

[电力安全]

# 电力系统视频监控网络信息安全风险及GB 35114实施意义

文/国网物资有限公司 于 胜

视频监控系统被广泛应用在各个领域，其中不乏变电站、电力沿线等场合。在使用过程中诸多的问题也暴露了出来，例如设备的合法性认证、大量使用弱口令、非法访问、信息泄密、视频信息篡改以及设备违规替换等问题非常严重。如何解决视频监控网络信息安全风险及应用GB 35114国家强制标准有着重要意义。

目前大多数视频监控网络在建设过程中，前端设备（摄像头）部署后，能够连通网络，并纳入视频管理系统中正常监控，即认为建设完成，而设备的合法性认证、视频信息的安全性问题基本没有考虑。同时由于大量使用弱口令、设备存在漏洞等管理及客观原因，视频监控网络中视频信息非法访问、信息泄密、视频信息篡改以及设备违规替换等问题非常严重。因此国家出台GB 35114—2017《公共安全视频监控联网信息安全技术要求》强制性标准，用以规范视频监控网络的建设，提升视频监控网络的安全性。GB 35114规定了公共安全领域视频监控联网视频信息以及控制信令信息安全保护的技术要求，包括公共安全视频监控联网信息安全系统的互联结构、证书和密钥、基本功能以及性能要求等技术，对提升电力系统视频监控系统的信息安全有重大意义。

## 现有视频监控系统已不满足相关政策法规要求

“没有网络安全就没有国家安全”，国网应充分重视视频监控系统的信息安全风险。

2016年11月7日《中华人民共和国网络安全法》的发布，从国家法律的高度重视网络空间安

全。《中华人民共和国网络安全法》第二十一条：国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。第二十三条：网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全监测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定，公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全监测结果互认，避免重复认证、监测。第三十一条规定：

“国家对公共通信和信息服务、能源电力、交通、水利、金融、公共服务和电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生和公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。

2017年4月14日《中华人民共和国密码法》征求意见稿发布，密码在数据加密、身份鉴别、访问控制和取证溯源等方面发挥难以替代的重要作用，通过密码实现可信互联、安全互通，以密码为核心技术和基础支撑的网络信息安全管。第十二条：关键信息基础设施应当依照法律、法规

的规定和密码相关国家标准的强制性要求使用密码进行保护，同步规划、同步建设以及同步运行密码保障系统；第十三条：国家密码管理部门负责政务活动中使用电子签名、数据电文的管理，对采用密码技术从事电子政务电子认证服务的机构进行认定。

2018年6月，《网络安全等级保护条例》规定见下表。

表 《网络安全等级保护条例》规定

| 等级保护（三级）技术要求项目 |       |                                                                                                                       |
|----------------|-------|-----------------------------------------------------------------------------------------------------------------------|
| 应用安全           | 身份鉴别  | 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；应对同一用户采取两种或两种以上组合的鉴别技术实现用户身份鉴别；应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用      |
|                | 通信完整性 | 应采用密码技术保证通信过程中数据的完整性                                                                                                  |
|                | 通信保密性 | 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始验证；应对通信过程中的整个报文或会话过程进行加密                                                                 |
|                | 抗抵赖   | 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能                                                       |
| 数据安全           | 数据完整性 | 应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施 |
|                | 数据保密性 | 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性                                                                                 |

2018年7月，网信办《关键信息基础设施安全保护条例》发布，第五十三条要求关键信息基础设施中的密码使用和管理，应对遵守相关国家强制标准和行政法规的规定。

2018年7月15日，两办发布36号文《金融和重要领域密码应用与创新发展规划》，规定了在城市基础网络、基础设施相关信息系统、城市数据采集和智慧城市中构建密码支撑体系。

GB 35114强制性标准介绍

为规范我国视频监控网络的建设和管理，实现加密视频设备的互联互通，我国出台《公共安全视频监控联网信息安全技术要求》强制性国家标准（国标代号：GB 35114—2017）。标准要求“系统应使用基于非对称密码算法的数字证书体系实现用户身份认证、前端设备认证、服务器设备认证和管理平台间认证等安全功能。应为用户、前端设备、服务器设备以及管理平台签发数字证书。”标准对网络的安全保护强弱要求分为三个等级：“A级应基于数字证书与管理平台双向身份认证的能力，达到身份真实目标。B级应基于数字证书与管理平台双向身份认证的能力和对视频数据签名的能力，达到身份真实和视频来源于真实设备，能够校验视频内容是否遭到篡改的目标。C级应具备基于数字证书与管理平台双向身份认证的能力、视频数据签名能力和视频数据加密能力，达到身份真实和视频来源于真实

设备，能够校验视频内容是否遭到篡改，能够达到对视频内容加密保护目标。”

GB 35114解决方案

GB 35114解决方案主要包含视频监控网络安全检测与管理系统、设备认证管理系统、视频监控安全网关及视频基础硬件设备四部分。CA数字证书系统为视频系统的摄像头密码模块、NVR网络硬盘录像机密码模块、身份认证网关、SIP网关和管理员智能密码钥匙进行数字证书颁发，并将颁发后的证书发布到目录服务中供系统用户管理使用。

1PC摄像头集成安全芯片，芯片内颁发证书，摄像头连入NVR网络硬盘录像机（或者视频监控平台）时采用SIP协议通信通过数字证书进行认证，视频内容采用对称密钥进行数据流加密，关键视频帧进行数字签名。

NVR网络硬盘录像机内集成密码芯片，对摄像头的接入认证请求进行认证，接入视频监控平台时与视频监控平台的SIP网关进行身份认证。

视频监控平台配套SIP网关，用SIP网关进行平台间身份认证和视频监控终端认证，NVR网络硬盘录像机认证。配套身份认证网关用于用户登录应用的身份认证。

用户使用智能密码钥匙进行视频监控平台登录认证。远程调用视频架空平台视频解码器进行视频播放。

IPC监测系统实时对视频网内的摄像头进行

合法性验证，向摄像头发送验证挑战码。摄像头按照验证协议对挑战码、设备信息等数据封装后进行数字签名后回复验证响应。IPC监测系统通过数字签名服务器对返回的验证响应进行验签，根据验签后的结果判断摄像头合法性。

视频监控安全网关是在传统网络安全网关的基础上，针对视频监控网络的特点进行完善，融合了设备准入控制技术、攻击检测、漏洞防护和Web安全防护等多种安全技术，实施对视频监控网络的安全防护。视频监控安全网关可以根据应用的行为和特征实现对应用进行识别和控制，能够识别网络中各种设备的特征，只有合法的设备方可正常通信，从而实现对设备的准入控制能力。视频监控安全网关具备漏洞特征库、木马插件等恶意内容特征库和Web应用威胁特征库，可以全面识别各种应用层和内容级别的各种安全威胁。

## GB 35114强制性标准实施意义

### 1. 提高视频监控网络安全检测

视频监控网络安全检测与管理系统是针对目前视频监控网络的普遍存在资产底数不清、管理不规范，大量存在使用弱口令及安全漏洞的设备，网络边界不清以设备违规替换等问题研发的综合管理系统，GB 35114标准要求设备带有CA证书，将极大帮助对视频监控网络进行快速扫描，快速掌握网络中的资产组成与分布情况，建立整个网络的设备资产库，同时也杜绝了设备的弱口令问题。此外，系统能够快速发现网络中违规接入的设备或非法外联行为并进行定位和处理，从而保障网络的边界安全。

### 2. 设备认证、安全网关多重保障接入安全

本方案中采用视频监控网络安全检测与管理系统、设备认证管理系统和视频监控安全网关系统相互联合，可确保通过合法认证的设备接入网络，并能及时发现网络中的各种违规行为。同时设备认证管理系统（CA认证系统）还可保障端到端通信的合法性，国密算法生成的CA证书难以伪造，具备唯一性，杜绝了摄像机端和后台端的非法接入，可以确保系统不受黑客攻击病毒感染，充分考虑抵御来自非法访问者的侵入和攻击，解决危及企业国家安全的问题。

### 3. 视频加密防控制，防泄密，防入侵，视频网更安全

符合GB 35114的前端摄像机向下兼容常见的

不加密的H.264、H.265等国外视频编码标准，还支持SVAC2.0标准。SVAC2.0标准规定了视频数据加密方法和规范。摄像机采用前端视频流加密技术，确保端到端指令数据加密，可以防止非法分子通过窃取视频流获得政府敏感信息、公民个人隐私；视频录像加密存储，杜绝了视频外流、防止敏感视频从内部泄露到社会；数据摘要加密，防止敌对分子通过视频篡改进行非法活动。视频监控系统具有高度的安全和保密性，通过中心管理机制对整个系统进行严格的自动化的安全管理，管理人员无需逐个对已安装摄像头更改密码，减少管理工作难度，并可使得系统无论在软件还是硬件都达到更高的安全标准。

### 4. 便于资产管理，让全网资产分类统计，清晰明了

GB 35114标准采用基于CA证书的设备管理方式，便于视频监控网络安全检测，可实现对视频监控网络全网资产的快速识别与智能分类，同时与设备认证管理系统联动，可建立全网高效可信的全网资产库，从而全面掌握网络建设情况和设备分部情况，同时对前端设备违规替换进行安全检查。

## 结束语

“关键信息基础设施是经济社会运行的神经中枢，是网络安全重中之重，也是可能遭到重点攻击的目标”，要求“要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改”。按照国家相关规定，国网应加强网络安全传输、系统安全保障和重要信息安全管理等技术手段建设，提升公共安全视频监控系统安全防护能力。严格公共视频图像信息的使用管理，完善安全技术措施，确保安全共享、规范使用。要严格安全准入机制，实现重要视频图像信息不失控，敏感视频图像信息不泄露。

视频监控联网建设需要标准化支撑，标准化是电力系统视频监控联网建设的基础和前提，通过标准促进监控系统的互联互通，有利于监控数据的开放、共享、挖掘和分析，有利于安全事件的实时研判，智能化处置。通过标准化可以打破视频监控的信息孤岛，能够有效整合资源，形成统一监控体系，提升视频监控的技术水平，实现最佳秩序和最大经济效益。EA

（收稿日期：2018.01.18）

（编辑：朱金凤）