ICS 29.120.01
CCS K 46

团 体 标 准

T/CPIA 0070—2024

光伏逆变器信息安全保护技术要求

Requirements of Information Security Protection for PV inverters

2024－08－30 发布　　2024－09－15 实施

中国光伏行业协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国光伏行业协会标准化技术委员会提出。

本文件由中国光伏行业协会标准化技术委员会归口。

本文件起草单位：之江实验室、中国电子技术标准化研究院、浙江省白马湖实验室有限公司、之江奇安科技有限公司、华为数字能源技术有限公司、阳光电源股份有限公司、国网山西省电力公司、国网山西省电力公司电力科学研究院、中国大唐集团科学技术研究院有限公司、杭州安恒信息技术股份有限公司。

本文件主要起草人：朱桢、沈曲、陈晓达、庄天奇、李臻、孙务本、张奕鹏、夏俊伟、殷志鹏、杜荣华、赵俊屹、冯磊、李若峰、吴灏。

光伏逆变器信息安全保护技术要求

1 范围

本文件规定了光伏逆变器控制安全、网络安全、数据安全、应用安全等方面的信息安全保护相关技术要求。

本文件适用于接入电网的具备通信功能光伏逆变器的设计、研制和验收，其他类型的逆变器、DC直流变换器、储能变流器、数据采集装置也可参照执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 36470—2018 信息安全技术 工业控制系统现场测控设备通用安全功能要求

GB/T 42456—2023 工业自动化和控制系统信息安全 IACS组件的安全技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息安全 information security

保护、维持信息的保密性、完整性和可用性，也可包括真实性、可核查性、抗抵赖性、可靠性等性质。

[来源：GB/T 25069—2010，2.1.52]

3.2

网络安全 network security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。采取措施包括：通信和传输保护、边界防护、接入认证授权、本地通信保护等。

[来源：GB/T 22239—2019，3.1，有修改]

3.3

数据安全 data security

通过采取必要措施，防止数据在传输过程中被泄露、损毁或丢失的情况发生，保护数据的完整性、保密性、可用性。采取措施包括数据加密及保护、数据缓存、日志安全保护、用户信息数据保护等。

[来源：GB/T 39477—2020，3.1，有修改]

3.4

应用安全 application security

通过采取必要措施，防止应用软件及相关组件在处理业务过程时出现数据的泄露、损毁或丢失。采取措施包括身份认证和访问控制、软件开发安全、更新和升级保护等。

3.5

控制安全 control security

通过采取必要措施，确保控制系统执行的控制命令来自合法用户正确的执行，控制软件出现的漏洞应被及时的处理，异常控制指令应被及时的发现，防护可预见的危险状况。采取措施包括采取控制协议安全机制、指令安全审计等。

3.6

个人数据 personal data

以电子或其他方式记录的能够单独或者与其他信息结合识别特定公民或组织，或者反映特定公民或组织活动情况的各种信息。

3.7

敏感数据 sensitive data

敏感数据的具体范围取决于产品的具体应用场景，典型的敏感数据包括认证凭据（如口令、动态令牌卡等）、大批量个人隐私数据等。

3.8

用户数据 user data

光伏逆变器上存储的由用户产生或为用户服务的数据。

[来源：GB/T 25069—2022，3.736，有修改]

4 总则

4.1 光伏逆变器的信息安全可由逆变器功率模块和通信模块协同实现，通信模块可集成在光伏逆变器内部，也可与光伏逆变器在外部相连。

4.2 光伏逆变器的通用信息安全要求应满足 GB/T 36470—2018 第 6 章要求、GB/T 42456—2023 第 13 章要求。

5 网络安全

5.1 接入认证授权

光伏逆变器应具有唯一性标识，并在接入网络时对接入方进行身份认证，认证通过后应根据身份进行授权。网络接入认证宜采用基于数字证书的身份认证等机制来实现。

5.2 用户标识

用户标识要求如下：

a) 光伏逆变器调试、管理与业务数据传输接口应具备标识用户的功能；

b) 光伏逆变器宜具备唯一标识用户的能力。

5.3 身份认证和访问控制

身份认证和访问控制要求如下：

a) 所有访问接口应具有实施身份认证功能，对用户的最终认证处理过程应放到服务器端；

b) 不应存在可绕过系统安全机制（认证、权限控制、日志记录）对系统或数据进行访问的功能；

c） 应区分不同身份角色，按照角色来授予对应权限；
d） 针对远程控制的业务场景，应设置独立账户，并控制其访问权限；
e） 每台逆变器应具有一个随机的出厂管理密码或首次登录时强制设置密码；
f） 对于远端访问宜采用 USB 密钥、数字证书、用户名+口令、智能卡、指纹、动态密码等身份认证管理技术中至少两种方式进行身份鉴别，身份鉴别过程应具备防重放机制；
g） 对于近端访问宜采用 USB 密钥、数字证书、用户名+口令、智能卡、指纹、动态密码等身份认证管理技术中至少一种方式进行身份鉴别，身份鉴别过程应具备防重放机制；
h） 用户的认证凭据信息（如密码，密钥）应支持修改或更换，不应公开明文展示，不应明文存储和传输；
i） 修改密码前应具备验证旧密码的功能；
j） 所有的对外接口和出厂默认口令，应在公开的用户资料中说明；
k） 不应在系统中存储的日志、调试信息、错误提示中明文打印认证凭据；
l） 用户修改的密码应满足复杂度要求，包含大写字母、小写字母、数字中、特殊字符的至少 2 种组合，长度不小于 8 字符；同时应提供密码的防暴力破解机制，当在一定时间段内重复输入错误口令次数超过阈值时应采取保护措施如锁定账号，锁定 IP，登录延迟等功能，超过一定时间后逆变器状态自动恢复；
m） 具备无线通讯功能的光伏逆变器，其无线模块的初始密码应不相同且密码支持修改；
n） 对于接入云托管系统场景的光伏逆变器，识别信息标识应唯一且不可预测，防止仿冒；
o） 身份认证和访问控制应使用安全的密码学算法，应满足附录 A.1 要求。

5.4 边界防护

边界防护要求如下：
a） 应保证跨越边界的访问和数据流通过受控接口进行通信，能监视和控制边界的通信。受控接口应在出厂时默认关闭，仅在使用时打开，不使用时应及时关闭；
b） 具有无线传输功能的光伏逆变器应支持关闭无线通信方式的功能；
c） 应具备对串口、可移动存储介质等物理接口的使用进行限制（禁用自动执行脚本、对传入/传出的代码和数据类型进行限制和校验等）的能力。

5.5 证书管理

数字证书管理要求如下：
a） 数字证书应使用安全的密码学算法，应满足附录 A.1 的要求；
b） 应具有唯一证书，在证书使用者主题中含有光伏逆变器唯一性信息（如电子序列号 ESN、IP 地址或 MAC 地址等）；
c） 应支持对证书内容校验，以确保身份合法；
d） 应支持证书有效期检测，有效期即将到期和到期前均上报告警；数字证书有效期应覆盖光伏逆变器全生命周期；
e） 应支持证书更换功能；
f） 应对证书私钥使用安全加密算法加密存储，不应明文导出；
g） 宜支持证书吊销功能，以及证书吊销列表校验；
h） 宜支持信任根证书管理功能，支持信任根证书的导入功能。

6 数据安全

6.1 数据通信和传输保护

数据通信与传输保护要求如下：

a) 应保证通信过程中的机密性、完整性和有效性，网络传输过程中不应被窃取或篡改，应保证合法用户对信息和资源的有效使用；
b) 基于网络的通信应采用安全协议实现数据安全传输，并提供数据加密通道，保障维护管理过程的数据传输安全。若采用 Transport Layer Security（TLS）协议，应使用 TLS 的安全版本，安全协议应满足附录 A.2 的要求；
c) 启用不安全协议应产生告警或用户提示；
d) 数据通信建立连接前，服务端应对发起端进行身份认证；通讯过程中应支持防重放攻击；通讯断链后应重新进行身份认证；
e) 对于人机接口，应支持超过一定时间未操作后自动退出会话，会话标识失效；
f) B/S(浏览器/服务器)应用中，用户名和口令认证通过后，应更换会话标识。

6.2 数据加密及保护

数据在存储、传输、使用时均应加密保护，要求如下：

a) 应支持分等级数据加密方法，根据数据密级采用不同的安全存储机制。敏感数据应进行加密存储，敏感数据包括密码、共享密钥，私钥等；
b) 应采用安全的加密算法，使用通过认证的或业界开源公认的密码算法库，应满足附录 A 的要求；
c) 应支持密钥管理，支持工作密钥、根密钥分层管理；加密数据与安全通信协议使用不同的工作密钥，支持密钥安全存储，如将密钥存储在安全存储区或特定代理内部，支持密钥安全生成和分发，宜支持密钥可更新；
d) 密码算法中应使用安全随机数；
e) 宜支持数据完整性保护，对敏感数据提供完整性检测机制，敏感数据损坏和丢失时应能及时发现。

6.3 数据安全使用

数据安全使用要求如下：

a) 应收集最小范围的数据，所使用的数据应是光伏逆变器功能所必须的；
b) 敏感数据不应明文显示，在呈现时应作匿名化或假名化处理，不应在软件界面，日志、客户资料、配置文件等向客户体现；
c) 收集的遥测数据应仅限于预期功能所需的最小范围。

6.4 日志安全保护

日志安全保护要求如下：

a) 具备检测、记录光伏逆变器自身状态和用户对光伏逆变器操作动作的能力；
b) 记录光伏逆变器自身重要运行状态和故障状态的信息，如开机、关机、重启、故障发生、故障恢复等；
c) 记录用户登录、注销、权限变更和核心参数变更等操作；
d) 记录用户对光伏逆变器操作时所使用的账号、操作时间、被访问的资源名称，访问发起端的地址或标识、操作内容以及操作结果；

e） 具备按用户角色分配日志文件读取的能力，防止日志文件未授权情况下被非法读取、删除或修改；

f） 不应在系统中存储的日志、调试信息、错误提示中明文打印认证凭据。

6.5 用户数据保护

光伏逆变器处理用户数据时，应遵循合法、正当、必要的原则，要求如下：

a） 对于逆变器数据上云场景、云侧系统的用户数据控制者，应明示事先收集的目的和范围，遵循最小必要原则，并只在用户同意的情况下进行；

b） 用户敏感数据存储在光伏逆变器内部时，应加密并进行控制访问权限；

c） 用户数据通过网络传输时，应确保信息在网络传输过程中的安全；

d） 不应在未经授权时进行用户数据转移，导出包含用户的数据时应对敏感数据进行过滤、匿名化或假名化处理，信息不应明文展示、打印或传输；

e） 在正常业务流程和标准协议之外，不应进行用户精确位置信息定位；

f） 日志中不应记录用户敏感数据含个人数据、交通数据或位置数据等；

g） 应具备快速删除用户数据的能力。

7 应用安全

7.1 软件开发安全

光伏逆变器固件中不应存在恶意代码程序，要求如下：

a） 外购部件安全：应识别和管理产品内使用的所有外部提供的组件的安全风险，提供安全测试报告；

b） 纵深防御设计：应根据威胁模型确定风险，采取措施缓解风险，实施多层防御策略；

c） 开发环境安全：开发环境所用的操作系统、开发工具、编译器、数据库应进行安全配置，及时进行补丁升级和漏洞修复，保护软件开发过程安全；

d） 安全测试：软件开发应经过严格的安全验证测试并提供测试报告。测试应包括安全需求测试、威胁缓解测试、漏洞测试和渗透测试等；

e） 安全接口：不应有未公开的接口；

f） 漏洞修复：应具备漏洞管理流程，及时对软件中出现的漏洞进行修复或提供其他替代解决方案。

7.2 软件更新和升级保护

软件更新和升级保护要求如下：

a） 应在经过充分测试评估后,在不影响光伏逆变器安全稳定运行的情况下进行补丁更新、固件升级等工作；

b） 对外发布的软件（包含软件包/补丁包）应提供数字签名证书来支持完整性校验机制；

c） 更新或升级前应确认软件包的完整性，应采用满足安全要求的完整性保护机制，宜通过在软件包中内置数字签名文件来对完整性进行验证；宜支持在升级前自动对软件包完整性进行校验；

d） 更新或升级程序前应进行身份识别，仅授权身份的用户允许执行；

e） 应支持软件升级版本防回退功能，防止升级到低版本后的降级攻击；

f） 宜支持基于硬件可信根的安全启动功能，防止软件被篡改。

7.3 安全资料

光伏逆变器安全资料要求如下：

a) 应提供通信端口列表，描述机器/网元/模块间的通信关系，包括：通信使用的端口、协议、IP 地址、认证方式、端口用途信息等；
b) 应提供安全相关的配置或加固指南；
c) 应提供产品缺省内置的账号清单及相应默认密码；
d) 应提供各数字证书的使用场景及用途。

7.4 安全配置

应确保系统服务做到默认安全，降低安全等级时应提醒。默认安全的安全参数，要求如下：

a) 默认关闭不使用的服务和端口；
b) 默认不允许空口令或默认口令；
c) 默认开启日志审计；
d) 默认关闭不安全的通信协议，如兼容原因需打开须用户确认并提示风险。

7.5 漏洞管理

漏洞管理要求如下：

a) 逆变器、操作系统、数据库、开源和三方组件存在已知漏洞，应及时将安全漏洞风险及修补方式告知用户并提供必要的技术支持；
b) 软件版本发布前应对已公开的漏洞进行管理，严重及以上等级漏洞应修复；未修复漏洞应给出风险评估；
c) 应支持对现网运行光伏逆变器的漏洞进行管理，监测公开漏洞，发现漏洞后及时提供修复版本，降低现网安全风险。

8 控制安全

8.1 控制协议安全机制

应对使用光伏逆变器的运维用户进行身份认证，不同的操作类型需要不同权限的认证用户来操作，未经认证的用户所发出的控制命令不应执行。在控制协议通信过程中，应避免攻击者实现针对控制指令的截获报文、劫持会话、重放指令等攻击手段。

——对 I 类指令：应由较高权限用户或管理员身份的用户下发，并对关键操作要实行二次鉴权。

——对 II 类指令：可由授权用户下发。

注1：I类指令为控制类，如启停机、参数修改等核心指令，包括启动、停机、口令、电气保护参数等。

注2：II类指令为监视类，如数据统计、运行监测等辅助指令，包括数据查询、状态查询等。

8.2 指令安全审计

控制指令应进行安全监测审计，并应进行日志记录。应及时进行安全事件的告警及上报，并可为安全事故的调查提供数据支持。

8.3 时间同步

应支持人工设定系统时间或自动时间同步。当采用自动时间同步时，应使用NTP最新安全版本、IEEE 1588 PTP或类似安全协议获取当前日期和时间。

附 录 A
（规范性）
密码学算法和安全通信协议

A.1 安全的密码学算法

A.1.1 对称密码算法如下：

——分组密码：

- AES-GCM(≥128 bits)；
- SM4（128bit）。

——流密码：

- AES-CTR(≥128 bits)；
- AES-OFB(≥128 bits)；
- chacha20-poly1305；；
- ZUC（128bit）。

A.1.2 Hash函数如下：

——SHA256 或以上；

——SHA3-256 或以上；

——SM3（256）；

——SHA224(HMAC/密钥派生/随机数产生场景)；

——SHA512/224(HMAC/密钥派生/随机数产生场景)；

——SHA3-224(HMAC/密钥派生/随机数产生场景)；

——PBKDF2, ≥ 5000 次。

A.1.3 非对称密码算法如下：

——RSA(≥3072 bits)；

——ECIES (≥256 bits)；

——DLIES(≥3072 bits)；

——SM2(只支持 256 bits)；

——SM9(只支持 256 bits)。

A.1.4 数字签名算法如下：

——RSA(≥3072 bits)；

——ECDSA(≥256 bits)；

——EdDSA(≥256 bits)；

——SM9(只支持 256 bits)；

——SM2(只支持 256 bits)。

A.1.5 密钥协商算法如下：

——DH (L≥3072 bits, N≥256 bits)；

——ECDH(≥256 bits)；

——SM9(只支持 256 bits)。

A.2 安全通信协议

安全协议包含：HTTPS、SSHv2、TLS1.2、TLS1.3、IPSec、SFTP、FTPS、SNMPv3等协议及其业界最新安全版本，不安全协议包含：HTTP，SSHv1.x、Telnet、SSL2.0、SSL3.0、TLS1.0、TLS1.1、TFTP、FTP、SNMP v1/v2等，安全通信协议包含如下：

——支持身份验证机制，支持基于数字证书的签名校验。

——使用安全的密码套件，参考附录 A.3。

A.3 安全密码套件

TLS1.2 允许使用的密码套件清单见表 A.1。

表 A.1 TLS1.2 允许使用的密码套件清单

IANA 编码	IANA 套件名	安全程度
0x00,0x9E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	高
0x00,0x9F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	高
0x00,0xA2	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	高
0x00,0xA3	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	高
0x00,0xAA	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	高
0x00,0xAB	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	高
0xCC,0xAD	TLS_DHE_PSK_WITH_CHACHA20_POLY1305_SHA256	高
0xC0,0x2B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	高
0xC0,0x2C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	高
0xC0,0x2F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	高
0xC0,0x30	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	高
0xCC,0xA8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	高
0xCC,0xAC	TLS_ECDHE_PSK_WITH_CHACHA20_POLY1305_SHA256	高
0xD0,0x01	TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256	高
0xD0,0x02	TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384	高
0xD0,0x05	TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256	高
0xC0,0x9E	TLS_DHE_RSA_WITH_AES_128_CCM	高
0xC0,0x9F	TLS_DHE_RSA_WITH_AES_256_CCM	高
0xCC,0xAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	高
0xC0,0xA6	TLS_DHE_PSK_WITH_AES_128_CCM	高

表 A.1　TLS1.2 允许使用的密码套件清单（续）

IANA 编码	IANA 套件名	安全程度
0xC0,0xA7	TLS_DHE_PSK_WITH_AES_256_CCM	高
0xC0,0xAC	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	高
0xC0,0xAD	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	高
0xCC,0xA9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	高

TLS1.3 允许使用的密码套件清单见表 A.2。

表 A.2　TLS1.3 允许使用的密码套件清单

IANA 编码	IANA 套件名	安全程度
0x13,0x01	TLS_AES_128_GCM_SHA256	高
0x13,0x02	TLS_AES_256_GCM_SHA384	高
0x13,0x03	TLS_CHACHA20_POLY1305_SHA256	高
0x13,0x04	TLS_AES_128_CCM_SHA256	高

参照 RFC8998，TLS1.3 新增国密算法套见表 A.3，这两个算法套不能用于 TLS 其他版本。

表 A.3　TLS1.3 允许使用的国密算法密码套件清单

IANA 编码	IANA 套件名
0x00,0xC6	TLS_SM4_GCM_SM3
0x00,0xC7	TLS_SM4_CCM_SM3

参 考 文 献

[1] GB/T 36572—2018 电力监控系统网络安全防护导则

[2] GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

[3] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[4] GB/T 37962—2019 信息安全技术 工业控制系统产品信息安全通用评估准则

[5] GB/T 25069—2022 信息安全技术 术语

[6] GB/T 39477—2020 信息安全技术 政务信息共享数据安全要求

[7] GB 40050—2021 网络关键设备安全通用要求

[8] GB/T 33008.1—2016 工业自动化和控制系统网络安全 可编程序控制器(PLC) 第1部分：系统要求

[9] 国能安全[2015]36号《电力监控系统安全防护总体方案》

[10] 工信部联网安[2021]66号《网络产品安全漏洞管理规定》

[11] NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations

[12] NIST SP 800-82 Guide to Industrial Control Systems(ICS) Security

[13] NB/T 32004—2018 光伏并网逆变器技术规范