ICS 03.100.01
CCS A02

中华人民共和国国家标准

GB/T XXXXX—XXXX/ISO 22384:2020

安全和韧性　产品和文档的真实性、完整性和可信性　保护计划的制定、监督及其实施指南

Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines to establish and monitor a protection plan and its implementation

(ISO 22384:2020, IDT)

（征求意见稿）

（本草案完成时间：2024 年 5 月）

XXXX－XX－XX 发布　　XXXX－XX－XX 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。

本文件等同采用ISO 22384:2020《安全和韧性-产品和文档的真实性、完整性和可信性-保护计划的制定、监督及其实施指南》。

本文件由全国公共安全基础标准化技术委员会（SAC/TC 351）提出并归口。

本文件起草单位：

本文件主要起草人：

引　言

由于全球经济互联程度的不断提高以及制造过程复杂化、贸易关系全球化的日益增多，进行造假、不公平贸易等导致产品受到威胁的动力及能力越来越强，被没收的品牌盗版和假冒产品数量越来越多就充分说明了这一点。为了增强韧性，制造商必须引入组织和技术方面的措施来作为保护计划的一部分，以抵御物理或数字攻击以及其他与产品相关的威胁。

为准确、有效地引入保护措施，组织宜实施系统的评估程序，根据各自的威胁选择适当的组织、技术和法律措施。市场上提供的保护措施只能解决部分问题。

要实现有效、长期的保护，就必须将各项措施合理、系统地结合起来，并进行适当的评估和实施。这个过程可以表示为一个策划-实施-检查-改进（PDCA）的循环，见图1。

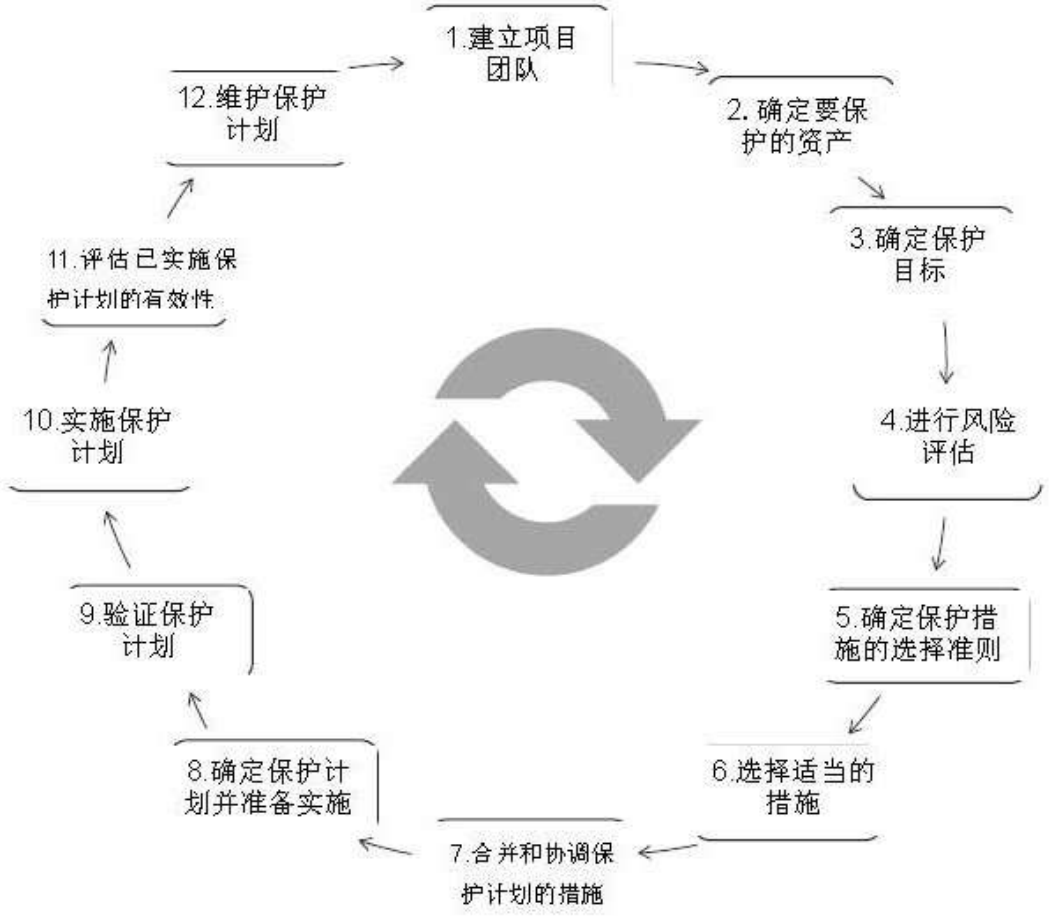


图1　实施保护计划的一般程序模型（PDCA）

与产品相关的威胁以多种方式影响着权利所有人、制造商、分销商、服务供应商和消费者。这类威胁的潜在损害包括：

— 创新领导能力损失；

— 销售减少；

— 损害声誉或品牌价值；
— 失业；
— 税收损失；
— 危害消费者的健康和安全；
— 环境问题。

安全和韧性　产品和文档的真实性、完整性和可信性　保护计划的制定、监督及其实施指南

1　范围

本文件通过制定适当的保护计划，支持其实施，并在实施后监控其有效性，为评估与产品安全有关的威胁、风险和对策提供指南。

包括考虑对诸如产品生命周期、供应链、制造、数据管理、品牌认知和成本等方面的影响和修正，从而相应地调整保护计划。

本文件适用于希望确保产品的真实性和完整性的所有类型和规模的组织，从而支持产品的可信度，包括与产品相关的文件、数据和服务。

本文件支持组织建立评估风险的程序，并选择和结合个别措施来制定产品保护计划。

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。

ISO 22300　安全和韧性 术语 （Secrity and resilience — Vocabulary）

3　术语和定义

ISO 22300 界定的以及下列术语和定义适用于本文件。

3.1

品牌　brand

无形资产，包括但不限于名称、用语、符号、形象、标识、设计或其组合，用于区分产品、服务和（或）实体，或兼而有之，能够在利益相关方意识中形成独特印象和联想，从而产生经济利益（价值）。

[来源：GB/T 39654-2020/ISO 20671:2019，3.1]

3.2

品牌盗版 brand piracy

未经品牌所有者许可擅自使用某一品牌（3.1）

3.3

假冒 counterfeiting

未经授权模仿、复制或修改资产的行为。

3.4

剽窃 plagiarism

不使用原设备制造商的品牌（3.1）而对产品进行不允许的复制，目的是为了模仿产品的特性。

3.5

保护计划 protection plan

处理资产或一组资产风险的协调措施集合。

4 概述

组织宜遵循一般程序来准备保护计划。图1中给出的模型为这种一般程序提供了一个框架。第5章中详细说明的个别步骤的设计，取决于各自的应用领域。

说明的步骤不一定必须要依次执行。这些步骤可以部分重叠，并以反复的方式执行。

5 一般程序模型

5.1 建立项目团队

组织宜将制定产品保护措施的工作作为一个项目来开展。

组织的项目小组宜选择包括来自产品生命周期所有阶段的内部相关者。项目小组可能包括以下领域的人员：

— 设计；
— 开发；
— 采购；
— 制造/装配；
— 信息技术（IT）；
— 运营技术（OT）；
— IT安全/OT安全；
—后勤；
— 销售；
— 市场营销；
— 仓储；
— 法务；
— 其他相关利益相关者。

任何外部支持宜：

— 根据问题的敏感性，在需要知道的情况下参与；
— 提供评估或评价威胁和风险的相关经验；
— 支持制定有效措施。

组织宜：

— 确定项目小组在组织中的位置（如市场营销、制造、设计、IT）；
— 任命一个小组长，负责会议时间安排和预算；
— 应用项目管理的最佳实践。

5.2 确定要保护的资产

组织宜确定哪些资产需要保护。这些资产可包括：

— 诀窍；
— 产品；
— 程序；
— 许可模式；
— 消费者的健康和安全；
— 与利益相关者的关系；
— 经营理念；

— 责任索赔；
— 形象/声誉/品牌价值。

组织宜根据其战略和任何适用的法规，在兼顾产品和市场需求的范围、以及时间框架的同时，优先考虑对资产的保护。

5.3 确定保护目标

组织宜：
— 确定和定量描述保护计划的目标；
— 在可能的情况下，提供可以定量测量的保护目标；
— 利用目标来评价保护计划的成功与否。

保护目标可以是不同性质的，可包括：
— 法律和知识产权（IP）保护；
— 遵守法规与符合标准；
— 资产完整性；
— 消费者保护；
— 声誉和竞争优势；
— 网络韧性；
— 商业及财务方面；
— 符合利益相关者的要求；
— 利益相关者遵守合约规定。

组织宜使用各种方法来识别和定义目标（如德尔菲法、设计思路）。

5.4 进行风险评估

组织宜根据附录A对与产品相关的威胁和风险进行详细评估。

注： 风险评估可以通过GB/T 27921中描述的标准化方法进行，例如SWOT分析、FMEA、平衡计分卡等方法。针对欺诈的评估，见ISO 22380。

组织宜识别并映射以下领域的威胁和风险：
— 时间（预期产品寿命）；
— 位置（生产国、分销）；
— 产品生命周期（见附录B）；
— 产品供应链（见附录C）。

5.5 确定保护措施的选择准则

组织宜在早期阶段就详细说明选择适当保护措施的标准。整套措施宜：
— 适合于达到确定的保护目标；
— 对已经存在的保护计划进行补充，允许在其实施后接受所有剩余风险；
— 观察框架条件，如可行性和可用资源；
— 从有效性和效率的角度来看是可验证的。

宜优先考虑选择准则，可包括：
— 保护要素及相关工具的采购；
— 与现有措施的兼容性；
— 遵守法规与符合标准；
— 成本；

— 进化途径（可升级性）
— 现有的参考文献；
— 对品牌声誉和认知的影响；
— 对生产和分销的影响；
— 整合限制；
— 可扩展性；
— 技术的安全稳健性；
— 技术可行性；
— 上市时间；
— 可用性；
— 风险标准和度量；

注：措施可以是组织的、技术的或法律性质的。

组织宜考虑到，安全机制的效力可能是暂时的，某些安全技术可能会过时，如加密密码套件。

5.6 选择适当的措施

组织宜为价值链上所需的每一个确定行动选择适当的措施。措施可以分为不同的类别（见表1）。措施可以特定的方式相互作用（见图2）。

表1 措施的分类

措施的类别	说明	示例
战略性	长期导向，产品工程早期，基于管理决策。 战略措施是总体保护计划的基础。	包含有价值诀窍的产品是在安全的环境中生产的（如场所、位置、地域）。 制造商努力实现高水平的垂直一体化制造，从而降低供应链的安全风险。 改变软件的零售和分销策略，从销售转为租赁产品（SaaS）。
基于产品的	实物上或数字上嵌入产品/与产品相关的措施，阻碍了： — 逆向工程； — 硬件插入； — 商业秘密的提取。	应用认证元素或利用内在属性。 芯片外壳的激光蚀刻，以隐藏制造细节。 使用定制的部件或材料来提高仿冒品的市场进入壁垒
基于流程的	保护独特或复杂的制造流程，包括供应和分销链。	在开发和制造中使用安全管理流程。 在明显独立的位置安装分布式制造，以限制工艺知识。 保护增材制造流程。 在分销过程中防止转移。
沟通方面的	有责任的披露、客户或公众沟通。	进行教育，以提高客户对高风险地区假冒分销中心的认识。 推广或传播有关伪造或网络犯罪的监管措施。 支持政府保护知识产权的举措。

表 1（续）

措施的类别	说明	示例
标记、标识、认证要素	产品或产品类型（包括其包装）完整性和真实性的证据。	产品材料采用独特、安全、不可移动的标记，以识别其来源。 机器可读的代码与认证要素相结合，使消费者能够检查真实性。 以 ISO 22383 和 ISO 16678 为指引，实施认证和识别要素。
与计算机或网络有关的（IT）	防止数据泄漏、数据提取、产品误用或数据误用。	使用带多重验证的身份和访问管理，来限制对 CAD 文件的访问。 利用硬件安全元件来对软件特性进行加密。 使用哈希算法验证固件的完整性。 持续监控网络通信，以检测异常事件或确定长期趋势。
法律方面的	基于知识产权的措施	用于创新功能的专利或实用专利。 边境查获侵犯知识产权的产品。 发起突击检查并没收制造现场的产品。

图2　措施的分类和相互作用示例

在选择适当的措施时，组织宜考虑：

— 认证特性的安全处理（见ISO 22383）；

— 在产品设计、开发和制造过程中保护敏感信息的措施（见附录B）；

— 在整个生产过程中对产品的处理；

— 相关的供应链/物流，考虑从以前/现有的攻击中获得的知识。

这些措施可包括：

— 安全要素；

— 识别（见ISO 16678）；

— 可追溯性（见ISO 16678）；

— 数据完整性；

— 包装完整性；
— 数据一致性；
— 可靠的入口点；
— 治理模式；
— 商标注册；
— 知识产权保护；
— 监管链；
— 退货分析；
— 在整个生命周期内对生产工具的控制；
— 网络监控；
— 预警系统。

5.7 合并和协调保护计划的措施

组织宜按照确定的选择准则，根据识别出的单独措施来编制保护计划。
组织宜讨论各种替代方案，并考虑、分析和记录措施之间的相互作用。
注：理想情况下，措施是相互支持的。
组织还宜处理可能的消极干扰。

5.8 确定保护计划并准备实施

组织宜明确：
— 在所有有关领域执行的项目计划，包括第5.1项中确定的所需项目资源；
— 实施每一项单个保护措施的责任；
— 控制工具（KPIs和基准）；
— 风险及可行性审查。

5.9 验证保护计划

组织宜：
— 在受控的测试环境中进行测试以验证计划；
— 根据资源的可用性和知识，利用内部利益相关者或独立第三方进行测试；
— 将测试结果与选择准则和保护目标进行比较；这可以作为未来比较评估保护计划有效性的起点（见5.11）。
组织宜对组织的相关方面进行影响评估，并在需要时对计划实施纠正措施。

5.10 实施保护计划

组织宜考虑不同类型的初次公开展出，可为：
— 在一个划定的测试市场中开始；
— 从一个划定的产品组合开始；
— 对市场或产品使用逐步推出计划；
— 即刻从所有产品和市场开始。
组织宜考虑与市场上不同保护水平的产品共存的有关问题，包括：
— 在有限或无限的过渡时期内共存；
— 召回分销产品并重新贴上标签；
— 引进新产品或新一代产品。

考虑实施方面的挑战。

组织宜对保护计划提出问题，并在出现严重偏差的情况下重新调整保护计划。

组织宜规定重新评估保护计划及其实施的时间，并考虑以下标准：

— 措施的预期有效期限；

— 成本/预算框架；

— 人力资源；

— 公司策略；

— 产品或部件的生命周期；

— 市场条件；

— 新的威胁。

5.11 评估已实施保护计划的有效性

保护措施实施后，组织应收集结果并进行检查，以确认部署的保护计划已实现第5.3节中定义的目标。

组织宜收集反馈信息，以评估保护计划的有效性，考虑：

— 市场上出现假货的证据；

— 产品的使用寿命和使用特点；

— 供应链参与者，如批发商、海关部门、专业用户或消费者；

— 第三方服务，在发现假冒或可疑产品时可以联系；

— 合适的检测方法，如通过可以进行数据交换的电子手段进行认证，设立以购物为掩护的调查或互联网监控；

— 实验室进行分析，例如检验可疑或仅仅只是退货的物品；

— 数据分析和统计方法的运用。

组织已检查成本效益比，并根据结果调整保护计划。

5.12 维护保护计划

组织宜：

— 确定是否需要变更保护计划；

— 按照迭代原理重新设计保护计划，如PDCA；

— 以原保护计划为改进的基础。

如以下方面发生变化，宜改进保护计划：

— 分销伙伴、部门或地区；

— 供应商；

— 市场监管；

— 技术规范。

附 录 A
（资料性）
与产品相关的常见威胁和风险

A.1 一般风险因素

宜考虑以下与产品相关的威胁和风险等：

— 对产品和技术的威胁；
— 对商业模式的威胁；
— 目前实施的对策，包括实施现状和效率测试；
— 整体公司策略；
— 整体品牌战略；
— 生产和后勤方面的威胁；
— 市场的变化；
— 已经出现的仿冒品及其造成的损害；
— 对研究或企业诀窍的威胁
— 供应商的可信度；
— 客户状况；
— 竞争形势。

例1：项目团队成员与公司内所有相关的利益相关者[研发（R&D）、制造、销售、供应、服务、IT]的员工进行访谈，以获得与造假相关之威胁、弱点、优势和机会的概况。这些访谈可以由包含相关项目的检查清单来支持。

例2：造假方面的个人威胁包括：

— 逆向工程；
— 制造工艺过程的限制；
— 侵犯知识产权，如设计抄袭、品牌复制；
— 自行生产的产品侵犯第三方产权；
— 第三方；
— 诀窍被（前）员工、客户、供应商外流；
— 披露要求和专利说明书的使用；
— 工业和经济间谍活动；
— 供应链中的信息外流；
— 非法干预供应链；
— 对产品相关服务的网络攻击；
— 身份盗用和未经授权的访问。

A.2 产品欺诈的类型

GB/T XXXX (ISO 22380:2018)第4.3节表3给出了产品欺诈一些类型的概述。考虑以下类型：

— 假冒；
— 侵犯知识产权；
— 掺杂物质；
— 篡改；
— 替代；
— 模仿；

— 转移；
— 盗窃；
— 超限运转；
— 许可滥用。

每个案例中，有一些成分或声明是虚假的。它代表了公共健康的弱点，也代表了欺诈者的利益。

A.3 信息泄露与诀窍外流

威胁产品或商业诀窍的方面可包括：
— 工业间谍活动；
— 诱惑员工；
— 披露要求和专利说明书；
— 商业秘密的泄露。

A.4 逆向工程

危及植入系统竞争优势、研发和非专利产品特性的方面可包括：
— 固件提取；
— 加密数据提取；
— PCB布局扫描和电路提取；
— 产品折毁；
— 功能系统分析；
— 对硬件和软件的操作。

A.5 网络安全

有关网络安全的各方面与机密性、完整性或资产或相关数据的可用性有关。可包括：
— 窃取或接触公司机密；
— 插入恶意软件；
— 未经授权插入硬件；
— 身份盗用；
— 越权访问。

附 录 B
（资料性）
产品生命周期一览

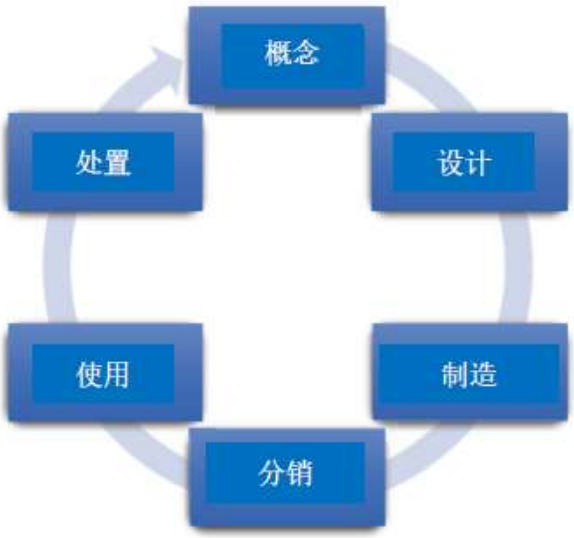
B.1 总则

保护措施的应用与产品的生命周期阶段有关。组织应识别和映射产品生命周期各阶段的威胁。这些阶段为：

— 概念阶段；
— 设计阶段；
— 制造阶段；
— 分销阶段；
— 使用阶段；
— 处置阶段。

如GB/T XXXX（ISO 22380）所述，在产品生命周期的早期阶段，未处理的威胁和风险会对产品的完整性及其相关经营者产生重大的负面影响。因此，应在概念和设计阶段整合缓解措施，以遵循ISO 22383中给出的“设计安全”原则。

图B.1和表B.1描述了产品生命周期的各个阶段。



图B.1 产品生命周期阶段

表B.1 产品生命周期及相关威胁

产品生命周期阶段	说明	威胁示例
概念阶段	基于技术和经济可行性，搜索和选择有前景的产品理念，并适合企业战略和客户需求。 选择思路之后是概念的开发，这个概念已经定义了产品设计和预期寿命的最初想法，包括所有即将到来的阶段（制造、分销等）。	攻击者可以实际进出研发会议室，并安装监控设备以记录所有信息。 猎头公司从中级管理层挖走技术熟练的员工。 攻击者使用鱼叉式网络钓鱼邮件在研发工作站安装木马。
设计阶段	从产品描述（并非生产工艺描述）的详细阐述到产品生产阶段的所有活动，包括几何模型、电气/电子平面布置、软件、图纸、零件清单等，包括全面发布相关文件。 注：在智能制造中，特定订单的产品设计流程占主导地位。设计和施工过程取决于客户设定的要求以及与客户的协作。	CAD 设计数据或原型的盗用。 在贸易展销会上拍摄原型的照片。
制造阶段	产品的创造，主要通过内部制造以及内部和供应组件的装配。结果是经过测试和批准的产品，包括其产品文档。	恶意供应商或客户将信息传递给竞争对手。
分销阶段	为有需要的客户或企业用户提供产品或服务的过程。此过程可以由生产者或服务提供者直接完成，也可以通过与分销商或中间商的间接渠道完成。	竞争对手将仿冒品偷运到合法的分销渠道。 官方经销商积极地重新分销仿冒品。 分销商将来自不同厂家的相同货号的产品混合在一起。
使用阶段	支持产品在预期环境中的操作或使用的过程。这意味着产品的服务/维护，以确保在发生故障时，功能状态得到维护或恢复。应考虑保养、检查、修理和改进等基本措施。 此外，如果产品长期使用（如机器），可以进行翻新（重新设计）。翻新是指以用户友好的方式使已使用的产品适应当前的技术水平或新的客户要求。	竞争对手对产品的软件进行逆向工程，并根据自己的目的重用源代码。 客户利用支持信息鼓励已知的仿冒者获得该产品的第二源。
处置阶段	部分或完全将产品拆卸为其组件或个别部件（退役），包括断开和分离所有操作材料（如润滑油、燃料），再利用或转售可用部件并回收利用，或处置不再使用的部件。	攻击者购买坏掉的产品，然后把它们的电子部件放在假冒包装内作为新的原始备件转售。

附 录 C
（资料性）
供应链一览

恶意供应商、分销商和服务商对产品的可信度和诚信有很大的影响。这种影响在物联网（IoT）和工业4.0的网络产品中更为明显。

从制造商的中心观点来看，制造商总是处于中间位置。供应商提供初步的产品、组件、软件或服务。用户使用或操作制造出的产品。供应链全貌参见图C.1。

图C.1 供应链全貌

组织宜确定供应商必须满足的标准，例如在其采购条款方面。标准可为：

— 支持终止（EOS）；
— 可打补丁；
— 产品或公司的符合性声明，如自我声明、证书、审核结果。

组织宜就如何证明其产品和零配件的真实性和完整性向顾客提供建议。可通过以下途径提出建议：

— 操作说明；
— 公司网站上的突出区域；
— 定制应用程序；
— 客户时事通讯。

参 考 文 献

[1] ISO 16678, Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade

[2] GB/T 39654-2020/ISO 20671:2019, 品牌评价 原则与基础

[3] ISO 22380:2018, Security and resilience — Authenticity, integrity and trust for products and documents — General principles for product fraud risk and countermeasures

[4] ISO 22381, Security and resilience — Authenticity, integrity and trust for products and documents — Guidelines for establishing interoperability among object identification systems to deter counterfeiting and illicit trade

[5] ISO 22383, Security and resilience — Authenticity, integrity and trust for products and documents —Guidelines for the selection and performance evaluation of authentication solutions for material goods

[6] ISO 28000:2007, Specification for security management systems for the supply chain

[7] GB/T 27921 风险管理 风险评估技术