 RFID 标签，基于国密 SM7 算法的应用，有两方面优势：1) 实现了移动终端与标签的双向身份鉴别，非法终端无法操作标签，加强了标签及移动终端的防伪性；2) 对标签进行 lock、kill、读、写指令操作时，在满足传统 RFID 标签 access password、kill password 安全机制的基础上，还需通过基于 SM7 算法的三种认证，提高了标签的防伪、防破坏性，进一步保证了资产数据的安全。为电力公司完成电网设备的安全管理，有效解决巡检工作中存在的漏检、不检问题，完善巡检督查监察，有效地杜绝因非法破坏、仿造标签造成违章用电及非法窃电事件，提升电网设备管理的安全等级提供了保障。

参考文献

[1] 唐敏. 电网资产管理中存在的问题及对策分析[J]. 广西电业, 2012(10): 42-43.

[2] 射频识别协议-第 1 类第 2 代 UHF RFID 860 兆赫-960 兆赫通讯协议[S].

[3] 高志江. 密钥管理系统的设计和实现[D]: [硕士学位论文]. 北京: 北京邮电大学软件工程, 2012.