ICS 97.120
CCS K 32

中华人民共和国国家标准

GB/T 43342—2023

带有远程操作功能的家用和类似用途电器自动控制器的安全要求

Safety requirements of automatic controls for household and similar purposes with remote operation

2023-11-27 发布　　2024-06-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由中国电器工业协会提出。

本文件由全国家用自动控制器标准化技术委员会(SAC/TC 212)归口。

本文件起草单位：青岛海尔智能技术研发有限公司、中国电器科学研究院股份有限公司、美的集团股份有限公司、海信家电集团股份有限公司、北京小米电子产品有限公司、青岛海尔科技有限公司、博西华电器(江苏)有限公司、青岛海尔空调器有限总公司、湖北美的电冰箱有限公司、威凯检测技术有限公司、广东中创智家科学研究有限公司、广州朗国电子科技股份有限公司、广州市威士丹利智能科技有限公司、宁波公牛生活电器有限公司、浙江绍兴苏泊尔生活电器有限公司、宁波方太厨具有限公司、广东新宝电器股份有限公司、深圳和而泰智能控制股份有限公司、浙江哈尔斯真空器皿股份有限公司、杭州萤石软件有限公司、青岛海信日立空调系统有限公司、广东欧曼科技股份有限公司、青岛博芬智能科技股份有限公司、佛山市顺德区本立电器科技有限公司、深圳市彩斓光电科技有限公司、中家院(北京)检测认证有限公司、广东华南家电研究院、施耐德电气(中国)有限公司深圳分公司、杭州鸿雁电器有限公司、代傲电子控制(南京)有限公司、广东合捷电器股份有限公司、浙江伟江电器股份有限公司、浙江东信电器有限公司、广东万和电气有限公司、通标标准技术服务有限公司、佛山市国星光电股份有限公司、中山市至拓智能控制系统有限公司、厦门华联电子股份有限公司、深圳拓邦股份有限公司、广东瑞德智能科技股份有限公司、汕头市天际电器实业有限公司、无锡飞翎电子有限公司、浙江飞哲工贸有限公司、佛山市雅洁源科技股份有限公司、宁波恒达高智能科技股份有限公司、中山市海宝电器有限公司、澳柯玛股份有限公司、宁波微科光电股份有限公司、广东智科电子股份有限公司、箭牌家居集团股份有限公司、宁波欧知电器科技有限公司、广东当家人智能电器有限公司、西安旭迈智能家电科技有限公司、广东飞成新材料有限公司、宁波亚辉智能科技有限公司、广东特华科技有限公司、浙江华丛数字科技有限公司、陕西硕恩大数据科技有限公司、宁波卡特马克智能厨具股份有限公司、宁波思朗智能科技发展有限公司、中山市迪生电气有限公司、江阴市志骏电器线缆有限公司、广东利英智能科技有限公司、浙江昂华新材料有限公司、广东益杜科技有限公司、浙江如晶科技有限公司、广东庆合科技有限公司、福建泰多科技有限公司、广东雅音科技有限公司。

本文件主要起草人：冯承文、孔睿迅、陈林、刘照光、陈灿峰、井皓、李玲、张桂芳、焦其意、景意新、庄伟玮、罗益峰、谭志勇、赵克锋、代松、刘俊翔、杨彬、汪显方、刘润军、王淼、李航快、张文强、李小祥、王建波、林诺锋、张彩兰、魏明然、赖静、黄志文、吴剑、张友福、康作添、应雨江、牛晟、卢仲宇、何径业、左清跃、黎国良、陈虢、欧亮、方桦、林镇城、苏忠城、夏月飞、李杰、祝良雄、余杰、李刚、邱奕航、李百尧、谢岳荣、柯赐龙、蒋惠兴、陈锋、段春芳、陈乃恩、张元林、邓代从、南少微、徐红卫、施冬冬、郑赞文、芦小山、马志军、丁春燕、王光建、李守英、肖本崇、周自新、林燕、张德军。

引　言

带有远程操作功能的家用和类似用途电器自动控制器相对于传统自动控制器有安全要求的变化，如：

——外部通信网络引入信息安全以及功能安全的变化；

——原有人值守转变为无人值守的工作状态引入安全变化；

——嵌入式操作系统引入安全变化；

——人机交互方式的多样性增加相应的安全要求；

——增加对过程数据的安全考虑，根据数据的重要性以及应用分类需进行分类管控；

——增加全生命周期的安全考虑，包括开发、销售、安装、运营、维修、转移、回收及销毁等过程。

因此，为了解决家用和类似用途电器自动控制器由于具有了远程操作功能可能出现的各种安全风险问题，需要一份安全文件来进行总体规范。

带有远程操作功能的家用和类似用途电器自动控制器的安全要求

1 范围

本文件规定了带有远程操作功能的家用和类似用途电器自动控制器(以下简称“自动控制器”)的通用要求、技术要求、指示、标识和说明文件。

本文件适用于家用和类似用途电器中以及公共场所使用设备中自动控制器的设计、生产和使用。

本文件不适用于专门用于工业用途的自动控制器以及彩电、手机、计算机和便携式移动终端等音视频及信息类产品自动控制器。

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 14536.1 电自动控制器 第1部分:通用要求

GB/T 25069 信息安全技术 术语

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 35273 信息安全技术 个人信息安全规范

ISO/IEC 15408(所有部分) 信息安全、网络安全和隐私保护 信息技术安全的评估标准(Information security, cybersecurity and privacy protection—Evaluation criteria for IT security)

3 术语和定义

GB/T 14536.1、GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

远程操作 remote operation

通过屏幕、语音、手势等交互方式,对连接网络(包括无线和有线方式)的自动控制器本体发出指令,对自动控制器进行操作或者自动控制器通过网络(包括无线和有线方式)向远程操作机构的管理者发送信息。

注1:操作包括对自动控制器的远程控制、查询、软件下载等。

注2:远程操作机构的管理者,包括但不限于:手机、电脑、服务平台、操作者、其他自动控制器。

注3:自身的红外线控制或者点对点的近距离无线通信不能称为远程操作。

3.2

远程操作机构 remote operating mechanism

无论是可见的位置还是不可见的位置,用于在人离开自动控制器的位置(包括可见的位置)对自动控制器进行操作的机构,包括但不限于:

a) 远程操作控制器(通过网络使用指令控制自动控制器的设备);

b） 移动智能终端；

c） 智能音箱。

注：远程操作机构既能与被远程操作的自动控制器在同一个空间（房间）位置，也能处于同一个家庭空间的不同房间，也可以处于家庭外部。

3.3

无人监控 unmanned monitoring

在没有人看管和操作的状态下运行。

4 缩略语

下列缩略语适用于本文件。

ADB：安卓调试桥（Android Debug Bridge）

AES：高级加密标准（Advanced Encryption Standard）

API：应用程序接口（Application Programming Interface）

ARP：地址解析协议（Address Resolution Protocol）

DHCP：动态主机设置协议（Dynamic Host Configuration Protocol）

DNS：域名系统（Domain Name System）

ECC：误差校正码（Error Correcting Code）

FTP：文件传输协议（File Transfer Protocol）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）

ICMP：Internet 控制报文协议（Internet Control Message Protocol）

IP：互联网协议（Internet Protocol）

MMU：内存管理单元（Memory Management Unit）

MPU：内存保护单元（Memory Protection Unit）

NTP：网络时间协议（Network Time Protocol）

OTA：空中下载技术（Over-the-Air Technology）

PCB：印制电路板（Printed Circuit Board）

PSK：预共享密钥（Pre-Shared Key）

SSH：安全外壳协议（Secure Shell）

URL：统一资源定位系统（Uniform Resource Locator）

WEB：万维网（World Wide Web）

5 通用要求

自动控制器应满足 GB/T 14536.1 和 GB/T 35273 要求。

自动控制器本地的安全措施优先级应高于远程安全措施，在断网或网络状况不佳、无人操作或操作人员缺乏操作知识的情况下，自动控制器应能保证安全。

当环境条件或操作条件发生变化时，自动控制器的安全应能达到与环境相适应的安全水平。

自动控制器应具有安全保护机制，当处于家用和类似用途使用环境（如温度、电压、电磁辐射、光照及网络等）时，应能保证自动控制器的安全及具备工作异常时的相应安全措施。

自动控制器在发生特定失效或故障时为保证安全，应向用户或上层监控系统发送警告，以便及时处理，将安全风险降低，且在设计时至少采取以下一项安全措施：

a) 利用部分系统维持工作，如：进入到安全保护模式，关闭或禁止该失效或故障相关的功能，限制失效或故障的问题扩散，维持基本的安全运行模式；
b) 切换到独立的备用系统。

6 技术要求

6.1 不同电源供应方式要求

自动控制器如采用电源供应方式为电池或对电源供应有限制的方式时，其设计的基本功能不应依赖于远程操作。

对于通信方式支持睡眠模式的自动控制器，在状态发生变化或报警时应能被唤醒，保证信息的及时传递，避免漏报安全事件。

6.2 长时间通电可靠运行

在无人监控状态下，自动控制器应能与产品要求相适应，实现长时间通电可靠运行。

6.3 远程操作功能的禁止和开启

自动控制器满足以下要求：

a) 有打开或关闭网络通信的功能；
b) 在正确安装配置后根据用户需求方可开启远程操作；
c) 有相应的指示，显示其是否开启了远程操作功能；
d) 允许远程操作功能时，能对网络通信状态进行监控，在网络通信状态不好时应保证相应的安全。

6.4 芯片安全

如自动控制器使用安全芯片，则该安全芯片应满足 ISO/IEC 15408(所有部分)中 EAL 4+的全部保证组件要求。

6.5 接口安全

自动控制器采取措施减少暴露的受攻击面要求如下。

a) 在出厂前应关闭不必要的硬件端口，不预留后门，对于可物理接入的调试接口，满足以下要求的一种：
   1) 自动控制器的调试功能应具备认证机制，保证仅已授权用户可以访问；
   2) 自动控制器的调试接口和调试功能应被加密处理或被禁用，以保证信息不被非授权用户读取或篡改。
b) 应具备打开和关闭外部通信接口的功能，自动控制器在出厂时默认外部通信接口为关闭。
c) 端口开放应遵循最小化原则，默认关闭非必需使用的端口，如：远程登录协议(Telnet)、安全外壳协议(SSH)等服务端口，对于必需使用的端口，使用后应立即关闭。
d) 应为用户分配最小必要的接口访问权限，默认关闭可直接进入自动控制器系统的特权能力或接口(如：工厂 OTA、未公开功能接口、调试后门等)，如实属业务必要，应具备鉴权机制。
e) 在初始化状态下，自动控制器网络接口应防止向未经身份验证的用户泄露非必要的安全相关信息，如配置信息、内核版本等。

f) 自动控制器应避免非必要地暴露物理接口，防止受到攻击。

g) 应保证无法通过内部和/或外部暴露的物理走线、引脚或接口等媒介获取敏感信息。

h) 自动控制器的 PCB 与信息安全相关的关键器件，不应存在用以标注芯片端口、接插件管脚、通信线路信号、测试和调试功能的可读丝印。

6.6 网络通信安全

6.6.1 网络通信部件的安全要求

设计自动控制器的软硬件时，宜采用模块化设计，网络通信部件采用接口方式与自动控制器主控部分进行软硬件分离。

自动控制器应能随时监控其网络通信的情况并取得相关网络数据。

通过网络通信方式对自动控制器进行远程操作，使用的网络通信协议应保证所传输数据的保密性、完整性、可用性，且自动控制器对于错误的指令应具有辨别的能力，对于不符合自动控制器运行逻辑的指令不予以执行。

6.6.2 访问控制

自动控制器的访问控制要求如下。

a) 对远程登录的用户具有认证功能，确保只有合法用户才能登录；自动控制器通信时应在数据传输之前进行双向认证，验证双方真实身份是否合法，检查控制权限是否与身份匹配，以防止越权或非授权控制。

b) 对远程登录的用户服务能力应覆盖高峰时期的用户访问数量。

c) 应对远程用户的访问进行访问控制管理，严格管理不同用户所能访问的数据、访问权限（读、写、执行、转发）和访问的时效性。

d) 自动控制器应根据产品类型支持不同远程操作功能，不同的远程操作功能对应不同的用户权限。

6.6.3 抗数据重放

自动控制器的抗数据重放要求如下：

a) 应能鉴别数据的新鲜性，避免历史数据的重放攻击；

b) 应能鉴别对历史数据的非正常修改，避免数据的修改重放攻击。

6.6.4 数据完整性

自动控制器应能检测重要数据在生成、传输、存储过程中完整性是否受到破坏。

6.6.5 通信安全

自动控制器的通信安全要求如下：

a) 关键安全参数和重要数据应采用非明文方式传输，保障通过远程接入网络访问时的关键安全参数的保密性；

注：关键安全参数是与安全相关的秘密信息，这些信息被泄露或被修改后会危及自动控制器的安全性。

b) 采用密码技术保障传输安全时，密码技术相关联网和安全功能模块应经过评估，并支持密码算法、组件、参数更新；

c) 在远程通信时应在数据传输之前进行双向认证，验证双方真实身份是否合法，检查控制权限是

否与身份匹配，防止越权或非授权控制，才能通过网络接口访问自动控制器；

d) 应进行用户身份认证后，才能通过网络接口修改安全相关配置参数（如权限管理、网络密钥配置、口令变更等），但 ARP、DHCP、DNS、ICMP、NTP 等网络服务协议除外；

e) 网络通信时应加密，并在会话结束时及时销毁会话密钥；

f) 远程操作会话时长应不超过一定数值，如超过时长需重新建立会话以及密钥协商；

g) 网络通信可使用滚动码或计数器机制，当请求操作计数大于其计数才准许自动控制器执行该操作指令，以防止他人通过抓包重放控制请求来对自动控制器进行非授权的控制；

h) 应默认关闭 FTP、SSH、Telnet、HTTP、ADB 等高风险管理服务或信息数据服务。

6.6.6 输入数据验证

自动控制器上的软件应验证输入数据，如：通过用户界面输入的数据、API 输入的数据或网络接口输入的数据。

6.6.7 内存清除

自动控制器应严格控制关键安全参数的存在时间和使用次数，关键安全参数及其过程信息使用完毕或超时后应立即从内存中清除。

6.7 不同工作状态的安全要求

6.7.1 通用要求

自动控制器可有不同的工作状态，如：初始化、配置、恢复出厂设置、固件更新、故障、维修、报废等。自动控制器不同的工作状态有不同的安全要求。

6.7.2 初始化

自动控制器在初始化时至少具备以下自检功能：

a) 检查安全相关自动控制器自身元器件或部件是否正常运行；

b) 检查安全相关传感元件是否正常运行；

c) 检查固件、安全机制以及安全状态，自检时发现故障，自动控制器相应功能应以安全的方式失去效用；

d) 自检时，不应出现明显的延迟，在发生电子、电气故障时，故障指示也不应出现明显的延迟；

e) 检查固件的完整性和真实性；

f) 检查固件是否有针对篡改迹象的安全机制。

6.7.3 配置

自动控制器只有在进行正确的配置后（包括但不限于网络配置、用户绑定）方可正确的实现相关功能。

自动控制器的配置状态只能在某种特定时间窗口或进行特定操作取得相应权限后方可进入，配置完成后应能自动转入正常工作状态。

6.7.4 恢复出厂设置

自动控制器恢复出厂设置要求如下：

a) 恢复出厂设置后应完全清除自动控制器中的网络数据、配置数据和个人信息，保证存储空间被

释放或重新进行配置前得到完全清除；

b） 应对不再使用的敏感个人信息和数据信息及其所有副本销毁，如因网络问题，导致信息无法同步，相关信息需在网络恢复后进行数据清除。

注：恢复出厂设置指由用户对自动控制器进行重置操作，使其恢复出厂设置。

6.7.5 固件更新

自动控制器固件更新要求如下。

a） 具备固件更新机制，更新前应取得相应的权限并确认。

b） 应对远程下载的固件更新文件的来源进行合法性认证，认证操作完成后需要建立安全通道，密文传输更新指令。

c） 应提供固件下载传输通道安全机制。

d） 应具有硬件版本对比、软件版本对比功能，以确认升级前后的版本信息符合预期。

e） 提供对固件升级文件完整性校验机制，验证更新固件的完整性和真实性。如果未确认其完整性和真实性，自动控制器应拒绝进行固件更新。

f） 应具备更新过程相关信息提示功能，含更新正常及异常相关信息提示。

g） 应确保固件升级失败后，需要有效的机制保证自动控制器处于安全状态，如自动恢复到未更新时系统版本且能正常使用，保持原有固件的可用性。

h） 应确保固件不能通过串口读取等手段被非授权用户提取出来。

i） 应具备对固件中的关键代码及重要数据进行防篡改和防逆向的功能。

j） 不应将登录用户名、口令等登录凭证明文存储在自动控制器固件中。

k） 应采用防止系统版本被降级的措施，防止原来有安全漏洞的版本被重新烧写回自动控制器。

l） 如果是电池供电，应具备在固件升级前检测设备剩余电量是否满足完成固件更新，如果剩余电量不足则应停止固件更新，并提示用户。

m） 在固件更新过程中，若自动控制器意外断电，则重新恢复供电时，应能自动恢复到固件更新前的版本并且功能正常可用。

6.7.6 故障

当自动控制器在运行过程中出现故障时，自动控制器宜根据故障等级进行故障信息的传送和提示，并对相应的故障进行基础的安全保护，必要时恢复到安全模式。

6.7.7 维修

当自动控制器出现故障时，需经用户权限许可后，自动控制器维修管理者可通过网络远程接入自动控制器并对其进行远程操作，维修管理者通过远程对自动控制器进行操作前需停止自动控制器常规操作，使自动控制器转入到维修状态方可操作。

维修替换下来的故障自动控制器，制造商应将自动控制器进行恢复出厂设置，并将其在运行期间的所有网络和数据信息以及自动控制器本体上的设置和运行数据删除。

6.7.8 报废

自动控制器进入报废阶段后，制造商应向用户提供删除相应数据的功能和方法，将运行期间的所有网络和数据信息以及自动控制器本体上的设置和运行数据删除。

6.8 在运行之前和运行过程中对可预见的安全风险进行预判和保护

6.8.1 通用要求

自动控制器应对可预见的安全风险具有预判和保护的能力。

6.8.2 对网络指令的处理

自动控制器对于正确的指令应能正常工作和应答，当接收到无效命令（包括错误顺序的命令、未知命令、错误模式下的命令、错误的命令参数）时，应能根据自动控制器目前的运行参数和运行逻辑判断其是否是有效指令，如为无效指令则自动控制器不予执行，并向远程操作者进行无效指令的反馈。

6.8.3 对系统感知数据的检查

当自动控制器使用和测量相关传感器件或外部的感知数据时，自动控制器应检查是否存在安全异常。

6.8.4 对操作中断的处理

自动控制器启动、再启动或停止等动作不应对其造成影响。自动控制器不会由于重新启动或意外动作的停止而对其自身造成损坏，也不会产生危害。

电磁干扰原因造成的自动控制器误动作，自动控制器即使发生误动作也不应引起安全问题。

自动控制器在无人监控状态下出现故障或紧急情况时，应能采取相应的安全保护措施，进行紧急处置和干预，不会对其自身造成损坏，也不会产生危害。自动控制器在发生可修复性故障时，会进入到故障保护模式，但相关人机交互、网络通信和其他一些基本的安全功能应保持。

自动控制器运行出现故障和异常时，应能进行相应处理，以避免安全问题。

6.8.5 对通信中断的处理

自动控制器的运行不依赖于外部网络，如断网或网络状况不佳时，其设计的基本功能可正常使用。

当家庭网络通信线路中断后，自动控制器应能检测到网络中断，应将当前的运行信息和未发出的数据信息及时保存，如需存储的数据信息超出自动控制器的存储容量，应保留最新的信息数据，待网络恢复正常后将相关信息数据传送出去，且该数据信息带有时间信息。

正在运转的自动控制器不会因为外部通信线路中断或故障引起安全问题，如：

a) 自动控制器需要从服务平台上获取所需的数据，并进行综合计算后方可进行对自动控制器的正确管控，但由于网络的故障导致数据无法获取，则自动控制器自身的算法应能保证其正常运行而不出现基本的安全问题；

b) 当自动控制器需要远程关闭操作，在外部通信线路中断时，在电源无法关闭的情况下仍可保持自动控制器安全。

6.8.6 对多来源操作指令的处理

当自动控制器接收来自两处及两处以上来源远程操作指令时，不应引起安全问题，可采取以下措施：

a) 检查源地址是否合法；

b) 指令的优先级和先后顺序；

c) 应用先进先出的规则；

d) 最后一条指令获胜的原则；
e) 检查指令运行逻辑的正确性；
f) 通过在新信息可能改变行为前完成来保护过程；
g) 通过停止和重启线程来保护线程；
h) 通过禁止和使能线程来保护线程。

6.8.7 人机交互的安全要求

使用语音、手势、屏幕等人机交互方式对自动控制器进行操作时，人机交互部件会有一定的交互错误率，自动控制器对于错误的指令有辨别能力，对于不符合自动控制器运行逻辑的指令不予以执行并给出警告提示。

自动控制器状态改变时，应支持本地指示或远程指示方式，指示方式应采用光学、声学或其他人体生物学中的至少一种方式。

自动控制器发生故障时，应支持本地指示或远程指示方式，指示方式应采用光学、声学或其他人体生物学中的至少一种方式，信息指示应明显。

多种人机交互方式可同时对自动控制器进行操作，自动控制器按照指令接收顺序，按照制造商规定的运行逻辑执行，如后面指令与之前指令的运行逻辑相悖，可能会造成安全风险，则自动控制器不予执行，并宜给予操作者以相应警告提示。

6.8.8 降低误操作带来的安全风险

自动控制器控制系统应在控制逻辑的设计上采取措施防止因增加远程操作引起的各种误操作，降低误操作带来的安全风险。

当自动控制器在运行过程中，短时间内可能会接收到多次相反的操作，如：ON 和 OFF，自动控制器不应出现操作逻辑上的混乱，且应根据当前状态判断是否符合操作逻辑，符合操作逻辑的才予以执行，不符合操作逻辑的不予以执行，并进行错误信息的传送和提示。

6.9 操作系统

6.9.1 集成安全

对于具备操作系统的自动控制器在进行操作系统服务裁剪时，应符合模块最小化原则，仅保留必需的模块。

6.9.2 操作系统权限控制

具备操作系统的自动控制器要求如下。

a) 对于支持多个用户账号的系统，用户权限分配应遵循最小权限原则，普通用户只拥有系统赋予的最小权限，不应越权操作。
b) 系统应具备远程控制请求的身份鉴别机制，防止非授权用户或非授权应用控制系统。
c) 系统不应预留任何未公开账号，所有账号应可被操作系统管理。
d) 不应存在绕过正常身份鉴别机制直接进入到系统的隐秘通道，如：特定接口、特定客户端、特殊URL 等。
e) 自动控制器在进行远程访问或远程应用时应设置安全的用户密码，提醒用户定期进行密码修改，密码需要有一定的复杂性、强度或长度的要求，密码最小字符长度应为 8 个字符，由大小写字母、数字、特殊符号中的两种或两种以上类型组成。

f) 用户在 1 h 内每 10 次连续输入密码不成功的，应有“禁止输入或在 30 min 后方可再输入密码”的提示。

6.9.3 操作系统安全启动认证

具备操作系统的自动控制器在进行操作系统启动时，应提供安全启动机制进行系统的完整性保护，当安全验证通过后，系统方能正常启动。

6.9.4 操作系统配置安全

对于具备调试功能的自动控制器，应限制调试进程在操作系统中的访问权限和操作权限，防止权限设置过高导致权限被滥用。

6.9.5 服务配置安全

对于具备操作系统的自动控制器要求如下。

a) 对于能安装外部应用的系统，应提供对系统 API 的访问控制功能机制，防止应用对系统接口的非授权调用。

b) 对于支持远程连接的自动控制器，其操作系统应使用安全的通信协议保障通道安全，包括具备建立通道时的身份鉴别和传输数据的机密性与完整性保护机制。

c) 对于通过 WEB 进行远程管理的自动控制器，对其进行管理和配置的行为应经过登录认证，其登录和退出过程需有日志记录。记录内容应至少包括登录使用的账号、登录是否成功、登录时间以及远程登录发起方的 IP 地址等信息。

6.9.6 内存的硬件级访问控制机制

自动控制器可具备有用于内存的硬件级访问控制机制，防止因内存缺乏访问控制而引起软件攻击，执行恶意代码，如：MMU、MPU、可执行空间保护、内存标记、可信执行环境等。

6.10 密码功能

6.10.1 密钥硬编码

自动控制器不应将用于传输加密或鉴权的密钥硬编码写在程序代码中，应采用 PSK 或通过 PSK 导出等方式生成密钥。

6.10.2 密钥生成

自动控制器的密钥生成功能要求如下：

a) 产生的非对称密钥，应满足参数的合法性检查，密钥长度等要求；

b) 产生的对称密钥，应采用多级密钥体系进行管理；

c) 产生的会话密钥，应保证每次会话的密钥不可预期，且具有对应的密钥更新机制；

d) 密钥生成后，除了非对称密钥的公钥之外其他密钥不可导出；

e) 如未采用硬件方式存储的非关键或临时性密钥，则应以加密、混淆、白盒密钥等逻辑防护措施进行存储。

自动控制器的密钥生成功能可采用硬件安全模块、安全芯片保证密钥的机密性与完整性。

6.10.3 密码运算

自动控制器的密码运算功能要求如下：

a) 密码运算应在隔离的安全环境里执行，密钥明文不出安全环境；
b) 在进行密码运算的过程中，应用进程中不应出现任何密钥数据；
c) 应采用具有足够强度的公开算法进行密码运算；

注：算法包括但不限于：SM2、SM3、SM4、SM9、AES、ECC、RSA、SHA256。

d) 采用足够长度的密钥进行密码运算，对称算法密钥不少于 128 位，RSA 算法密钥不少于 2048 位，ECC 算法密钥不少于 224 位。

6.10.4 密钥管理

自动控制器的密钥管理功能要求如下：

a) 应确定各密钥的用途，防止非授权的更改和替换；
b) 对于存储在自动控制器内的固定密钥，不应把密钥明文从高安全性的组件传送至低安全性的组件中去；
c) 会话密钥及密钥过程信息使用完毕后应立即从内存中清除；
d) 当密钥不再需要时，应将其销毁；
e) 在密钥被销毁之后，不应有任何信息可用来恢复已销毁的密钥。

6.10.5 随机数

自动控制器可具备真随机数发生器，随机数应满足 GB/T 32915 要求。

6.11 数据存储

自动控制器应采取措施确保重要数据的存储安全，要求如下：

a) 应提供安全存储功能，采取安全的方式存储重要数据，保证存储数据的完整性和真实性；
b) 应采用密码技术对重要数据实时机密性保护，确保这些数据在存储中的保密性，可提供重要数据的备份功能；
c) 敏感数据存储时应保证其机密性，采用硬件安全区域、安全模块或安全芯片等方式进行存储；
d) 在使用该自动控制器的硬编码唯一标识时，应防止通过物理、电气或软件等手段进行篡改；
e) 软件源代码中不应使用自动控制器硬编码的关键安全参数。

6.12 审计日志

自动控制器应具备对保护数据、信息操作以及安全事件的审计功能，并生成审计日志，检测到潜在的安全侵害时，应采取合适的响应机制，要求如下：

a) 审计日志应包括日期、时间、操作用户、操作类型等信息；
b) 审计日志中不应包含关键安全参数和个人敏感信息(比如用户口令等)；
c) 应能保护已存储的审计日志，以避免未授权的修改、删除、覆盖等；
d) 应有日志上传功能。

7 指示、标识和说明文件

7.1 指示和标识

自动控制器的指示和标识应满足以下要求：

a) 具备唯一网络标识，且具有逻辑或物理的安全机制保证该标识不易被修改、不易被擦除；

b) 列明在其预期配置中的所有外部接口或物理输入、输出接口列表及所支持的通信协议标识；
c) 各种对外通信接口有相对应的网络配置和网络状态指示；
d) 清晰明确地显示出硬件和软件的版本，并与提供的文档保持内容一致。

7.2 说明文件

自动控制器的说明文件要求如下：

a) 应提供自动控制器所有设计功能、安全功能和管理功能的配置说明；
b) 应提供自动控制器在配置、使用、维护、报废过程中可能会引起的安全风险以及出现安全问题的基本解决方案；
c) 应提供自动控制器在其预期配置中的所有外部接口或物理输入、输出接口列表及所支持的通信协议说明；
d) 说明文件可为纸质或电子版说明书。