ICS 49.020
V 00

中华人民共和国国家标准

GB/T 38931—2020

民用轻小型无人机系统安全性通用要求

General requirements for safety of civil small and light unmanned aircraft system

2020-07-21 发布　　2021-02-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国航空器标准化技术委员会(SAC/TC 435)提出并归口。

本标准起草单位:中国航空综合技术研究所、中航金城无人系统有限公司、西北工业大学、南京航空航天大学、中国航空工业集团公司西安飞行自动控制研究所、易瓦特科技股份公司。

本标准主要起草人:舒振杰、胡应东、胡永红、罗伟、曹国杰、王亮、张小林、何志凯、张锐、王昂、罗秋凤、王琳、禹科、唐强、孟宪锋、赵国成、叶川。

民用轻小型无人机系统安全性通用要求

1 范围

本标准规定了民用轻小型无人机系统全生命周期内安全性工作的一般要求、详细要求和安全性验证。

本标准适用于最大起飞重量在0.25 kg～150 kg之间的民用无人机系统(以下简称“无人机系统”)的研制、生产、试验和使用的安全性工作。其他民用无人机系统可参考使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是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 15236—2008 职业安全卫生术语

GB/T 30174—2013 机械安全 术语

GB/T 35018 民用无人驾驶航空器系统分类及分级

GB/T 38152 无人驾驶航空器系统术语

3 术语和定义

GB/T 15236—2008、GB/T 30174—2013、GB/T 38152和GB/T 35018界定的以及下列术语和定义适用于本文件。为了便于使用,以下重复列出了GB/T 15236—2008、GB/T 30174—2013中的某些术语和定义。

3.1

事故 accident

造成死亡、疾病、伤害、损伤或其他损失的意外情况。

[GB/T 15236—2008,定义3.1]

3.2

危险 hazard

潜在的伤害源。

[GB/T 30174—2013,定义2.6]

3.3

安全性 safety

产品所具有的不导致人员伤亡、系统毁坏、重大财产损失或不危及人员健康和环境的能力。

3.4

安全性指标 safety index

每飞行小时发生严重飞行事故的概率。

3.5

风险 risk

伤害发生的概率与伤害严重程度的组合。

[GB/T 30174—2013,定义 2.11]

3.6

危险可能性　hazard probability

某种危险发生的可能性。

3.7

危险严重性　hazard severity

某种危险可能引起的事故后果的严重程度。

3.8

安全性关键项目　safety critical item

对产品安全性有重大影响的项目,通常包括功能、硬件、软件、操作规程和信息等。

4　一般要求

4.1　工作目标

在无人机系统全生命周期内,综合权衡性能、进度和费用,将系统的风险控制到可接受水平。必要时,确定无人机的安全性指标,并在任务书中予以确认。

4.2　基本原则

无人机安全性要求的基本原则应包括:

a)　在充分分析和研究的基础上,安全性要求应合理、科学、可实现并可验;

b)　遵循预防为主、早期投入的指导方针,无人机安全性工作宜从方案论证阶段开始,以降低系统中危险的数量及其风险,通过及时、有效、经济的方式将安全性综合到产品设计中去;

c)　在系统研制阶段,安全性工作应纳入系统的研制工作,并根据系统特点和安全性要求,对安全性工作进行统筹策划,确保协调开展;

d)　无人机系统安全性应从设计制造、质量控制、可靠性、维修性、人-机-环境系统工程、健康保障、经济性等因素综合协调,确保安全技术措施的实施;

e)　当安全性技术措施与其他因素发生矛盾时,应优先保证安全技术措施的落实。

4.3　工作过程

4.3.1　策划与管理

围绕无人机系统的安全性要求,策划全生命周期中所需要开展的安全性工作,并规定在安全性工作计划等文件中。以文件为依据,组织、协调、实施和管理系统的安全性工作。

4.3.2　危险识别

无人机系统安全性关键项目包含:无人机飞行平台(任务载荷)、地面控制站等。安全性定性要求和指标分解到规定的产品层次,作为产品研制单位规划安全性工作和提出外协、外购产品安全性要求的依据。

依据历史事故信息与相似产品经验教训,采用相应的技术方法(如初步危险表、故障模式、影响及危害性分析、故障树分析等),综合考虑硬件、软件、环境及使用与维修规程等因素,识别系统在全生命周期中所有可能存在的危险。

4.3.3　危险分析和风险评价

4.3.3.1　危险分析

分析每个危险的发生原因、发生可能性及后果,并确定其危险可能性和危险严重性。

4.3.3.2 危险严重性

定性的危险严重性等级划分及定义可参考表1。

表1 危险严重性等级划分

等级	程度	定 义
Ⅰ	灾难的	人员伤亡、设备完全损毁或报废、严重的不可逆的环境破坏
Ⅱ	严重的	人员严重伤害、设备严重损坏、较严重但可逆的环境破坏
Ⅲ	轻度的	人员轻度伤害、设备或环境轻度破坏
Ⅳ	轻微的	轻于Ⅲ级的人员伤害、设备或环境破坏

4.3.3.3 危险可能性

定性的危险可能性等级划分可参考表2。

表2 危险可能性等级划分

等级	说明	产品个体	设备总体
A	经常	可能经常发生	连续发生
B	很可能	可能发生若干次	经常发生
C	偶然	可能偶尔发生	发生若干次
D	很少	很少发生,但有可能	很少发生,但有理由预期可能发生
E	极少	极少发生,可认为不会发生	极少发生,有理由认为几乎不可能发生

4.3.3.4 风险评价

从危险可能性和危险严重性两方面,综合评价危险的风险水平。评价可采用定性或定量的方法,本标准给出定性的风险指数评价法作为参考,风险指数越大代表风险越低,确定风险指数的参考示例见表3。

表3 危险的风险指数参考示例

危险可能性等级	危险严重性等级			
	Ⅰ	Ⅱ	Ⅲ	Ⅳ
A	1	3	7	13
B	2	5	9	16
C	4	6	11	18
D	8	10	14	19
E	12	15	17	20

4.3.4 消除危险或减少风险

根据风险分析和评价的结果，通过在系统研制过程中有重点、有针对性、持续地采取安全性设计措施，消除危险或降低风险。采取安全性措施的优先次序宜为：

a) 最小风险设计：首先在设计上消除危险，若不能消除已判定的危险，应通过设计方案的选择将其风险降低到可接受水平；
b) 采用安全装置：采用永久性的、自动的或其他安全防护装置，使风险减少到可接受水平，并且应规定对安全装置作定期的性能检查；
c) 采用告警装置：采用告警装置来标示或检测危险，并向有关人员发出适当的告警信号，告警标记或信号应明显，并满足标准化要求，以减少人员对信号做出错误反应的可能性；
d) 制定专用规程：制定保证设备安全操作的专用规程；
e) 相关人员培训：对从事产品安全相关工作的人员，应进行培训。

对于危险严重性等级为Ⅰ级和Ⅱ级的危险（见 4.3.3.2），应根据使用需求，采取一种或多种组合的提醒方法以减少风险。

4.3.5 安全性要求验证

选择合适的方式（试验、演示、分析等），验证设备对安全性要求的满足情况。

4.3.6 安全性水平评价

综合安全性设计、分析与验证的结果，评价系统的安全性水平。

4.3.7 危险跟踪

在系统生命周期内建立并运行危险跟踪系统，建立危险清单，对每个危险、危险严重性及可能性、危险原因、所采取的控制措施、验证方法及结论、危险消除或风险减低措施及残余风险等进行记录、管理和控制，并提出评估要求。

5 详细要求

5.1 安全性要求分解

应考虑实施任务的不同，采用适当的指标分解策略，将安全性要求和定量指标分解到规定的产品层次，作为产品安全性工作和提出外协、外购产品安全性要求的依据。

5.2 初步危险分析

初步危险分析工作应包括：

a) 应考虑无人机发射方式、回收方式、控制方式和任务载荷的不同，根据设计方案，初步识别具有危险特性的功能、产品、材料以及与环境有关的危险因素等，分析可能发生的危险，编制初步危险表。
b) 针对初步危险表，开展初步危险分析。通过分析每项危险的危险严重性和危险可能性，应用风险指数评价法（见 4.3.3.4）或其他方法，初步评价风险，并提出安全性管理和控制措施，以便在方案的选择和权衡中考虑安全性问题。
c) 在系统全生命周期，应结合研制或使用进展更新初步危险分析，以确保全面识别设计中存在的危险。
d) 初步危险分析的结果应作为确定安全性关键项目和制定安全性设计准则的依据。

e) 应对初步危险分析的过程和结果进行记录。

5.3 安全性设计准则制定

制定并贯彻安全性设计准则，以指导设计人员开展安全性设计，应包括如下要求：

a) 应分析设计要求、分系统/设备任务书、系统接口要求说明书或其他相关文件，确保全面、正确地制定安全性设计准则。

b) 应总结相似系统的工程经验和事故教训，并根据系统特点以及相关规章、条例、标准、规范、文件或要求以及初步危险分析的结果，制定安全性设计准则，作为本系统应满足的安全性设计要求。安全性设计准则应纳入规范或设计文件之中，供设计人员在设计中贯彻。

c) 应检查安全性设计准则的执行情况，编制安全性设计准则符合性报告，作为安全性评审的重要内容。

5.4 系统危险分析

在初步危险分析的基础上，随着设备研制进展，进一步全面、系统地识别、评价和消除或控制可能存在的危险，提高设备的安全性，应包括如下要求：

a) 系统危险分析的结果应作为制定安全性关键项目清单的依据，并进行记录。

b) 应随着设备研制的逐步具体与细化，在初步危险分析的基础上，进一步识别可能由产品故障或功能异常、能源、环境因素、人为差错、接口等导致的危险，制定详细的危险清单。

c) 应针对设备详细设计和细化后的危险清单，在确认初步危险分析所制定安全性措施的有效性和充分性的基础上，应用风险指数评价法(见 4.3.3.4)或其他方法，对危险进行风险评价，对不可接受的危险，提出设计改进或使用补偿的措施。

d) 系统危险分析应在设备各层次(如系统、分系统、部件、组件等)全面展开，并在研制阶段迭代进行，直到确认系统的危险均得到消除或风险降低到可接受水平，安全性要求得到满足。

e) 系统危险分析应重点考虑以下方面：

1) 应重点针对飞行器平台和测控部分，考虑与规定的安全性设计要求或设计准则的符合程度；

2) 分析独立失效、关联失效或同时发生的危险事件，主要包括人为差错、单点故障、系统故障、安全装置故障及产品间相互作用导致的危险或增加的风险；

3) 软件的正常工作、故障和其他异常情况对安全性的影响；

4) 为实现产品要求所采取的设计更改对安全性的影响(如：是否降低安全性水平、引入新危险等)；

5) 低层次产品危险对高层次产品安全性的影响及其控制措施。

5.5 试验的安全

确保在各种试验中考虑了安全性问题，向试验人员提供安全性分析报告和其他安全性资料，保证受试产品满足实验室和试验场所的安全性要求，应包括如下要求：

a) 试验前，应结合试验条件(试验环境、参试设备及其状态等)，进一步识别试验中可能发生的危险。

b) 首飞试验前应开展安全检查和评审。

c) 在产品试验中应考虑如下因素：

1) 规划与试验有关的危险分析、风险评价以及对试验计划和规程等的审批程序，确保对整个

试验过程都考虑了安全问题；

2） 危险分析应包括参试设备及其安装调试、检测仪器等；

3） 与负责试验安全的人员进行协调与沟通，对受试产品的状态进行确认，确保对试验提出的安全要求得到了落实；

4） 应明确实验室或试验场地的特殊安全要求，并对试验中发现的与设备安全性有关的问题进行分析和跟踪管理。

5.6 使用与保障危险分析

识别由环境、人员、设备、使用与保障等造成的危险，评价用于消除、控制或降低风险措施的充分性和有效性，应包括如下要求：

a） 识别并评价由人员操作、执行任务或实施保障导致的危险，分析中应考虑各阶段的设备状态、设施间接口、设定的环境（或区域）、保障工具或其他专用设备等，并重点考虑软件控制的测试设备、使用或任务次序、并行工作的效果与限制、人的生理因素、意外事件的影响、人为差错等导致的危险。

b） 分析工作应确定以下内容：

1） 需在危险环境下完成的工作内容、工作时间及将其风险降到最低所需的措施；

2） 为消除、控制或降低相关危险，对设备软硬件、设施、工具及试验设备在功能或设计要求方面进行的更改；

3） 警告、告警或专门的应急规程；

4） 安全性培训和人员资格的要求；

5） 与其他系统部件或分系统相关联的非研制硬件和软件的影响；

6） 操作人员可控制的危险状态。

c） 应在产品外包装显著位置及产品说明书中提示依法依规飞行，警示飞行风险，并在机体标注无人机类别。

d） 应按相关法规或合同规定的准则，提出消除危险或将风险降低到可接受水平所需的安全性措施。

e） 应对设备生产、安装、试验、使用、维修、服务、运输、贮存、改进和报废处理等工作规程进行安全评价并记录成文。

f） 当系统设计或使用规程发生更改时，应更新使用和保障危险分析。

g） 使用和保障危险分析的结果应作为制定安全性关键项目清单的依据。

h） 应对使用和保障危险分析的过程和结果进行记录，为制定安全的设备使用和保障规程提供依据。

6 安全性验证

验证系统安全性是否达到了规定的安全性要求，同时对采取的安全性措施的有效性和充分性进行确认，应包括如下工作要点：

a） 应通过试验、演示、仿真、分析、设计评审等方法，验证设备是否符合安全性要求；

b） 应评审验证（包括设计验证、使用评价、技术资料验证、生产验收、贮存寿命验证）计划、验证规程和结果，以确保充分验证了设备的安全性；

c） 对于采用安全装置、告警装置及特殊规程来控制危险的项目，应通过专门的安全性试验来验证

措施的有效性；

d) 对于较复杂的无人机系统，可通过选择低层次产品的试验和高层次产品的综合分析相结合的方式来实施安全性验证；

e) 安全性验证工作应尽可能与产品研制过程中的其他验证工作协调进行，如需通过产品可靠性来保证其安全性，则应按可靠性验证要求进行验证；

f) 安全性验证工作应在系统集成过程中，在不同层级开展。