ICS 13.310
CCS A 91

GDAF

广东省公共安全技术防范协会团体标准

T/GDAF 002—2021

智能家居网关安全技术要求

Security technical requirements for smart home gateway

2021－11－18 发布　　2021－11－28 实施

广东省公共安全技术防范协会　发布

GDAF

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这些专利的责任。

本文件由广东安居宝数码科技股份有限公司提出。

本文件由广东省公共安全技术防范协会归口。

本文件主要起草单位：广东安居宝数码科技股份有限公司、广东产品质量监督检验研究院、广州凯高机电有限公司、广州朔月电子科技有限公司。

本文件主要起草人：张瑞斌、夏根生、温永彩、殷平生、王标、马小康。

本文件及其所代替文件的历次版本发布情况为：

——本次为首次发布。

智能家居网关安全技术要求

1 范围

本文件规定了智能家居网关的系统和安全构成、安全等级和安全技术要求。

本文件适用于家庭或类似场所的智能家居网关的安全技术设计、开发和测试，可为智能家居网关的安全评估提供依据。本文件不适用于通常意义上具有公众通信网接入、转换和管理功能的网关。

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 4943.1—2011 信息技术设备 安全 第1部分：通用要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GA/T 681—2018 信息安全技术 网关安全技术要求

GA/T 1347—2017 信息安全技术 云存储系统安全技术要求

3 术语、定义和缩略语

3.1 术语和定义

GA/T 681—2018界定的以及下列术语和定义适用于本文件。

3.1.1

智能终端 intelligent terminal

连接到家庭内部网络的、协同提供智能家居服务的各类终端设备或部件。

3.1.2

智能家居网关 smart home gateway

位于外部网络和内部网络之间，实现外部网络和内部网络智能终端互联的设备或部件，具有智能家居系统的协议转换、数据处理、设备管理、安全管理和控制等功能。

3.1.3

智能家居系统 smart home system

综合利用互联网、物联网和人工智能等技术，实现对家庭范围内的智能终端进行控制和信息交互的智能服务系统。

3.1.4

云平台 cloud platform

对智能终端设备提供注册、管理、控制功能和智能家居服务的平台。

3.1.5

用户 user

能访问网关并对网关进行管理和维护的个人或单位，分为普通用户和管理员用户。

3.1.6

安全等级　security grade

根据网关安全功能的强度不同划分的安全级别。

3.2　缩略语

下列缩略语适用于本文件。

LAN：局域网（Local Area Network）

WLAN：无线局域网（Wireless Local Area Network）

RF：射频（Radio Frequency）

RL：基准电平（Reference Level）

IL：干扰电平（Interference Level）

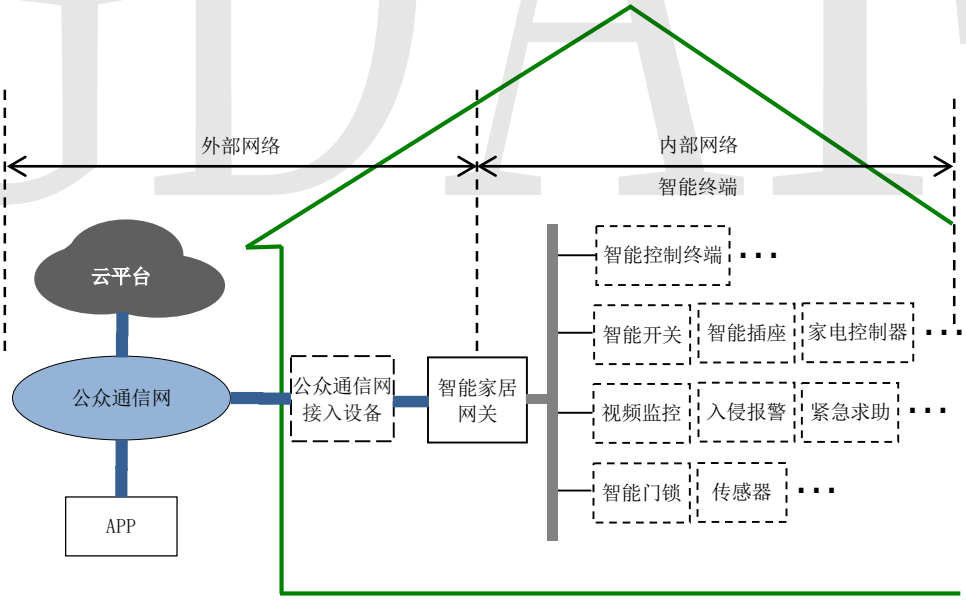
CAN：控制器局域网络(Controller Area Network)

DoS：拒绝服务(Denial of Service)

4　智能家居系统和网关安全构成

4.1　智能家居系统构成

智能家居系统主要由智能家居网关、智能终端、云平台、APP和通信网络等构成。智能家居系统的构成示意图见图1。



说明：

——网关与外部网络的连接可以是 LAN 和/或 WLAN 连接；

——网关与智能终端的连接可以是有线和或无线连接方式，如 LAN、WLAN、Zigbee、RS485 和 CAN 等的一种或多种；

——用户可通过 APP 或智能控制终端对智能家居系统进行访问、控制和管理。

图1　智能家居系统构成示意图

4.2　智能家居网关安全构成

智能家居网关的安全构成主要包括硬件安全、通信安全、数据传输安全、数据存储安全和安全管理。智能家居网关安全构成示意图见图2。

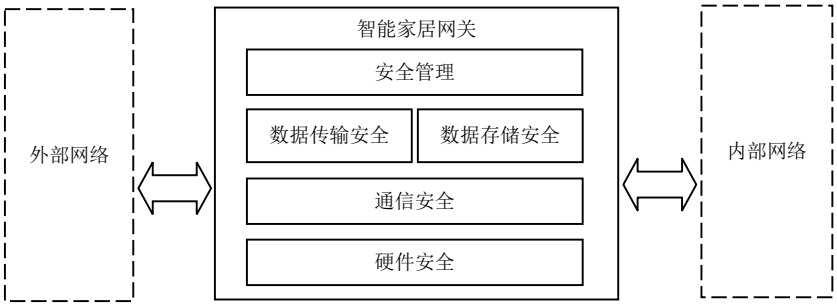


图2　智能家居网关安全构成示意图

5　安全等级

本文件按照GA/T 681—2018安全等级的级别，将安全等级划分为基本级和增强级。安全功能强弱是智能家居网关安全等级划分的具体依据。

6　安全技术要求

6.1　硬件安全

智能家居网关的硬件安全主要包括电气安全和物理防护安全，应符合表1的规定。

表1　硬件安全

序号	要求	安全等级	
		基本级	增强级
1	符合GB 4943.1-2011的相关规定	M	M
2	供电不稳或中断，不应导致发出误动作和数据丢失	M	M
3	有线输入/输出回路（若具有），满足以下安全要求： —— 一个输入/输出回路故障，不影响其它回路 —— 标识输入输出端的负载类型、容量或其它关键接入参数	M	M
4	出厂时默认关闭不必要的下载和调试端口，防止对设备的非法访问或修改	M	M
5	具有防拆检测的能力	Op	M
M = 强制　Op = 可选。			

6.2　通信安全

智能家居网关的通信安全应符合表2的规定。

表2　通信安全要求

序号	要求	安全等级	
		基本级	增强级
1	连接外部网络和内部网络的通信接口应符合相关标准要求	M	M
2	通信建立前能对访问端进行身份鉴别，防止未经授权的访问	M	M

表2　通信安全要求（续）

序号	要求	安全等级	
		基本级	增强级
3	出现会话超时，自动中断连接，并清除会话信息	M	M
4	能提供通信连接状态信息	Op	M
5	能发现来自内部和外部网络的恶意攻击，并发出本地或远程告警信息	Op	M
6	受到恶意攻击时，具有进一步的抵抗或处理机制，如： ——阻断机制 ——跳频机制，改变通信频点 ——记录该事件信息，如恶意数据的发起地址、发起时间和攻击类型等	Op	M
M = 强制　Op = 可选。			

6.3　数据传输安全

6.3.1　概述

智能家居网关的数据传输安全主要包括数据传输保护和无线链路安全。

6.3.2　数据传输保护

智能家居网关应符合表3规定的数据传输保护机制，以及相关的处理措施，确保数据的保密性、完整性、真实性和可追溯性。

表3　数据传输保护

序号	要求	安全等级	
		基本级	增强级
1	对控制指令、用户口令、生物特征和密钥等重要信息加密传输	M	M
2	关键数据在传输过程中不会意外泄密	M	M
3	采用密码算法符合国家密码管理主管部门的相关规定	Op	M
4	具有传输数据的完整性校验机制、通信延时和中断的处理机制	M	M
5	能鉴别传输数据是否被有意伪造或篡改	Op	M
6	具有抗抵赖处理机制，能证明已发送过和接收过的信息	Op	M
7	记录数据传输安全事件信息	Op	M
M = 强制　Op = 可选。			

6.3.3　无线链路安全

6.3.3.1　智能家居网关的无线工作频段和发射功耗应符合国家相关规定。

6.3.3.2　抗冲突能力

冲突率要求目的是确保智能家居网关和智能终端之间无线数据传输的可靠性，从而降低系统内不同设备之间产生干扰的概率，防止信号损坏和信息丢失。为保持尽可能低的冲突率，传输介质的占用率应符合表4所规定的条件。

表4　抗冲突要求

安全等级	最高占用率/%	时间周期/s
基本级	10	120min
增强级	10	100s

设备运行过程中应遵守相关占空比的要求。

6.3.3.3　抗干扰能力

6.3.3.3.1　抗干扰测试通用要求

抗干扰测试具备以下要求：

a) 抗干扰能力分为带外和带内抗干扰能力，是检验接收设备区分有效信号和射频干扰信号的能力；

b) 抗干扰要求适用于所有射频接收设备。而针对下述定义的所有干扰信号，均不应引发误动作或周期性的通信故障告警信息；

c) 在连续施加干扰信号的测试过程中，接收设备应能正确接收并处理所有的 20 个系统相关信息；其中，干扰信号强度的要求见 6.3.3.3.2 和 6.3.3.3.3，而上述 20 个系统相关信息是由发送设备发射的测试信息。

6.3.3.3.2　抗带外干扰

当在频率F_1和频率F_2受到表5的干扰信号干扰时，接收设备应能正常工作，测试频率F_1和F_2具备以下要求：

a) F1 = Fmin - 5%Fmin，Fmin 是设备使用频段的最低频率；F2 = Fmax + 5%Fmax，Fmax 是设备使用频段的最高频率；

b) 接收设备能够工作在多个使用频段上时，应单独测试每个使用频段。

表5　带外干扰等级

频率	干扰信号强度	
	基本级	增强级
F1 时	10 V/m	10 V/m
F2 时	10 V/m	10 V/m

6.3.3.3.3　抗带内干扰

当在测试频率Ft受到表6的干扰信号干扰时，接收设备应能正常工作，测试频率F_t具备以下要求：

d) 接收设备使用单一频率 F_w，F_t等于 F_w；

e) 接收设备使用同一使用频段中的多个频率，F_t等于$(F_{min}+F_{max})/2$，F_{min}是设备使用频段的最低频率，而 F_{max}是使用频段的最高频率；

f) 接收设备使用不同使用频段中的多个独立频率，应单独测试每个使用频段。

表6　带内干扰等级

频率	干扰信号强度	
	基本级	增强级
F_t	RL + 8 dB	10 V/m

表 6　带内干扰等级（续）

注： RL 的强度说明见附录A.1.3。

6.3.3.4　无线链路监测

6.3.3.4.1　通信故障监测

智能家居网关应与智能终端建立周期性的通信连接，通信周期应符合表7的规定，并判定是否出现通信故障。

表7　通信周期

安全等级	周期
基本级	120min
增强级	100s

6.3.3.4.2　干扰监测

若干扰信号的持续时间和强度达到足以损坏设备间正常信号传输的程度，并且持续时间超过表8规定的时间,则设备应能检测到干扰电平。干扰检测的最大持续时间和干扰信号的强度应符合表8的规定。

对于所有级别的设备，在60s的周期内干扰信号的持续时间小于5s，可不作为干扰信号。

表8　干扰检测的最大持续时间和干扰信号的强度

安全等级	干扰检测的最大持续时间	干扰信号的强度
基本级	在任何 60s 时间内，干扰信号的总持续时间达到 30 s	IL + 40bB
增强级	在任何 20s 时间内，干扰信号的总持续时间达到 10 s	IL + 9bB
注：IL 的强度说明见附录A.4.2。		

6.4　数据存储安全

智能家居网关应符合表9规定的保证数据存储安全的措施，制造商应在说明文件中说明数据存储安全的实现。

表9　数据存储安全

序号	要求	安全等级	
		基本级	增强级
1	访问数据时进行身份认证	M	M
2	重要数据加密存储	M	M
3	存储的数据（事件记录和日志文件等）不应被篡改	M	M
4	记录访问事件	M	M
5	对于部署在云平台的存储，符合GA/T 1347-2017的相关规定	Op	M
M = 强制　Op = 可选。			

6.5 安全管理

6.5.1 登录访问安全

智能家居网关的登录访问安全应符合表10的规定。

表10 访问安全要求

序号	要求	安全等级	
		基本级	增强级
1	用户必需通过身份认证才能登录网关	M	M
2	输入密码不应明文显示	M	M
3	登录后一段时间不活动，应自动注销登录状态，不活动时间可配置	M	M
4	用户必需通过身份验证才能进行重置密码操作	M	M
5	因帐户名或密码错误登录不成功的操作，不得连续超过 5 次，并且在 10min 内禁止进行下一步操作或增加额外的身份验证机制方可进行一下步操作	Op	M
6	出厂默认密码不应使用弱口令，应使用随机生成密码	Op	M
7	出厂默认密码未更改，应发出提示信息	Op	M
8	能注销长时间未使用的帐户，时间长度可设置	Op	M
9	能记录登录事件，至少应包括用户名、登录时间和日期、任何查看和修改等内容	Op	M
10	支持对异常登录行为的安全审计功能，并应发出告警信息	Op	Op
M = 强制 Op = 可选。			

6.5.2 用户权限管理

智能家居网关应支持普通用户和管理员用户两级帐户管理。用户操作权限应符合表11的规定。

表11 用户权限管理

序号	要求	安全等级	
		基本级	增强级
1	普通用户的操作权限由管理员用户授权	M	M
2	对网关和内部网络资源的访问和操作，具有访问权限控制功能	M	M
3	禁止未经授权的操作和更改	M	M
4	能发现越权操作，且相同操作达到一定次数时发出提示信息	Op	M
M = 强制 Op = 可选。			

6.5.3 设备管理

智能家居网关应符合表12规定的设备管理安全机制，确保设备的接入安全和运行安全。

表12　设备管理安全机制

序号	要求	安全等级	
		基本级	增强级
1	对网关接入云平台、终端设备接入网关的合法性进行身份验证	M	M
2	禁止直接使用设备的 ID 作为接入验证凭证	Op	M
3	已接入的设备节点发生故障或失效时，支持对其进行注销、禁用或锁定功能，并具有防止相关敏感数据可能被恶意利用的机制	Op	M
4	对于集成了其它功能的网关，非网关功能的组件出现异常时，不应影响网关功能的正常运行	Op	M
5	能记录故障信息，至少包括故障类型、故障时间和日期	Op	M
6	设备自身性能严重下降时，应产生告警信息	Op	M
7	支持对非法尝试接入行为的安全审计功能，并应发出告警信息	Op	Op
M = 强制　Op = 可选。			

6.5.4　日志管理

智能家居网关应符合表13规定的安全事件记录生成日志文件,日志内容应至少包含事件时间/日期、事件主体、事件类型、事件描述和事件结果等信息。

表13　日志管理

序号	要求	安全等级	
		基本级	增强级
1	登录和配置操作事件	M	M
2	重要信息更改事件,如用户信息、配置信息和终端设备的注册信息等	M	M
3	数据处理失败事件，如通信异常或中断导致的数据转发或处理失败	Op	M
4	恶意攻击事件，如数据重放、DoS 和无线干扰等	Op	M
5	设备状态事件，如开/关机、资源可利用率异常、故障等	Op	M
M = 强制　Op = 可选。			

6.5.5　重启和恢复

重启和恢复出厂操作应符合表14的规定。

表14　重启和恢复

序号	要求	安全等级	
		基本级	增强级
1	非授权用户不可进行重启和恢复出厂操作	M	M
2	执行恢复操作前具有风险提示信息，且用户确认后方可进行	M	M
3	执行重启操作后，用户数据、配置参数不应丢失	M	M
4	执行恢复出厂设置后，清空用户数据和配置参数	M	M
M = 强制　Op = 可选。			

6.5.6 软件升级

软件升级操作应符合表15的规定。

表15 软件升级

序号	要求	安全等级	
		基本级	增强级
1	非授权用户不可进行软件升级操作	M	M
2	操作前应具有风险提示信息，且用户确认后方可进行	M	M
3	确保用户数据和相关配置文件不受破坏	M	M
4	若设备支持自动更新软件，则应由用户决定启用、禁用或推迟更新	M	M
5	对升级包的完整性和合法性进行校验，防止升级包被篡改或替换	Op	M
6	禁止软件版本的降级更新，防止利用历史版本的BUG或安全漏洞进行攻击	Op	M
7	升级失败时，能恢复到原软件版本，并能正常工作	Op	M
M = 强制　Op = 可选。			

6.5.7 用户信息安全

智能家居网关应具有用户信息安全的保证措施，操作用户信息时应进行相关风险提示，在获得用户授权后才能操作。增强级网关还应符合GB/T 35273—2020的相关规定。

附 录 A
（规范性）
无线链路安全测试方法

A.1 通用试验要求

A.1.1 试验条件

A.1.1.1 除特别声明外，所有的测试都应使用dBm级的频谱分析仪进行测量。频谱分析仪输入端的射频信号强度应与送至天线的射频信号强度相同。测试用的所有电缆应具有相同的阻抗特性。

A.1.1.2 制造商应提供最小测试系统，主要包括智能家居网关、智能终端和配套的辅助设备/装置。

A.1.1.3 使用电池供电的设备，应确保测试过程中电量充足。

A.1.2 确定中心频率

按照附录B.1的要求布置测试设备与环境。使被测试的发射设备连续发射信号，读取频谱分析仪当前峰值为被测试设备的发射频率的中心频率。

A.1.3 确定基准电平（RL）

应确定被测接收设备的基准电平，并作为其他测试的基准。确定基准电平的步骤：

——应按照附录 B.2 的方法测量基准电平。测试应在电波暗室中进行，接收设备和发射设备之间应保持 3m 的距离；

——应使用附录 B.2 的方法，但可用适当的负载替换信号发生器；

——基准电平 RL 应测量两次，一次将天线水平放置，另一次将天线垂直放置。在进行所有其他测试时，将天线置于基准电平最小时所处的位置；

——应使接收设备处于最灵敏的状态；

——为确定基准电平，应持续增加衰减直至被测接收设备达到以下条件，使发射设备每发送 50 个测试信息，接收设备仅能收到 35～38 个测试信息。基准电平的值为频谱分析仪的观测值加 3dB。

示例：

频谱分析仪的当前观测值为：-80dBm。

基准电平的值为：RL= -80dBm + 3dB = -77dBm。

A.2 抗冲突要求试验

A.2.1 系统的冲突率应由发射设备的最大数目、单个监测信号的传输时间和监测信号发送数量的数据导出。

A.2.2 计算中所需的发射设备的最大数量应遵守制造商的规定。制造商应说明该系统是如何满足表4的冲突率要求。

A.2.3 发射设备受触发后应发出监测信息和测试信息，测试应在电波暗室进行。

A.3 抗干扰试验

A.3.1 抗干扰试验通用要求

A.3.1.1 对于高场强（场强大于1V／m）的测量环境，首先在电波暗室中建立均匀电场。

A.3.1.2 所有测试都应重复两次，一次将产生干扰信号的天线垂直放置，另一次将天线水平放置。

A.3.2 带外干扰测试

应按附录B.3的要求布置测试设备与环境。测试方法应按如下步骤进行：

——在施加干扰信号之前，应将接收设备置于基准电平的状态。降低衰减直至频谱分析仪上的观测信号电平处于 RL+20dB；

示例：

若基准电平为-77dBm，则观测值为-77dBm + 20 dB = -57dBm。

——使用信号发生器连续施加干扰信号。干扰信号为二进制序列“01010101”进行 80％的幅度调制信号。调制率 R = 1/t，单位为波特（baud），其中 t 为原始发射信号的最小信号周期；

——干扰信号的电平见表 5；

——应对接收设备使用频段中的频率 F1 和频率 F2 分别进行测试，也应对天线的不同极性分别进行测试；

——如果被测接收设备正确处理了发射设备发射的用于测试的全部 20 个信息，则通过测试。

A.3.3 带内干扰测试

应按附录B.3的要求布置测试设备与环境。测试方法应按如下步骤进行：

——在施加干扰信号之前，应将接收设备置于基准电平的状态。降低衰减直至频谱分析仪上的观测信号电平处于 RL+20dB；

示例：

若基准电平为-77dBm，则观测值为-77dBm + 20 dB = -57dBm。

——使用信号发生器连续施加干扰信号。干扰信号为二进制序列“01010101”进行 80％的幅度调制信号。调制率 R = 1/t，单位为波特（baud），其中 t 原始发射信号的最小信号周期；

——干扰信号的电平见表 6；

——对接收设备使用的每个使用频段中的频率F_t进行测试，也应对天线的不同极性分别进行测试；

——如果被测接收设备正确处理了发射设备发射的用于测试的全部 20 个信息，则通过测试。

A.4 无线链路监测试验

A.4.1 通信故障监测试验

A.4.1.1 本测试应在附录B.2所示的电波暗室中进行。

A.4.1.2 将接收设备置于基准电平状态，以接收发射设备发送的信号。然后，根据制造商的说明确认接收设备正确收到了监测信号。断开发射设备的电源连接以中止任何信号传输或者阻止信号传输。

A.4.1.3 接收设备应按照表7中的时间要求产生通信故障告警信息。

A.4.2 干扰监测试验

干扰监测测试应按如下步骤进行：

——若使用标准的发射设备，则被测接收设备应置于附录 B.3 所示的测试环境，并施加强度为 RL+20dB 的射频信号。制造商应提供测试用的改装过的发射设备（称为干扰器），干扰器使用和被

测接收设备相同的传输协议，并可连续发射信号。干扰器应使用不同的识别码，以使接收设备在正常情况下无法识别；

——对于可使用多个频率进行射频传输的设备，干扰信号在此测试中应可在多个频率中同时传输，或者与标准发射设备的发射频率序列同步；

——应按附录 B.4 的要求布置测试设备与环境。增加干扰器的干扰强度直至标准发射设备发送的 20 个报警信息中有 5 个或 5 个以上的报警信息没有被接收设备收到；

——经过频谱分析仪测量的干扰器的干扰强度称为电平 IL；

——终止标准发射设备的发射，干扰器的发射强度应按照表 8 的值进行增加；

——当下列测试步骤完成时，通过测试：

a) 干扰信号的持续时间小于 5s，不会产生任何告警信息；

b) 施加表 8 中规定强度的干扰信号，在表 8 中指定的时间内应产生告警信息；

c) 按照附录 B.5 的规定施加干扰信号，干扰信号的持续时间应符合表 A.1 的要求。

表A.1 干扰信号的持续时间

安全等级	信号的总持续时间/s
基本级	31
增强级	11

附 录 B
（规范性）
测试图例

B.1 发射设备测试配置

图B.1规定了发射设备测试配置。

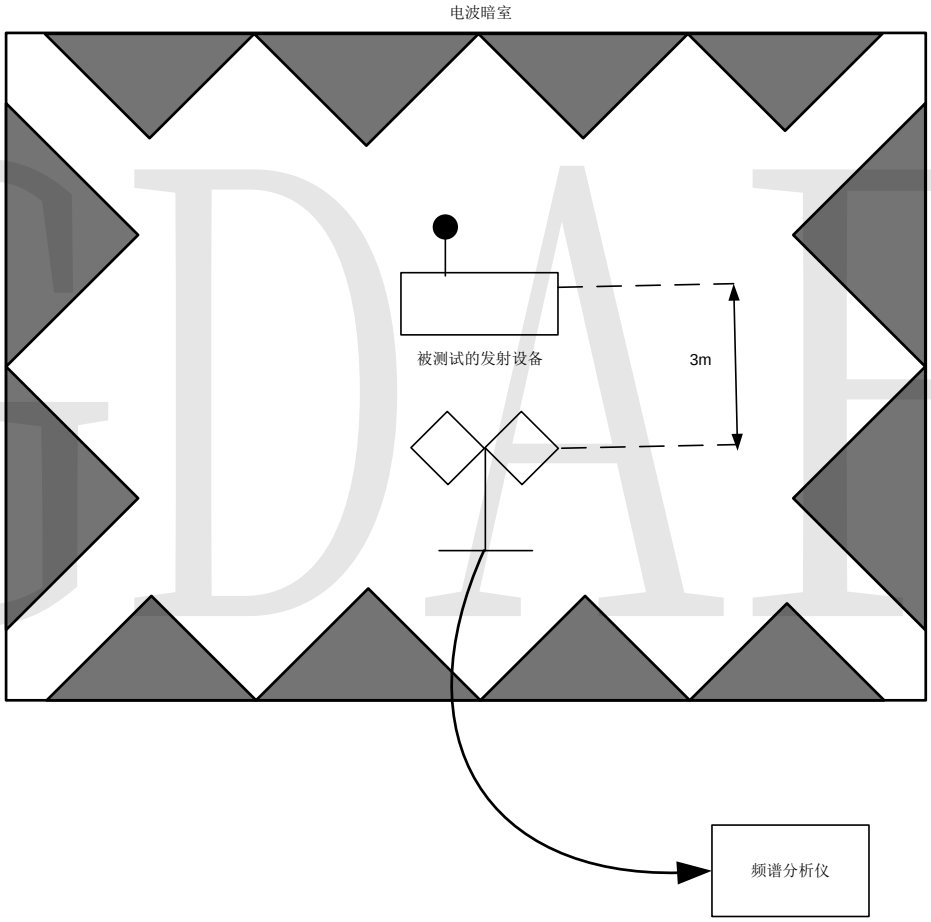


图 B.1 发射设备测试配置图

B.2　接收设备的通用测试配置

图B.2规定了接收设备的通用测试配置。

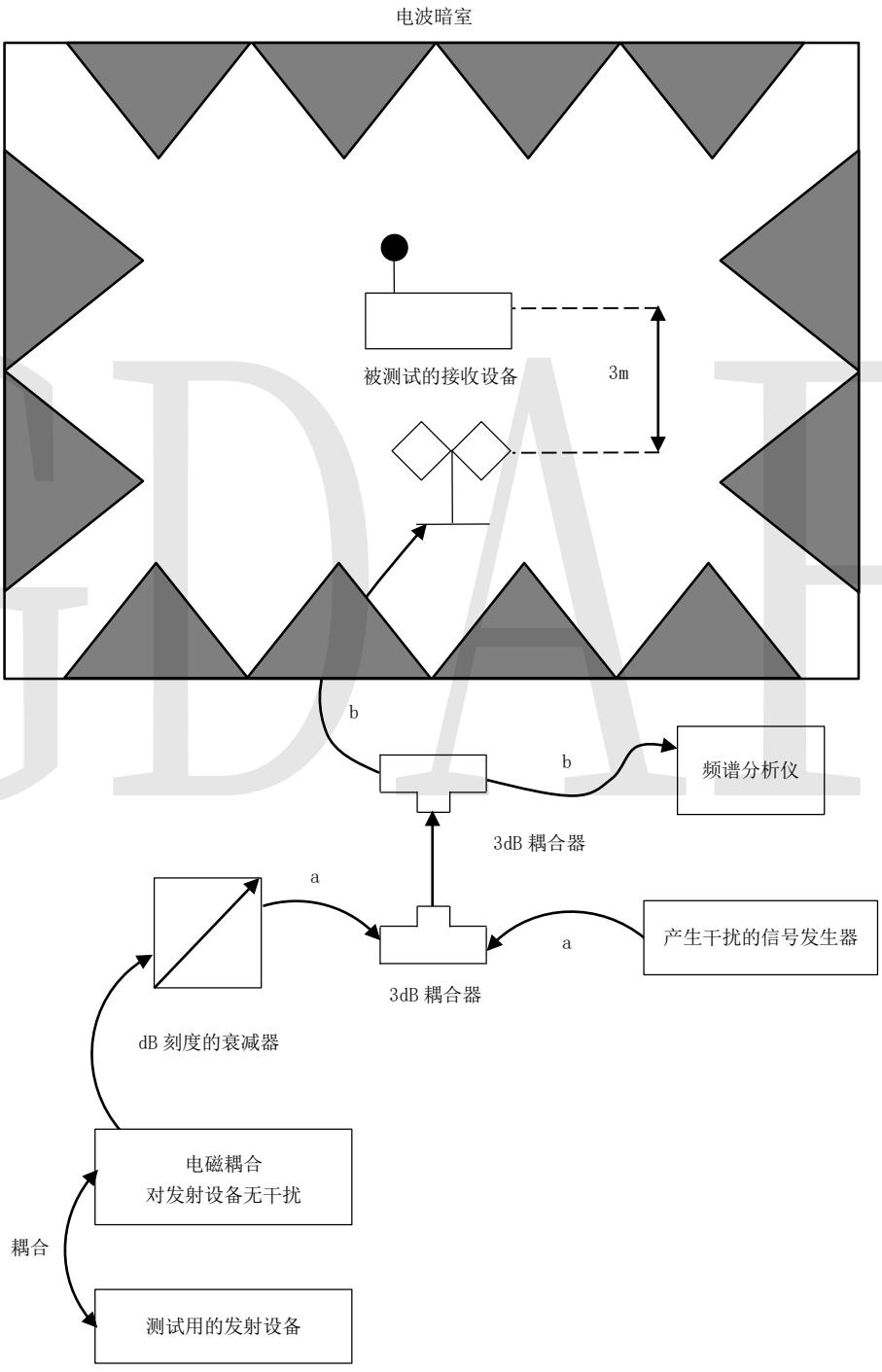


图 B.2　接收设备的通用测试配置图

B.3　干扰测试配置

图B.3规定了干扰测试配置。

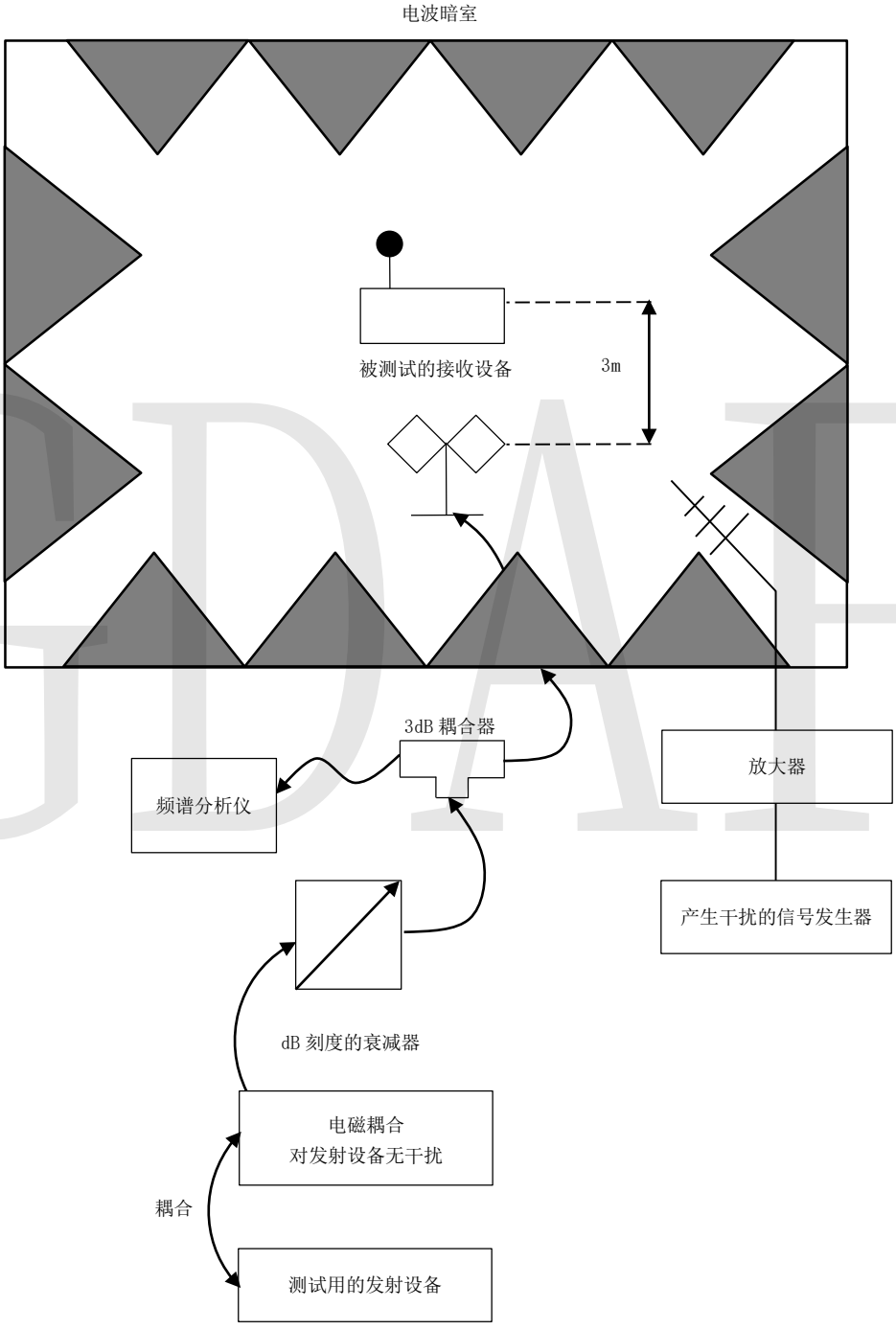


图 B.3　干扰测试配置图

B.4　干扰监测测试配置

图B.4规定了干扰监测测试配置。

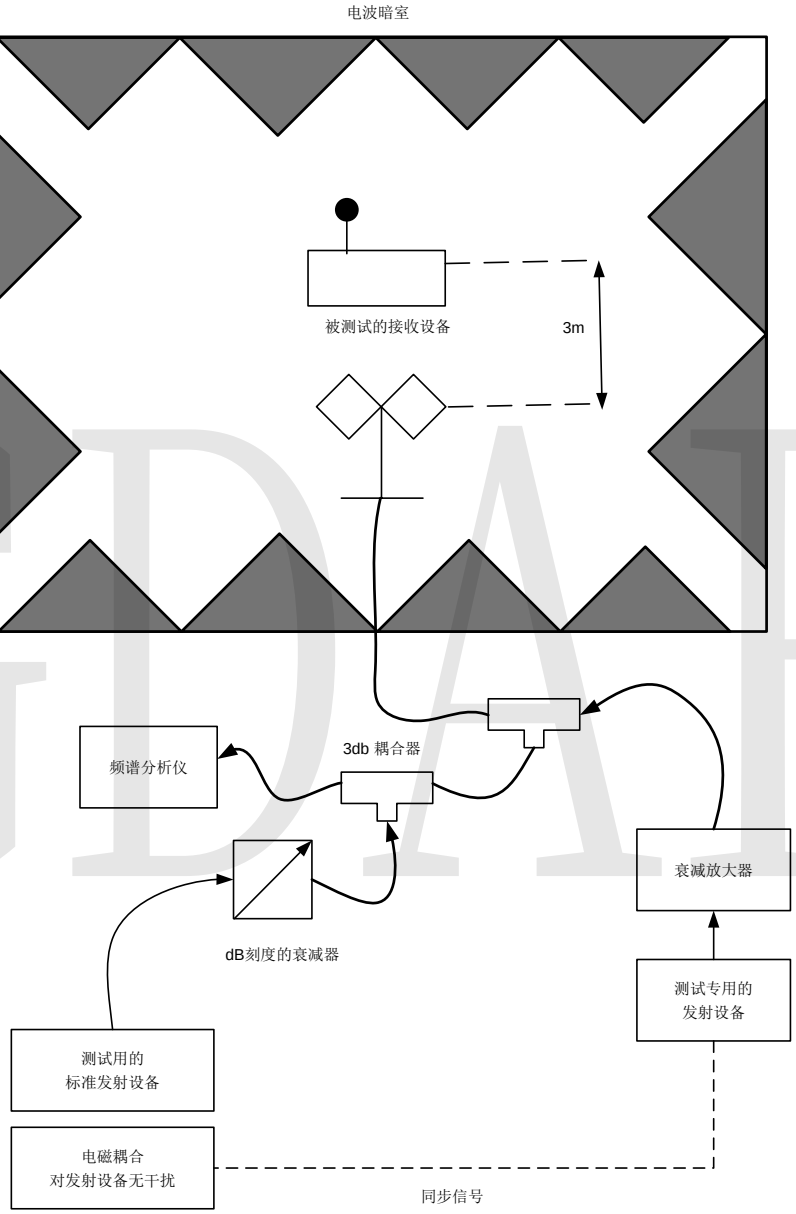


图 B.4　干扰监测测试配置图

B.5　干扰时序图

图B.5规定了干扰时序图。

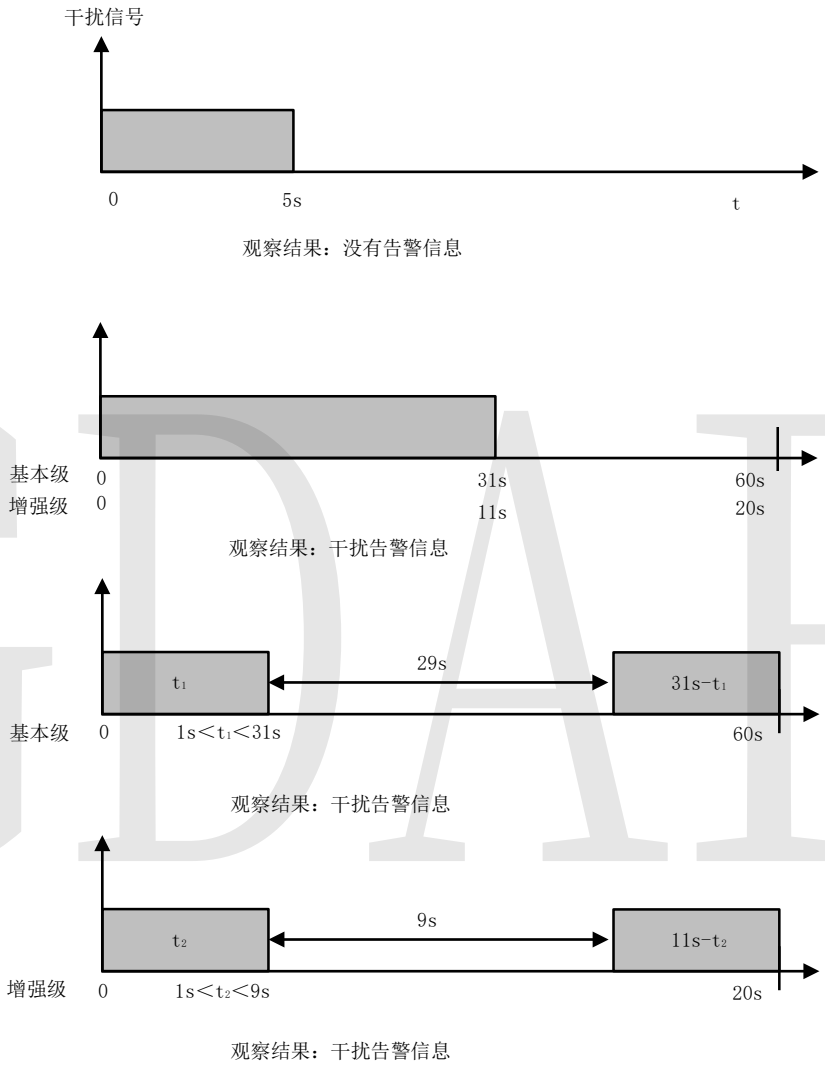


图 B.5　干扰时序图

参 考 文 献

[1] ETSI EN 303645 V2.1.1(2020-06): “CYBER;Cyber Security for Consumer Internet of Things:Baseline Requirements”

[2] GB/T 37024-2018 信息安全技术 物联网感知层网关安全技术要求

[3] GB/T 31132-2014 入侵报警系统 无线（射频）设备互联技术要求