

**无人机系统的网络安全风险评估**陈忠德

**引用这个版本：**

陈忠德。无人机系统的网络安全风险评估。自动的格勒诺布尔阿尔卑斯大学[2020-…]，2021年。英语NNT:2021GRALT004。电话：03200719v2

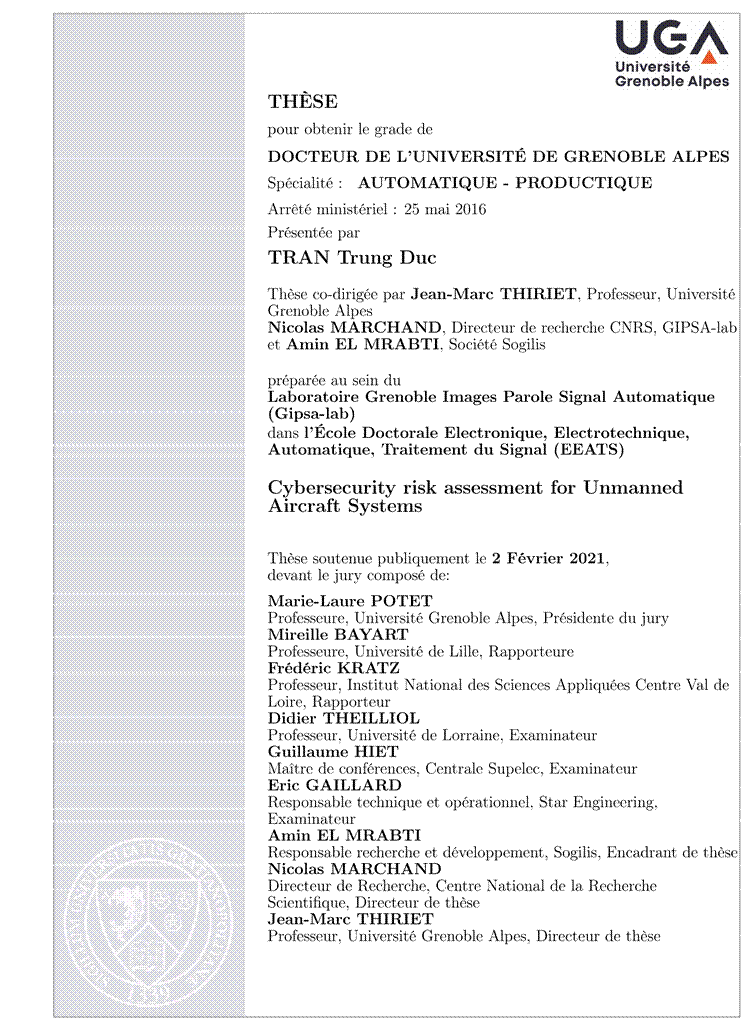
**HAL Id:电话-03200719**

https://hal.archives-ouvertes.fr/tel-03200719v2

2021年6月1日提交

**哈尔**是一个多学科的开放存取档案库，用于存放和传播科学研究文件，无论这些文件是否已出版。这些文件可能来自法国或国外的教学和研究机构，也可能来自公共或私人研究中心。

“档案馆”是一个多学科的机构，它的目的是传播研究所、公共机构和私人实验室的科学文献。



|  |
| --- |
|  |
|  |  |

Résumé-Aujourd&apos;hui，无人机系统（UAS）组成部分的名称羊角面包是网络安全问题公共领域的灵魂。在这一点上，我们需要为解决阿联酋发展问题的方法学发展提出合理的建议。这是我最喜欢的地方。塞特·塞斯提议两份重要的捐款。这是联合国现存网络安全体系（ou conçu）上的方法学中心。Cette méthodologie fournitál&apos;Usilizate联合国“工作流程”倾注分析仪，标识符les scénarios d&apos;Attaches Possibiles and les contre Measures Appripries。我们出现了“东方网络安全体系危机的手势”这一说法。第二种方法是在运营中心进行的，即在系统概念初始阶段完成网络安全问题。Cette méthodologie aétéconçue comme e versionétendue de la méthodologie“特定运营风险评估”（SORA）。C.Couix&apos;Suffik Paulle FaTeKa La SoRa。在塞雷特的集中统一和网络安全的无知中，没有任何模块的扩展，无法实现对人类的补偿。巴黎圣母院“对科学和网络科学的理性科学研究的评估”（英语版，SORA-C2S）。在方法学的基础上，我们的雅芳建筑在网络上提供了一个辅助工具，用于半自动地评估婚姻关系和网络安全的两个方面。在Gipsa-lab实验室和社会研究中心的合作干部培训课程中。

格言：网络居里、风险评估、无人机系统、索拉、猫腻。



GIPSA实验室，数学街11号

38400，法国圣马丁·德希尔



摘要-如今，越来越多的无人驾驶飞机系统（UAS）操作引起了公众对网络安全问题的关注。因此，在UAS开发过程中需要解决这些问题的方法。这是我们研究的重点。本论文有两个重要贡献。首先，我们提出了一种以系统为中心的方法来加强现有（或设计的）无人机的网络安全。该方法为用户提供了分析UAS、确定可能的攻击场景和确定适当对策的工作流。我们将此方法称为“系统网络安全风险管理”。其次，我们提出了一种以操作为中心的方法，在UAS开发的早期阶段（在UAS设计之前）考虑网络安全问题。该方法是特定操作风险评估方法（SORA）的扩展版本。SORA是一种广为人知的评估“特定”类别下无人机操作风险的方法。然而，SORA方法的当前阶段只关注安全，而忽视网络安全。我们的扩展模块完成了这个缺失的部分。我们将扩展方法称为安全和网络安全的特定操作风险评估（SORA-C2S）。基于此方法，我们构建了一个基于web的工具，帮助用户半自动执行风险评估。本论文是SOGILIS公司与GIPSA实验室合作的一部分。

关键词：网络安全、风险评估、无人机系统、SORA、特定类别。



GIPSA实验室，数学街11号

38400，法国圣马丁·德希尔

目录

导言1

1        无人机系统和相关网络安全问题3

1.1       定义。4.

1.2       系统说明。4.

1.3       UAS市场与应用。9

1.4       无人机融入空域。10

1.5       网络安全问题。14

1.6       结论17

2        安全与安保/网络安全的比较19

2.1       介绍20

2.2       定义。20

2.3       安全和安保的不同方面。21

2.4       风险管理的标准和方法。26

2.5       安全分析技术。29

2.6       安全分析技术。39

2.7       安全和安保综合方法。43

2.8       结论43

3        系统网络安全风险管理45

3.1       介绍46

3.2       拟议方法。46

3.3       个案研究53

3.4       结论60

我

二、内容



4        运营风险评估：从安全到网络安全61

4.1       介绍62

4.2       SORA方法的解释。62

4.3       将SORA方法扩展到网络安全的解决方案。67

4.4       伤害扩展：索拉和隐私伤害。69

4.5       威胁扩展：SORA面临新的网络安全威胁。74

4.6       用于风险评估的扩展SORA网络工具。79

4.7       结论81

5        扩展SORA方法说明83

5.1       介绍84

5.2       我们的方法与MULTIDRONE 84项目中使用的方法的比较

5.3       适用于其他案例研究。90

5.4       利用扩展的SORA方法进行系统开发。97

5.5       结论107

全球结论和展望109

A业务网络安全目标113

B网络工具手册121

B.1一般信息页。121

B.2地面风险等级（GRC）的确定。122

B.3空气风险等级（ARC）的确定。124

B.4隐私风险等级（PRC）的确定。127

B.5运营网络安全敏感等级（OCSL）确定。128

B.6结果。130

C风险管理结果131目录三



C.1故障。131

C.2网络安全要求。132

C.3风险等级。137

C.4攻击树。140

D-GPS欺骗及其对策151

D.1 GPS基础。152

D.2对策的现状。154

E原始SORA方法中的运行安全目标157

参考书目200

数字一览表

|  |  |  |
| --- | --- | --- |
| 1.1 | UAS架构。 | 4 |
| 1.2 | 从左到右：固定翼、旋转翼、飞艇和扑翼 |  |
|  | 机身。 | 5 |
| 1.3 | 三类无人机操作。 | 11 |
| 1.4 | U形空间图解[47]：。 | 14 |
| 2.1 | ISO 27005风险管理框架。 | 24 |
| 2.2 | 标准ARP4754[75]中的双V循环工艺。 | 26 |
| 2.3 | ANSI/ISA 84.00.01标准中SIL分配的风险矩阵。 | 31 |
| 2.4 | SIL分配的风险图[114]。 | 32 |
| 2.5 | 故障树分析示例[125]。 | 33 |
| 2.6 | 事件树图[126]的示例。 | 34 |
| 2.7 | 领结图示例[128]。 | 35 |
| 2.8 | 状态转换图[93]。 | 37 |
| 3.1 | 一般方法。 | 46 |
| 3.2 | 拟议方法的工作流程。 | 47 |
| 3.3 | 攻击树构建工作流程。 | 49 |
| 3.4 | UAS的体系结构。 | 54 |
| 3.5 | 与故障2-完整性相关的完整攻击树。 | 56 |
| 3.6 | 攻击场景到不同目标组件的分布。 | 58 |
| 3.7 | 将风险情景分布到不同的目标组件和风险级别 | 59 |
| 4.1 | 以蝴蝶结图表示的SORA方法的风险模型。 | 63 |
| 4.2 | 根据SORA[103]，地面和空中发生致命伤害的可能性。 | 64 |
| 4.3 | 简化的风险评估流程。 | 65 |

v

六数字一览表



|  |  |
| --- | --- |
| 4.4扩展风险模型。 | 67 |
| 4.5危害扩展的新步骤。 | 69 |
| 4.6侵犯隐私的可能性。 | 70 |
| 4.7最大像素密度位置。 | 71 |
| 4.8危害扩展的新步骤。 | 76 |
| 4.9申请概述。 | 79 |
| 4.10一些必需的信息。 | 80 |
| 4.11带有2D-SAIL的结果页。 | 81 |
| 5.1交付操作。  5.2将扩展SORA分析整合到devel中的拟议方法- | 92 |
| 选择过程。 | 97 |
| 5.3无人机操作。 | 99 |

5.4业务量。102

5.5系统架构。104

5.6地面站。105

5.7开发过程中提出的两种方法。110

B.1一般信息页。121

B.2计算固有GRC的信息。122

B.3计算最终GRC的信息。123

B.4战略缓解的相关特征。124

B.5计算初始电弧的信息。125

B.6减少电弧的缓解方案。126

B.7计算初始PRC的信息。127

B.8摄像机特性。127

B.9计算OCSL的信息。129

B.10根据GRC和ARC值计算的帆。130图七一览表



C.1 1可用性故障的攻击树-第1部分。140

C.2 1-可用性故障的攻击树-第2部分。141

C.3 1-可用性故障的攻击树-第3部分。142

C.4 1-可用性故障的攻击树-第4部分。143

C.5 1-完整性故障的攻击树-第1部分。144

C.6 1-完整性故障的攻击树-第2部分。145

C.7 2-机密性故障的攻击树。146

C.8 2-机密性故障的攻击树-第1部分。147

C.9 2-机密性故障的攻击树-第2部分。148

C.10 3-机密性故障的攻击树。149

C.11 3-完整性故障的攻击树。150

D.1到达时间测量[210]。152

D.2合成天线阵列结构[219]。155

表格一览表

|  |  |  |
| --- | --- | --- |
| 1.1 | 比较流行的开源和商业自动驾驶仪[17]。 | 6 |
| 2.1 | 不同社区的风险定义。 | 22 |
| 2.2 | ISO14971医疗器械风险管理中的风险评估矩阵。 | 23 |
| 2.3 | IEC61508[114]中的SIL值。 | 30 |
| 2.4 | 基于结果的SIL分配[115]。 | 30 |
| 2.5 | 风险评估技术比较。 | 38 |
| 2.6 | IAS99/IEC62443[145]中的SAL。 | 39 |
| 3.1 | 安全属性丢失导致的故障。 | 50 |
| 3.2 | 风险等级。 | 51 |
| 3.3 | 准备意味着。 | 52 |
| 3.4 | 机会之窗。 | 52 |
| 3.5 | 执行方式：。 | 52 |
| 3.6 | 攻击难度等级。 | 52 |
| 3.7 | 与故障2-完整性相关的攻击场景的风险评估。 | 57 |
| 4.1 | 确定SORA方法[104]。 | 66 |
| 4.2 | 图像细节分类[201]。 | 71 |
| 4.3 | 固有PRC测定。 | 72 |
| 4.4 | 中国伤害屏障修正系数。 | 73 |
| 4.5 | 与PRC值相对应的SAIL值。 | 73 |
| 4.6 | 3D-SAIL测定。 | 74 |
| 4.7 | 网络安全威胁的类别。 | 75 |
| 4.8 | 与CS相关的操作特征。 | 78 |

九

x表格清单

|  |  |
| --- | --- |
| 4.9 OCSO的确定。 | 79 |
| 5.1无人机和操作规范（来自多无人机项目）。 | 85 |
| 5.2 SORA方法中的固有GRC表。 | 85 |
| 5.3最终GRC确定的缓解措施。 | 86 |
| 5.4摄像机规格（来自多无人机项目）。 | 86 |
| 5.5固有PRC确定。 | 87 |
| 5.6风帆测定[104]：。 | 87 |
| 5.7 3D-SAIL测定。 | 88 |
| 5.8 OCSL测定结果。 | 89 |
| 5.9结果比较。 | 90 |
| 5.10 OCSL测定结果。 | 93 |
| 5.11交付操作的分析结果。 | 93 |
| 5.12修改交付操作的分析结果。 | 94 |
| 5.13 OCSL测定结果。 | 95 |
| 5.14带有隐私保护过滤器。 | 96 |
| 5.15“补充点”评估。  5.16应用软件后三种监测操作之间的比较- | 96 |
| 心理要点。 | 97 |

5.17中等稳健性水平的OCSO定义。101

缩写词表

|  |  |
| --- | --- |
| 弧 | 空气风险等级 |
| 在 | 攻击树 |
| 空中交通管制 | 空中交通管制员 |
| BVLOS | 视线之外 |
| 英国电信 | 领结 |
| C2 | 控制与指挥 |
| CONOPS | 行动概念 |
| 反恐精英 | 网络安全 |
| 欧洲航空航天局 | 欧洲联盟航空安全局 |
| 电子稳定控制系统 | 电子速度控制器 |
| ET | 事件树 |
| 英尺 | 故障树 |
| 地面军事系统 | 地面控制站 |
| GRC | 地面风险等级 |
| 全球定位系统 | 全球定位系统 |
| 人机界面 | 人机界面 |
| IACS | 工业自动化与控制系统 |
| 国际民航组织 | 国际民用航空组织 |
| 集成电路 | 工业控制系统 |
| INS | 惯性导航系统 |
| 即 | 初始事件 |
| 物联网 | 物联网 |
| 信息技术 | 信息技术 |
| 加卢斯 | 无人系统规则制定联合机构 |
| 梅哈里 | 风险协调分析方法 |
| OCSL | 操作网络安全敏感级别 |
| 奥克索 | 网络安全行动目标 |
| 奥索 | 作业安全目标 |
| OT | 操作技术 |

席

十二第0章。缩写词表

电源管理单元

中国隐私风险等级

SAIL特定的保证和完整性级别

SAL安全保证级别

SCADA监控和数据采集

SIL安全完整性等级

SORA特定操作风险评估

无人驾驶飞机

无人机系统

无人机

意外事件

视觉视线

介绍

无人机系统（UAS）最初用于军事目的，但如今，这种系统越来越多地用于民用目的。在过去的几年中，民用无人机市场在市场规模和应用领域方面呈指数级增长。市场规模从2016年的20亿美元增加到2018年的141亿美元[1]。目前，我们可以在不同的经济领域找到许多UAS应用：摄影、建筑、采矿、农业、现场监控、物流。UAS运营商正在继续探索和开发新的UAS应用程序。预计将有越来越多的无人驾驶飞机在我们、我们的家园、城市或工业基础设施上方运行。一方面，这种系统的普及可以给我们的生活带来新的便利和体验。另一方面，它也可能给我们带来麻烦。这些系统的故障或误用，无论是有意还是无意，都可能导致严重后果。例如，无人机操作可能有意或无意地侵犯人们在飞行中的隐私；无人驾驶飞机可能坠落并撞击地面上的人员和基础设施；或者它可能与载人飞机相撞。这些疑虑阻碍了公众的接受，也减缓了无人机的普及。它吸引了不同利益相关者的关注：运营商、制造商、立法者。

网络安全是阻碍公众接受UAS应用程序的主要问题之一。UAS是一个网络物理系统，其中数字组件（传感器、软件、通信等）协作控制和监控物理部件（如执行器、机身）。与许多其他网络物理系统（工业控制系统、汽车等）一样，UAS的数字部分始终存在漏洞或缺陷，可被攻击者利用。在文献中，有一些关于网络安全漏洞的报告：GPS干扰和欺骗[2]，视频拦截[3]，通过通信进行的劫持攻击[4]，传感器欺骗[5]。通过利用数字部分的漏洞，对手可能会干扰UAS的运行或出于恶意目的接管系统的控制：伤害地面人员、侵犯隐私、破坏基础设施等。因此，应考虑UAS的网络安全，以防止可能的负面影响并获得公众认可。本文以无人机系统的网络安全为主要研究对象。

由于网络安全在UAS领域发展中的重要性，在该领域有许多研究。通过观察有关UAS网络安全的文献，我们发现了两种传统的研究趋势。一是寻找新的漏洞或新的攻击策略。换言之，这是为了回答“我们如何才能攻击系统？”的问题。另一个是寻找针对可能的攻击的网络安全对策。换言之，这是为了回答“我们如何才能防止可能的攻击？”。网络攻击和防御技术日新月异。但是，对于特定任务中的特定UAS，考虑所有这些可能的网络安全攻击并实施所有相应的对策可能会花费高昂且不必要。因为

1

介绍

UAS和任务的性质是，从攻击者的角度来看，攻击的成本可能高于获得的利润。从运营商的角度来看，对抗成本可能高于损失。因此，在考虑网络安全问题时，我们应该考虑损失或成本效益之间的平衡为此，我们感兴趣的不是这两个传统问题，而是另一个问题：“应该考虑哪种网络攻击和对策以及优先顺序？”。

为了回答这些问题，我们需要进行风险评估。风险评估方法为检测、分析、评估可能的安全攻击和选择适当的对策提供了一种系统而有效的方法。长期以来，不同的风险评估方法已被开发并用于不同的工业领域。风险评估方法首次用于预防潜在事故（安全）。由于计算机在工业中的广泛应用，风险评估方法在保护系统免受网络攻击（网络安全）方面起着至关重要的作用例如，我们有针对IT系统的MEHARI、针对汽车系统的EVITA、针对工业自动化和控制系统的IEC61508、针对航空电子系统的ED202A和ED203。在UAS领域，针对UAS的网络安全风险评估研究不多。最流行的风险评估方法是特定操作风险评估（SORA）。但是，目前它只关注安全。因此，本论文主要针对UAS应用程序开发网络安全风险评估。

本论文的组织结构如下。第1章向读者概述了无人机系统，包括无人机的定义、总体架构、市场、法规和网络安全漏洞。第2章从不同方面比较了安全与安全/网络安全：定义、风险概念和风险人的最新技术管理。第3章介绍了第一个贡献-一种加强现有或预定义UAS网络安全的方法。第4章首先解释SORA方法，然后介绍我们提出的将该方法扩展到网络安全的解决方案。第5章用不同的案例说明了扩展的SORA方法研究并演示如何在开发过程中使用评估结果。最后，结论总结了我们的工作成果，并对未来的工作提出了一些建议。

第一章

无人机系统及相关网络安全问题



目录



               1.1定义4

               1.2系统说明4

                        1.2.1无人机部分5

                        1.2.2地面段7

                        1.2.3通信段8

               1.3无人机市场和应用9

               1.4无人机融入空域10

                        1.4.1法规11

                        1.4.2 U型空间概念13

               1.5网络安全问题14

                        1.5.1全球定位系统14

                        1.5.2 IMU 15

                        1.5.3通信16

                        1.5.4自动驾驶仪和地面军事系统16

               1.6结论17



3

1.1定义

根据国际民用航空组织（ICAO）[6]，无人机（UAV）或者，无人机是一种可以在无人驾驶的情况下飞行的飞机，并且可以从另一个地方远程或完全控制。但是，无人机不能单独运行，但需要与地面操作员保持交互。因此，另一个术语是无人机系统（UAS）该系统包含无人机和所有必要的设备、网络和人员，以控制无人机并完成特定任务[6]、[7]、[8]。这种系统首次用于军事领域的危险任务。如今，技术的进步降低了获取该技术的成本。这导致无人机在货物运输、农业、航空摄影等许多民用领域的应用不断增加[4]。

1.2系统说明

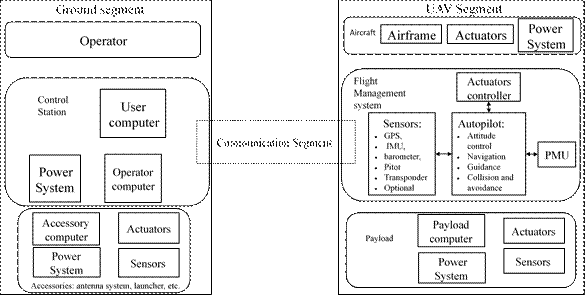


图1.1:UAS体系结构

根据任务期间无人驾驶飞机的自主程度，系统复杂性可能会有所不同[9]。至于最低程度的自主性，我们可以指出于爱好的简单无人机，它由一架简单的遥控飞机、一个远程无线电控制器和一名地面飞行员组成。同时，为了获得更高程度的自主性，无人机可以由一组配备有精密传感器、处理器、通信设备和通信设备的飞机组成无人机设备，允许飞机在无需飞行员交互的情况下飞出可视范围。本部分介绍了无人机系统架构的一般描述。基本无人机系统的组件可分为三个部分：

1.2.系统说明

无人机（UAV）段、地面段和通信段[7]、[8]。这些段可以如图1.1所示进行描述，在下一节中有详细说明。

1.2.1无人机部分

无人机部分包括三个主要模块：飞机、飞行管理系统和有效载荷（见图1.1）。

1.2.1.1飞机

该模块集机身、执行器和动力系统于一体。

机身是指不包括推进系统的车辆机械结构。无人机的机械结构以各种形式存在，具有不同的特征，如空气动力学、尺寸、质量，这些特征是根据目标操作的要求选择的。无人机机身基本上分为以下四类之一：固定翼、旋转翼（如直升机、多直升机）、小飞艇和扑翼[8]、[10]（见图1.2）。除基本机身外，还有具有基本机身特征的混合机身。例如，倾转旋翼机身是固定翼机身和旋转机身的组合[11]。

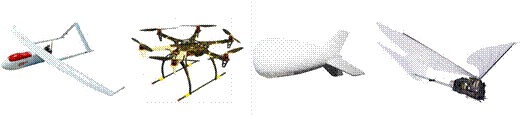


图1.2：从左到右：固定翼、旋转翼、飞艇和扑翼机身

执行器负责将控制命令转换为机械部件的物理运动：螺旋桨、襟翼、方向舵、扰流板和降落伞发射器。因此，飞行器可以改变其姿态和高度。

电力系统由用于存储、产生和分配能量的电气或机械部件组成。起初，电力系统的主体是内燃机[12]，适用于大型军用无人机。如今，对于轻型商用无人机，电力系统越来越受欢迎，有许多先进技术，如燃料电池[13]、[14]、太阳能电池[15]、[16]和电池。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 开源 | 机身 | 硬件 | 多无人机 | 飞行计划 | 地理栅栏 | 避碰 | 最后释放 |
| 狗仔队 | 固定翼，旋转翼 | 多种多样的 | 对 | 对 | 对 | 对 | 19-12-18 |
| 皮克斯霍克 | 固定翼，旋转翼 | 具体的 | 对 | 对 | 对 | 对 | 21-04-20 |
| 飞行员 | 固定翼，旋转翼 | 多种多样的 | 对 | 对 | 对 | 正在开发中 | 29-02-20 |
| OpenPilot | 固定翼，旋转翼 | 具体的 | 没有一个 | 对 | 不适用 | 不 | 18-07-15 |
| AeroQuad | 旋转翼 | 多种多样的 | 没有一个 | 不 | 不适用 | 不 | 31-01-13 |
| 贸易的 |  |  |  |  |  |  |  |

        Picollo固定翼，旋转翼专用是是不适用

微型飞行员固定翼、旋转翼、飞艇专用翼是是不适用

在下面

       维蒙特固定翼、旋转翼、飞艇专用翼是不适用

发展

表1.1：流行的开源和商用自动驾驶仪的比较[17]

1.2.1.2飞行管理系统

飞行管理系统是一套所有航空电子组件，用于观察车辆和控制执行器/发动机的行为，以执行安全和自动飞行。该模块的关键要素是自动驾驶仪、基本传感器、电源管理单元、执行器控制器和车载通信模块。

自动驾驶仪涉及硬件和软件两个方面。它是飞行管理系统（FMS）的中心，与FMS的其他部件（传感器、执行器、通信、电源管理单元（PMU））进行通信。该组件的基本作用是根据地面飞行员的指令或程序飞行计划，估计飞机的状态并导航飞机。随着无人机数量的逐渐增加，开放式sourc下自动驾驶仪的硬件和软件呈指数级增长表1.1简要比较了当前流行的开源和商业自动驾驶仪。

传感器是允许飞机导航的机载传感器。传统上，无人机的主要核心传感器是全球导航卫星系统（如全球定位系统-GPS）和惯性测量单元（IMU）。因为它们具有互补性（例如，GPS的精度高但数据速率低；IMU的数据速率高但误差累积[18]），GPS和IMU传感器是大多数飞行管理系统的首选传感器耦合[19]。这些传感器的输出由自动驾驶仪进行集成，以估计飞机的行为。GPS/IMU集成有许多已开发的算法，如非耦合集成、松耦合集成、紧耦合集成和深度耦合集成[20]。除了传统的GPS/IMU耦合，本研究还研究了其他传感器组合，如GPS/vision computer耦合[21]，IMU/vision computer耦合[22]。为了增强飞机状态估计，无人机可以配备多个传感器

1.2.系统说明：各种补充传感器，如气压计或磁强计。

执行器控制器是将自动驾驶仪指令转换为控制信号并发送至执行器的电子元件。典型的执行器控制器之一是调节电机速度的电子速度控制器（ESC）。

PMU由负责测量和管理车辆能量的电子部件组成。

1.2.1.3有效载荷

有效载荷是无人机飞行所不需要的组件，但却是实现特定操作目标所必需的。为安全起见，有效载荷应配备与飞机主电源系统隔离的自身电源系统，且不应直接连接到自动驾驶仪或其他关键系统[7]。因此，有效载荷系统可以有自己的传感器、执行器、外围设备和处理器。根据应用情况，无人机可以配备各种类型的有效载荷组件。最流行的有效载荷组件是摄像头。该组件广泛用于与视听pro相关的许多UAS应用生产、监测应用或大型基础设施的检查，如桥梁、风车或电力线[23]、[24]、[25]。激光雷达是另一种受欢迎的传感器有效载荷，吸引了大量与无人机相关的研究。激光雷达允许以高精度测量距离，因此可用于制作高分辨率地图[26]，[27]。随着无人机应用数量的增加，如今，越来越多的设备可以作为有效载荷安装在无人机上，如用于精确农业的喷洒系统[28]，[29]，或用于良好运输的货物。

1.2.2地面段

地面段（见图1.1）包括所有不是飞行器本身组成部分但飞行所需的元件。该部分的主要元素包括：操作员、控制站和附件（见图1.1）。

1.2.2.1操作员

根据国际民用航空组织（ICAO）[6]的定义，运营商是指从事或提议从事飞机运营的个人、组织或企业。根据UAS操作或应用的复杂性，运营商的规模可能会有所不同。例如，对于最简单的UAS操作，操作员只能是手动驾驶遥控飞机的飞行员。同时，在更复杂的UAS操作中，操作员可以是由许多人组成的结构化组织，如飞行员（或机组人员）、维修人员、经理。每个运营商成员的角色应由当地民航局确定。

1.2.2.2控制站

控制站由地面上用作人机界面（HMI）的硬件和软件组成，用于控制/观察车辆和有效载荷。根据UAS应用程序的用途，UAS可能有多个控制站[7]。例如，为了观察一个工业现场，一个UAS可以部署两个控制站。第一个安装在远离工业现场的地方，供飞行员完全控制车辆和有效载荷。第二种是移动台（如平板电脑、智能手机）。该移动站由工业现场内的人员使用，并且只能访问有效载荷数据，例如相机数据。

1.2.2.3附件

附件是指不直接参与UAS操作但需要执行该操作的设备，如天线/摄像机跟踪系统、UAV弹射器发射器、电池充电器或运输箱。

1.2.3通信段

通信段（见图1.1）对于任何类型的UAS应用都至关重要。该部分包括为UAS提供远程控制和远程数据采集能力的不同通信系统[30]。在操作过程中，通信系统可以传输各种数据。大多数无人机的基本功能是控制和指挥（C2），包括遥测数据、飞行控制数据、飞行配置数据。这种数据在飞机和飞行员之间交换，以进行安全飞行。另一种数据是有效载荷数据，包括用于控制有效载荷的数据和由有效载荷生成的数据，例如视频数据。这类数据对飞行并不重要，但对实现运行目标很重要（如监控应用的视频数据）[31]。除了这两种数据外，通信系统还可以传输交通数据。这种数据在飞机、地面控制站和空中交通管制员（ATC）之间交换，以维持空域的安全和高效。随着未来无人机数量的增加，此类数据和相关技术是将无人机成功集成到国家空域系统中的关键因素[30][32]。

根据预期操作的连接性需求（例如范围、带宽），通信系统的复杂性可能会有很大变化。为了便于操作，通信系统只能提供飞机与地面控制站（GCS）之间的连接。对于更复杂的操作，通信系统可以

1.3. 无人机市场及应用

将无人驾驶飞机与其他飞机连接，以构建无人机群，或将地面军事系统与ATC连接，以共享交通信息。

1.3无人机市场及应用

无人机的历史始于20世纪初，当时它们首次被用作军事实践的目标[33]。从那一刻起，无人机市场逐步形成。在上个世纪，市场只关注军事应用，如侦察/作战任务，而不认可无人机的民用应用。从21世纪开始，民用UAS市场开始成长。起初，在民用环境中，无人驾驶飞机被用作个人娱乐目的的玩具。然后，技术的发展（如部件小型化、计算能力的提高、传感器和电池容量的提高）使UAS变得更小，在许多经济部门的专业和商业用途中更具吸引力，例如：

•摄影和媒体部门：在UAS技术出现之前，为了从空中拍照或拍摄电影，摄影师和电影制作人别无选择，只能使用价格昂贵且不灵活的直升机或飞机。如今，这项任务可以通过使用配备高质量摄像机的无人机来实现。随着价格的下降，这种无人机在这一领域越来越受欢迎。事实上，2016年，该行业中与无人机相关的产品和服务产生了民用无人机行业的大部分收入（占总收入的60-70%[34]，[1]）。

•农业部门：该部门还得益于UAS技术的出现，以降低运营成本。农民可以不用飞机或卫星，而是使用无人机喷洒杀虫剂，收集和分析农田数据（如农田养分吸收强度[35]，在植物出现明显压力前几天的压力[36]，…）。根据2017-2027年农业机器人和无人机：技术、市场、玩家[37]，农业无人机应用将是一个主要市场，2027年将达到4.7亿美元。

•能源部门：UAS对能源部门的公司也有吸引力。该部门的重点是使用UAS进行维护和检查，以减少与执行危险任务的基础设施和员工相关的各种风险。根据2019年开展的一项调查[38]，超过三分之二的能源公司（超过247家公司参与了调查）目前正在使用无人机开展活动。然而，大多数无人机操作仍处于概念验证或无人机应用研发领域。UAS应用最需要的特性是飞行的耐久性、灵活性和可靠性，未来需要改进。

•物流和运输部门：预计未来UAS将成为物流和运输系统的一部分。无人驾驶飞机系统可用于在密集（次）城市地区交付具有最大竞争优势的小包。这种应用吸引了亚马逊、UPS、联邦快递等电子商务领域大公司的大量考虑。根据SESAR联合企业（负责欧洲空中交通管理现代化的公私合作伙伴）的预测，2035年，该应用的无人机机队规模可能达到70000架[32]。然而，目前，用于良好交付的无人机系统还没有得到广泛部署和接受，该领域的大多数航班仍然是出于概念验证目的实现的。此类应用最重要的促成因素之一是未完全定义的法规[32]。

在过去十年中，我们认识到民用无人机市场的爆炸性增长。从2012年到2019年，该领域投资超过30亿美元，市场规模从2016年的20亿美元[1]增长到2018年的141亿美元[39]。同时，军用无人机市场始终由波音、洛克希德·马丁、空中客车等在行业中拥有强势地位的公司主导，民用无人机市场几乎由新的参与者或初创企业主导[33]。这种趋势的最好例子是中国公司DJI和法国公司Parrot，它们是市场上最成功的UAS制造商。市场的爆炸性增长不仅给制造商带来了机会，也给该领域的其他参与者带来了发展业务的机会。他们是提供行业服务（无人机监控、观察、检查等）、培训计划和软件解决方案以分析无人机收集的海量数据的公司[33]。

展望民用UAS的未来，许多组织和市场研究公司都会给出市场预测。西尔联合事业公司预测，2050年将有大约400000架商用无人机在欧洲上空飞行（不包括700万架休闲无人机）[32]。根据市场研究未来，民用无人机市场的规模将在2027年达到700亿美元的估值[40]。《无人机行业洞察》预测，民用无人机市场将在2024年达到431亿美元[1]。Interact分析公司预测2022年市场价值为150亿美元[41]。尽管这些数字只是或多或少准确的预测，但它们都是乐观的。换句话说，这些数字反映了人们对民用无人机市场在不久的将来增长的信心。

1.4无人机融入空域

空域的组织和维护基本上基于复杂的规章制度和标准，以确保所有航班以安全和高效的方式运行。这些法规和标准涵盖了航空工业从飞机设计到运行的许多方面。例如，载人飞机必须按照计划进行认证、注册和维护；船员必须持有执照，操作员必须经过认证[42]。此外，飞机需要与空中交通管制员交换以避免碰撞。然而，目前的调节系统设计为适合有人驾驶飞机，而不是无人驾驶飞机。

1.4. 无人机融入空域

事实上，要将无人机安全高效地集成到空域中，还有很多挑战[43]。其中一个挑战是，现有的载人飞机法规不适用于无人驾驶飞机系统[42]。与有人驾驶飞机市场不同，无人机市场由大量低成本无人机主导，无人机周期短（约30个月[44]）。因此，基于用于载人飞机的昂贵流程设计、认证和操作无人机是没有意义的。另一个挑战是如何利用无人驾驶飞机和有人驾驶飞机维持空域的安全运行。为避免空中碰撞，载人飞机通常配备了若干设备，允许与空中交通管制员和其他飞机进行通信，以接收许可和紧急警告，如无线电通信、应答器。对于所有无人机操作员来说，遵守这些要求似乎是一项负担[42]。此外，由于其体积小和操作灵活性高，无人驾驶飞机可以在任何地方起飞/降落，并且不会像有人驾驶飞机那样沿着固定和命名的航路点飞行[45]，[42]。这使得有人和无人驾驶飞机的空中交通管制成为一项复杂的任务。



图1.3：三类无人机操作

1.4.1法规

为了将UAS整合到领空中，欧洲委员会2008通过发布法规EC2008 / 216开始考虑这一车辆。本法规是第一份专门针对无人机操作的法律文件。然而，本文件仅详细说明了飞机重量超过150千克的UAS操作规则。150公斤以下飞机的操作规则由每个成员国负责。这意味着欧洲国家对这种过程有自己的规则。这种多样性导致了无人机市场的细分，并可能阻止某些无人机运营（如跨境飞行）。因此，它需要欧盟层面的法规，考虑所有的UAS操作来修改EC2008／216规则。2015年，欧盟委员会委托欧盟航空安全局（EASA）制定监管框架和监管建议。然后在2015年和2017年，欧洲广告标准联盟发布了两份文件：NPA2015-10[46]和NPA2017-05[44]。这些建议的原则可恢复如下：

新法规考虑了各种UAS。这意味着应取消150kg的限制。

•该监管框架以运营为中心。这意味着监管是根据运营风险组织的。它应该建立从低风险到高风险的三类业务：

–开放类：包括低风险运营，如大多数休闲航班和一些专业活动。这类业务不需要民航当局的明确授权。对于这些操作，通过严格的操作限制来确保安全（例如，不靠近人员、交通、基础设施、无危险物品、无物品掉落、每个飞行员只有一个UAS）。

–具体类别：重新组合中等风险的操作，例如视线以外的操作（即飞行员和无人机在飞行过程中没有视觉接触）。对于此类操作，需要进行风险评估。

–认证类别：包括风险相当于载人飞机操作的操作。这些操作的要求与载人航空要求相当，例如无人机、持证远程飞行员和经主管当局批准的操作员的认证。

•法规应针对不同的安全风险：与载人飞机的空中碰撞、人身伤害和财产损失。

•要求应与操作风险成比例。

•应考虑安全和隐私。安全不仅限于敏感区域的飞越。网络安全也是无人机的一个问题

2019年，根据上述提议，欧盟委员会发布了委员会授权条例（EU）2019/945和委员会实施条例（EU）2019/947。委员会授权条例（EU）2019/945规定了认证要求，包括CE标志和第三国运营商。委员会实施条例（EU）2019/947规定了操作和注册要求。在2019/947法规中，三个运营类别的边界定义如下：

•开放类：在以下情况下，UAS运营始终被视为属于该类：

–最大起飞质量小于25kg。

–飞机不携带危险品。

–飞机不会掉落任何材料。

–远程飞行员年龄等于或大于16岁。

–飞行员始终将飞机保持在其可视范围内（可视视线操作）。

1.4. 无人机融入空域

–飞机不会飞越人群。

–地面以上的最大高度为120m。

•特定类别：当不满足开放类别条件时，UAS运营始终被视为属于该类别

•认证类别：在以下情况下，UAS运营始终被视为属于该类别：

–飞机飞越尺寸超过3m的人员集合；或–人员运输；或–运载危险品。

预计大多数无人机操作将在特定类别下运行。对于此类，运营商必须根据SORA方法进行并提交风险评估。但在某些情况下，运营商可以跳过全面风险评估：

•操作符合2019/947法规中预定义的标准场景（STS-01和STS-02）。

•运行符合委员会实施条例（EU）2019/947指导文件中规定的预定义风险评估中规定的运行特征。

1.4.2 U形空间概念

除了监管提案外，欧洲航空航天局在UAS整合方面的另一项努力是“U-Space”提案"概念。该概念并非顾名思义，它不是指分配给无人机操作的新空域容量，而是指一套支持无人机操作的新技术服务。这些服务正在或将要开发，以使复杂的无人机操作能够在所有操作环境（包括城市、次区域）中实现高度自治城市、农村[47]。随着无人机连接和自动化水平的提高，U-space概念提出了四个服务模块：

•基本服务（U1）包括电子注册、电子识别和地理围栏服务。这些服务有助于管理局识别无人机，并支持安保和安全要求。

•初始服务（U2）支持无人机运行管理，可能包括飞行规划、飞行批准、跟踪、空域动态信息以及与空中交通管制的程序接口。

•先进服务（U3）使无人机在密集区域飞行时能够自动检测并避免与其他无人机发生冲突。



图1.4:U形空间示意图[47]

•全方位服务（U4）提供与载人航空的集成接口，支持U-space的全面运作能力，并将依靠无人机和U-space系统的高度自动化、连接性和数字化。

由于与U-space相关的标准和技术是由许多公共组织和私营公司同时开发的，因此今天可以提供许多这一概念的服务。然而，这并不意味着U-space可以立即实施，因为此类开发工作零碎且缺乏实际条件下的实际测试[42].

1.5网络安全问题

1.5.1全球定位系统

如1.2.1.2所述，GPS接收机是无人机的一个重要组件，尤其是当无人机可以在自动模式下飞行时。该组件提供无人机上的原始信息

1.5.网络安全问题

根据卫星信号确定车辆位置。这些信号来自距离地球1300英里的GPS卫星，必须穿过地球大气层。当到达无人机上的接收器时，它们非常弱。这使得GPS接收机容易受到干扰攻击（GPS干扰），攻击者可以通过更高功率的GPS信号连接原始GPS信号。这种攻击可以使用市场上可用的低成本设备进行[48]，不需要任何专业知识。此外，民用GPS数据未加密。这使得GPS接收器容易受到欺骗攻击（GPS欺骗）。在这种攻击中，攻击者可以用包含错误位置信息的假GPS信号欺骗GPS接收器。事实上，有几起无人机事件被怀疑是由GPS欺骗攻击造成的，例如S-100 Camcopter无人机坠毁、军用无人机RQ-170被俘[2]。在研究中，GPS欺骗的可能性已经通过许多工作中的攻击实验得到了验证。例如，2012年7月，UT Austin的无线电导航实验室在受控条件下对小型无人机进行了GPS欺骗攻击，导致指令俯冲[49]。Seo等人[50]进行了另一项实验，通过使用GPS欺骗技术迫使无人机降落在错误的位置。与GPS干扰攻击相比，成功实施GPS欺骗攻击需要复杂的设备和GPS知识。GPS欺骗的后果可能比GPS干扰攻击更残酷。因为在GPS干扰的情况下，可以检测到攻击并将其视为GPS组件故障（GPS信号丢失）。大多数商用无人机都有故障安全机制来处理这种情况（例如基于其他传感器的安全着陆）。同时，在GPS欺骗的情况下，攻击者可以在飞行员不知情的情况下接管无人机飞行路径的控制权。文献中提出了针对GPS欺骗的不同对策（详见附录D）。

1.5.2           伊姆

惯性测量单元（IMU）是无人机的另一个基本组件。该组件使无人机能够在无需外部参考的情况下感知运动（例如，GPS使用卫星信号作为外部参考）。一个简单的IMU由一个陀螺仪（感应角速率）和一个加速计组成。这些传感器根据传感质量的位移测量无人机的运动。由于尺寸、功率和成本的限制，大多数小型/商用无人机都配备了低成本的无屏蔽IMU。这使得IMU容易受到声音干扰。虽然没有关于通过IMU进行网络攻击的报告，但已经做了几项工作来说明这种攻击的可能性。Yunmok等人[51]通过传感器近共振频率处的故意声干扰，对无人机的陀螺仪进行了拒绝服务攻击实验。同时，Lu等人[52]展示了一种通过基于短时傅立叶分析的有意声干扰完全控制陀螺仪输出信号的方法。Trippel等人[53]也对加速度计进行了同样的攻击。除了与IMU相关的攻击技术外，还研究了不同的防御方法。想到的常见方法是传感器冗余。但是，它需要额外的传感器。Tu等人[54]提出了一种不添加传感器的IMU攻击检测和容错方法。如果IMU受到攻击，则仅基于位置数据和航向数据估计姿态数据。Crispoltoni等人[55]提出了一种基于数据的方法来检测IMU数据中的异常。Yaseen等人[56]提供了一种带有故障检测机制的广义预测控制器。该机制可用作检测受损IMU数据的对策。

1.5.3           表达

根据通信要求（范围、带宽、成本等），UAS使用的通信技术可能会有所不同，如WiFi、RF、4G/LTE、卫星等。由于这些技术用于一般用途，不仅用于UAS应用，还引入了许多工作来保护这些技术。对于小型/商用UAS，由于资源限制或配置错误，通信的安全性无法达到正确的水平。文献中的一些工作是为了说明通过通信系统对UAS进行网络攻击的可能性。Vattaparamban等人[4]利用WiFi的漏洞对不同的低成本UAS进行了反认证攻击实验。对于相同的通信技术，Fournier等人[57]在无人机杰克项目中成功地接管了无人机的控制权。

许多商用无人机使用通信系统顶层的开源MAVLink协议来传输无人机和地面军事系统信息。但是，Mavlink协议的原始版本（1.0版）没有提供任何机制来保护交换的消息（机密性、可用性、身份验证）。在这个版本中，通信通道的安全性完全基于较低的通信层。例如，如果WiFi通信受损，MAVlink无法提供任何保护。自动驾驶仪资源的限制可能会妨碍MAVlink协议的可靠加密的实施。[58]. Marty[59]的论文中讨论了加密的MAVlink协议。

1.5.4           自动驾驶仪和地面军事系统

自动驾驶仪有时与外部设备连接，用于多种目的，如下载飞行数据、获取更新包或重新配置。这使得自动驾驶仪容易受到病毒感染或未经授权的访问。在此类攻击中，攻击者可能恶意更改飞行参数，以改变系统的行为/控制规律[60]。对于大多数商用无人机，地面军事系统通常构建在带有地面军事系统软件的通用计算机（笔记本电脑、台式机、智能手机）上。因此，与基于这些设备的其他应用程序一样，地面军事系统可能成为网络攻击的初始目标。例如，攻击者可以恶意修改GCS上存储的数据（如飞行参数、飞行计划、地图），以欺骗飞行员[60]。Heiges等人[61]试验了一种攻击场景，其中地面军事系统软件遭到破坏，并显示错误信息，以阻止对自动驾驶仪的其他攻击。

1.6. 结论

1.6结论

本节为读者提供了无人机系统的概述。由于技术的发展，该系统的价格在过去十年中迅速下降。这导致该系统变得越来越流行，并被用于许多经济部门：农业、建筑、摄影等。空域无人驾驶飞机数量的快速增长要求采取行动确保空域、地面人民生命和财产的安全。为了满足这一需求，欧盟委员会和欧盟航空安全局（EASA）制定了无人机操作规则。除新法规外，欧洲航空航天局还引入了“U空间”概念，以有效组织无人机在空域内的运行，尤其是在市区。UAS是数字组件和机械组件的组合。除了安全，网络安全也是无人机系统的一个问题。文献中报告了许多安全问题。

第二章

安全与安全/网络安全的比较



目录

|  |  |
| --- | --- |
| 2.1导言。 | 20 |
| 2.2定义。 | 20 |
| 2.3安全和安保的不同方面。 | 21 |
| 2.3.1风险概念。 | 21 |
| 2.3.2风险管理。 | 21 |
| 2.3.3系统设计过程。 | 25 |
| 2.3.4操作和人为因素。 | 25 |
| 2.4风险管理的标准和方法。 | 26 |
| 2.4.1安全。 | 26 |
| 2.4.2安全。 | 27 |
| 2.5安全分析技术。 | 29 |
| 2.5.1危险与可操作性分析。 | 29 |
| 2.5.2 SIL分析。 | 29 |
| 2.5.3故障树分析。 | 32 |
| 2.5.4事件树。 | 34 |
| 2.5.5领结分析。 | 35 |
| 2.5.6马尔可夫分析。 | 36 |
| 2.5.7 Petri网。 | 37 |
| 2.5.8失效模式与影响分析。 | 37 |
| 2.5.9总结。 | 38 |
| 2.6安全分析技术。 | 39 |
| 2.6.1从SIL水平到SAL水平。 | 39 |
| 2.6.2安全方面的危险与可操作性分析。 | 40 |
| 2.6.3从故障树到攻击树。 | 40 |
| 2.6.4基于FMEA的技术。 | 41 |
| 2.6.5领结安全性分析。 | 41 |
| 2.6.6安全的马尔可夫过程。 | 42 |
| 2.6.7用于安全的Petri网。 | 42 |
| 2.7安全和安保综合方法。 | 43 |
| 2.8结论。 | 43 |

19

2.1导言

在上一章中，我们介绍了无人机系统的一般概念以及公众对其安全和安保/网络安全的关注。因为安全和安保都是指人和资产的保护，所以在语言的日常使用中，它们有时可以互换使用[62]。这可能会导致一些混乱。因此，在本章中，我们首先提供这些术语的定义，强调它们之间的差异。然后，我们讨论了安全和安保之间的相似方面。本章还回顾了行业和学术界如何解决安全和安保/网络安全问题。

2.2定义

有许多不同的方法来定义两个术语：安全和安保。从一个专家到另一个专家，从一个技术团体到另一个技术团体，这些可能会有所不同[63]。例如，在航空航天工业中，安全可定义为“人身或财产伤害风险降低到可接受水平的状态”[64]，而对于工业控制系统（ICS），安全可定义为“该状态不受“某物”的影响”这可能会产生负面后果，如对人类或动物的伤害、经济损失或任何其他形式的损害或损失”[65]。对于信息系统，安全性可以解释为“一个涉及保护信息免受各种威胁的过程，以确保业务连续性并将业务风险降至最低”[66]，而对于嵌入式系统，该术语可以定义为“安全性是一个实体保护其承担保护责任的资源的能力”[67]。这两个术语没有绝对的定义：安全性和安全性[68]。这有时会导致在使用这些术语时出现歧义。此外，安全和安保都指风险和某种保护，因此，在某些情况下，这些术语可以互换使用，如[69]。

然而，安全和安保仍然是两个不同的术语，应该有不同的含义。本文介绍了文献中的一些作品，以说明这些术语之间的差异。例如，基于对86份官方文件（不同部门的国际、国家标准/法规）中定义的审查，Piètre Cambacédès等人[70]提出了安全和安保定义之间的两个主要区别。第一个是恶意与意外（M-A）区别。安全解决了源于恶意行为的意外风险，同时安全解决了源于意外/非故意事件的风险。这种区别似乎在文献[68]、[71]、[72]、[73]、[74]中得到广泛接受。第二种区别称为环境系统（E-S）原产地区分。安全性涉及来自环境的风险（所考虑的系统周围的所有其他事物）和可能影响系统的风险。同时，安全性涉及所考虑的系统产生的风险和可能影响环境的风险。这种区别也被其他一些研究所接受，如[68]然而，在我们看来，第二个区别不是很清楚。例如，与飞机的安全有关，我们可以考虑由恶意行为引起的场景，不仅影响飞机，而且影响乘客的生命，公司的财务等。同时，与飞机的安全有关，我们可以担心不安全的SC。因恶劣天气条件引起的疾病。

基于上述简短分析，我们采用以下定义：

•安全性是指系统受到保护，免受恶意意图造成的风险。网络安全是仅与数字世界相关的安全性的子术语。

*注：在我们的研究背景下，安全一词实际上是指大多数情况下的网络安全，除非明确说明。*

•安全是指保护系统免受事故或意外事件风险的状态。

上述两个定义不应被视为绝对定义。我们采用这些定义的目的是避免在我们的上下文研究和文件的剩余部分中产生误解。此外，我们认为，理解安全和安保的性质比创建一个简短的短语来描述更有趣因此，在下一节中，我们将深入分析安全与安保在不同方面的异同。

2.3安全和安保的不同方面

2.3.1           风险概念

安全和安保有一个共同点，即术语“风险”。在这两个领域中，风险被实践者和研究人员广泛用作推动活动以保护所考虑的系统或操作的基本概念。如表2.1所示，该术语的定义在不同的技术团体之间可能略有不同。尽管在不同的社区之间存在一些差异因此，风险术语始终可以表示为两种测量（或估计）的组合：“事件可能有多严重？”和“可能发生的频率？”或用简单的公式表示：风险=可能性x后果严重性。

2.3.2           风险管理

通常，负责安全风险或安全风险的人员必须回答一些问题，如“是否已识别所有事件？”，“实施的保护是否充分或必要”为了回答这些问题，风险通常通过风险管理来处理。风险管理提供了一种系统有效的方法来检测、分析、，

|  |  |
| --- | --- |
| 社区和来源 | 风险定义 |
| 安全  原子能的  （原子能机构术语表[69]） | 表示与实际或潜在接触相关的危害、危险或有害或伤害性后果的可能性的多属性量。它与诸如可能产生特定有害后果的概率以及此类后果的大小和性质等量有关。 |
| 航空学  （ARP4754a[75]） | 发生频率（概率）及其相关严重程度的组合。 |
| 化学制品  （CCP术语表[76]） | 根据事故发生的可能性和损失或伤害的程度来衡量人身伤害、环境损害或经济损失 |
| 医疗器械（ISO 14971[77]） | 伤害发生概率和伤害严重程度的组合 |
| 安全  油气  （OLF-104[78]） | 事件发生概率及其后果的组合 |
| 通用IT  （NIST SP800-53[79]） | 鉴于威胁的潜在影响和威胁发生的可能性，信息系统的运行对机构运营（包括任务、职能、形象或声誉）、机构资产或个人的影响程度。 |
| 信息系统（ISO 27000[80]） | 风险通常表示为事件后果和相关发生“可能性”的组合 |
| 互联网  （IETF RFC 4949[81] | 损失预期，表示为特定威胁利用特定漏洞造成特定有害结果的概率 |

表2.1：不同社区的风险定义

评估可能发生的事件，并选择适当的应对措施。此外，风险管理有助于平衡运营与实施应对措施的经济成本[82]。大多数风险管理包括风险评估。风险评估是“关键组成部分”，提供足够的风险知识、意识和理解，以证明安全措施的合理性，从而降低风险管理过程中的风险[83]。风险评估包括风险识别步骤、风险分析步骤和风险评估步骤：

•风险识别（见图2.1）旨在识别可能发生并产生意外影响的风险情景。对于这一步，不同的风险管理方法可以提出不同的策略。一些方法通过向用户提出一系列基本场景（例如，用于信息系统安全的MEHARI方法（见2.4.2）和用于UAS操作安全的SORA方法（2.4.1））来简化此步骤。其他方法提供工具或模型来帮助用户分析可能的场景。这种方法可以采用演绎法或归纳法[84]。归纳法侧重于回答“给定结果如何发生？”或“给定结果的原因是什么？”的问题。这种情况的好例子是故障树方法和攻击树方法。同时，演绎方法从初始事件（组件故障或错误）开始，并试图回答“危险事件的后果是什么？”的问题。HAZOP方法和FMEA方法就是这种方法的好例子。所有这些方法将在以下部分中介绍。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 可能 | 频繁的 | 低的 | 中等的 | 高的 | 高的 | 高的 |
| 可能的 | 低的 | 中等的 | 中等的 | 高的 | 高的 |
| 偶尔的 | 低的 | 低的 | 中等的 | 中等的 | 高的 |
| 遥远的 | 低的 | 低的 | 低的 | 中等的 | 中等的 |
| 不可能的 | 低的 | 低的 | 低的 | 低的 | 中等的 |
|  |  | 可以忽略不计的 | 少数的 | 不好的 | 专业 | 批评的 |
|  |  | 严重程度 |  |  |

表2.2:ISO14971《医疗器械风险管理》中的风险估计矩阵

•风险分析（见图2.1）是理解与风险识别中确定的情景相关的风险性质的活动。如上所述，风险是后果的可能性和严重性的组合；因此，风险分析涉及对这些因素的估计[85]。对可能性和严重性的估计可以是定性的，也可以是定量的。为了安全起见，根据Khan等人[86]的观察，定量方法和混合方法比定性方法越来越受到重视。同时，对于安全性，定性方法是最可取的[87]。这些现象的原因可能是数据的可用性。在安全方面，通常可以访问部件故障或事故的数据（例如，通过测试，我们可以估计机械/电子部件的生命周期），并且可以公开收集安全事故的信息（报纸、报告等）。因此，可以使用统计和概率等数学工具来估计与安全相关的风险的可能性因素。而就安全而言，安全事件的信息通常不是全部都可以访问的[68]。此外，成功攻击的可能性很大程度上取决于许多不确定因素，如攻击者的能力、动机以及日益发展的攻击技术。这使得安全规程中的定量评估变得困难。在估计之后，可能性和严重性被合并到一个风险等级中。通常，可以使用风险评估表进行组合。（如表2.2）

•在风险评估中，决策者根据风险分析结果决定哪些风险可以忽略，哪些风险应该处理。最高风险将首先以最高优先级处理，较低风险将被忽略或稍后处理。

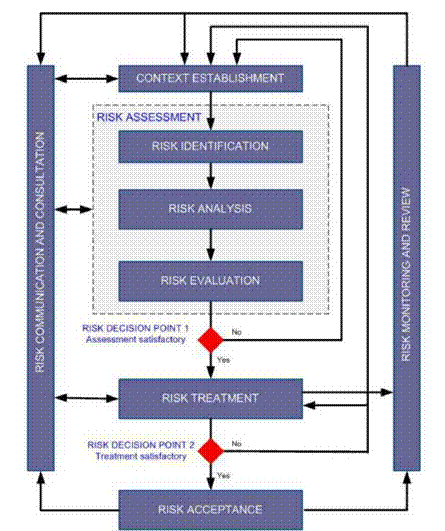


图2.1:ISO 27005风险管理框架

除了风险评估，风险管理还可以包括其他活动：环境建立、风险处理、风险沟通。背景建立旨在为风险评估准备所有必要的输入信息（如操作、系统、设置风险评估标准、风险接受标准等信息）（见图2.1）。上下文建立被认为是影响最终结果的关键活动[83]，

[88]. 风险处理是指通过实施不同的处理方案，降低风险评估后的风险。传统上，有四类治疗方案：风险规避、风险降低（或缓解）、风险接受和风险转移[68]。风险沟通是在安全经理和其他利益相关者（如开发商、客户、供应商[89]、[90]）之间交换和共享风险信息的活动。图2.1展示了ISO 27005安全信息风险管理标准提出的完整风险管理框架。该框架与同一组织的一般风险管理指南ISO 31000:2009[91]中提出的框架一致。

2.3.3           系统设计过程

安全性和安全性对系统设计都有重大影响。它们不仅被认为是系统设计的补充，也是衍生系统设计的最重要目标之一[68]。例如，安全要求，如核工业中的单一故障标准，会导致子系统或组件的冗余、多样化和物理分离[92]。另一个例子是，在IT系统中，安全需求导致需要对网络进行细分，其中组件根据其功能和安全风险进行虚拟分离。这些措施或策略的实施对系统的体系结构有着巨大的影响。因此，在设计过程中越早考虑安全和安保要求，其实施就越有效，财务效率也就越高[68]，[93]。这种思想被用于设计关键系统，如飞机。在航空工业中，产品的设计是根据V循环过程展开的，该过程包括功能需求识别、需求实现和需求验证。为了在设计过程的每个步骤中考虑到安全问题，标准ARP4754提出了第二个V循环过程，该过程涵盖安全需求识别、实施和验证（ARP4754标准在航空领域广泛用作开发指南）。两个过程并行展开，如图2.2所示。然后，当网络安全成为航空业的一个重要问题时，该行业采用了与网络安全评估相关的第三个V周期过程，该过程在标准ED-202A/DO-326A[94]中提出。网络安全过程与其他两个过程同时进行。

2.3.4           操作与人为因素

不仅在系统开发中，而且在运行中，都应考虑安全和安保。与安全和安保相关的风险可以通过“非开发”活动（如维护、检查、监控）来降低。维护、定期检查、变更记录和活动日志对系统的保持起着重要作用

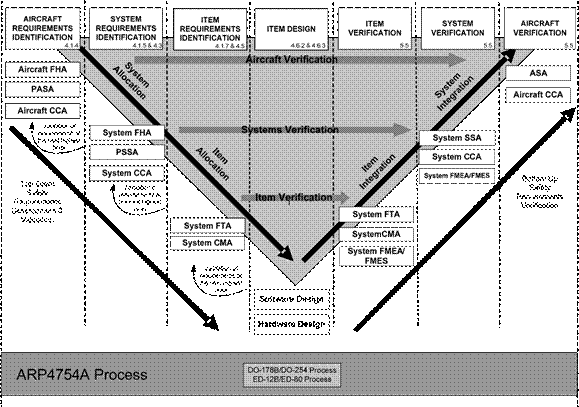


图2.2：标准ARP4754[75]中的双V循环过程

安全操作[95]和安保[96]。一方面，这些活动被视为降低风险的预防措施。另一方面，这些活动有助于产生运行反馈，以制定新的技术措施或更新。除了这些活动外，员工培训、应急计划制定和定期测试练习也是确保运行中系统安全的其他活动[97]、[98]、[92]。这些活动涉及操作中的人为因素，这被视为安全事故的重要来源。在安全方面，三里岛事件是由操作员故障引起的典型核事故，引起了对人为因素的关注[68]。人类因素在安全（网络安全）中的作用在20世纪90年代初黑客Mitnick实施社会工程攻击后得到承认

[99].

2.4风险管理的标准和方法

2.4.1安全

IEC 61508是国际电工委员会（IEC）为电气/电子/可编程电子（E/E/PE）安全相关系统制定的安全标准。

2.4. 风险管理的标准和方法



本标准自20世纪80年代计算机系统在行业内越来越多地使用以来制定。一方面，采用基于计算机的系统带来了许多安全优势、功能改进和经济效益。另一方面，这种采用会增加系统的复杂性，并在设计这些系统以防止危险故障方面带来挑战[100]。IEC 61508指南旨在将所有E/E/PE安全相关系统中的这些故障降至最低。本标准有助于确定要求，以确保系统的设计、实施、运行和维护达到所需的安全完整性水平（SIL）[101]。

ARP4754、ARP4761构成航空电子系统安全分析和开发指南。其中，ARP4754标准指导高度集成航空电子系统的适航认证过程。硬件和软件的详细开发过程分别在DO-254标准和DO-178C标准中处理。DO-254和DO-178标准与ARP4754标准之间的接口为开发保证级（DAL）。DAL通过ARP4754中提到的过程分配给软件/硬件系统，并通过DO-254和DO-178C中提到的过程详细实施。伴随着4754标准，ARP4761标准提供了风险评估技术方面的深度指导，以执行ARP4754标准中规定的流程。为了进行风险评估过程，结合使用不同的技术，如故障树分析、马尔可夫分析、故障模式影响分析

[102].

特定作战风险评估（SORA）是一种专门针对无人机作战的风险评估方法。该方法得到欧洲航空安全局（EASA）的认可，作为满足欧盟要求的一种手段。一方面，该方法为UAS运营商和航空局提供了管理流程（如运行验证）背景下的沟通工具[103]。另一方面，该方法为无人机建造商、硬件/软件制造商提供了一种工具，用于在开发的早期阶段预测与安全相关的必要要求[103]。目前，SORA方法侧重于安全方面，而忽略了安全方面。[104]中给出了该方法的更详细描述。

2.4.2安全

ISO 27005标准2.3.2部分解释了本标准。我们提醒您，它是在组织中实施信息安全风险管理的指南。本标准并未提供具体的风险管理方法，而是构成了风险管理流程的框架[90]。该框架包括六项活动：背景建立、风险评估、风险处理、风险接受、风险沟通和风险监测/审查。除了组织中的信息安全之外，ISO/IEC 27005还被称为确保网络物理系统中的网络安全的指南，其中IT部分和物理部分同时存在并相互作用。

IEC 62443是一个风险管理行业标准，用于确保工业自动化和控制系统（IACS）的安全。本标准提供了开发、集成和评估网络安全威胁组件的流程和最佳实践。IEC 62443基于ISO 27005系列的概念，并对其进行了改进，以适应操作技术（OT）和信息技术（IT）之间的差异[83]。然而，物联网（IoT）设备与IACS的集成加速了OT和IT的融合，并给IACS带来了新的网络安全威胁。因此，Leander等人[105]认为，在某些情况下，当前的IEC62443标准不足以应对物联网设备给IACS带来的新的安全威胁，例如跨区域通信和软件更新的处理。

ED202A/DO326是适航安全流程指南，由两个工业委员会航空无线电技术委员会（RTCA）和欧洲民用航空设备组织（EUROCAE）制定。本文件的目的是在APR4754标准中定义的当前飞机开发和认证过程中增加处理故意未经授权的电子威胁的新过程。适航安全流程包括三个主要部分：（1）认证活动，（2）风险评估相关活动（相当于ISO/IEC 27005标准中的背景建立和风险评估活动）和（3）安全开发活动（相当于ISO/IEC 27005标准中的处理活动）[106]。ED202A标准之后是ED203标准，该标准对活动进行了更详细的解释。

风险协调分析方法（MEHARI）是一种开源信息风险管理方法。它由CLUSIF（法国信息安全俱乐部）开发和维护，CLUSIF是自20世纪90年代中期以来由信息安全领域的公司和专家组成的协会。该方法旨在根据ISO/IEC 27005[107]实施风险管理。MEHARI的最新版本不仅根据ISO/IEC 27005中的活动提供了详细的定义、过程和具体示例，还提供了漏洞、安全事件和安全解决方案方面的知识数据库；用于评估安全服务质量的问卷。由于MEHARI最初的应用领域是“组织中的信息安全”，因此现有的数据库和支持工具适用于该领域。然而，CLUSIF还提供了建立新知识数据库的指导，以使MEHARI适应其他特定系统，如工业自动化和控制系统（IACS）、监控和数据采集（SCADA）等[108]。

E-safety Vehicle Intrusion proTected Applications（EVITA）[109][110]是一项由欧盟委员会和一个由汽车制造商、汽车供应商、安全专家、硬件/软件专家组成的财团资助的研究项目。本项目的目标是设计、验证、原型化模块化、经济高效的安全解决方案，以保护由电子控制单元（ECU）、电子传感器和电子执行器组成的车载网络的敏感数据。为此，本项目提出了一种安全需求分析方法。尽管未提及ISO/IEC 27005标准的合规性，也不是一个目标，但该方法可涵盖ISO 27005框架的一些重要活动，如背景建立、风险评估和治疗活动。

2.5安全分析技术

2.5.1危险与可操作性分析

危险与操作（HAZOP）是一种系统和结构化技术，在世界范围内用于识别系统的危险及其操作问题。换句话说，该方法旨在识别与给定系统相关的风险场景。该方法基于一个重要论点，即风险情景是由系统偏离预期设计引起的[111]。因此，为了确定情景，HAZOP侧重于寻找偏差（状态、行为等）并推断这些偏差的后果。偏差识别过程依赖于结合过程参数（如温度、流量、压力）使用指导词（少、多、晚、早、快、慢等）[112]。基于这些话，负责人集体讨论不同的偏差，如“电机运行速度超过设计意图”。由于只关注设备和工艺参数的故障，该方法不考虑与人为因素相关的情景。HAZOP分析最早出现于20世纪60年代，旨在识别化学设施中可能存在的危险，以消除导致重大事故的任何来源，如有毒物质释放、爆炸和火灾。几十年来，HAZOP已扩展到其他类型的设施。CHAZOP（计算机危险和可操作性研究）是HAZOP技术的衍生版本，但专门用于控制和安全系统（PLC、I/O卡、断路器、执行器、本地控制面板等）[113]。该版本提出了新的指导词和参数，如无信号、超出范围信号、无电源、无通信、I/O卡故障、软件编程、不正确/不充分和网络攻击[113]。EHAZOP（电气危险和可操作性研究）是HAZOP技术的另一个外推版本，但它专门用于电气系统（发电、变电、输电和配电…）。该版本还提出了新的指导词，如电涌、24 VDC电源故障、闪络、变压器事故变电站母线故障、缺乏维护等。

2.5.2 SIL分析

安全完整性水平（SIL）表示为达到工业过程可接受的风险水平所需的安全措施性能水平。根据按需失效概率（PFD）测量所需的安全性能。SIL一词在世界范围内使用，并在IEC 61508中标准化，该标准为安全仪表系统的设计、安装、操作、维护和测试提供了指南[114]。本标准提出了具有不同PDF值的4个SIL等级，如表2.3所示。在安全过程中，SIL根据风险降低量分配给安全措施

|  |  |  |
| --- | --- | --- |
| 恳求 | 低需求 | 高需求 |
| SIL | PDF平均值 | 故障/小时 |
| 1 | [10−2, 10−1] | [10−6, 10−5] |
| 2 | [10−3, 10−2] | [10−7, 10−6] |
| 3 | [10−4, 10−3] | [10−8, 10−7] |
| 4 | [10−5, 10−4] | [10−9, 10−8] |

表2.3:IEC61508[114]中的SIL值

必须确保系统处于安全状态。根据Summers的工作[115]，SIL分配有以下几种基本技术：

•修改后的HAZOP是HAZOP分析的延伸。这是一项基于团队对严重性和可能性的定性理解的主观任务。因此，这在很大程度上取决于团队成员的经验。因为这种方法非常主观，它要求团队成员不仅了解所考虑的系统，而且了解公司可接受的风险承受能力。此外，各项目SIL分配团队的人员之间需要保持一定的一致性。

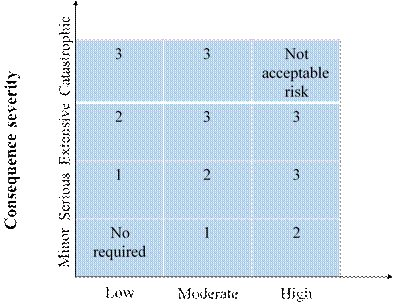
|  |  |
| --- | --- |
| SIL | 结果 |
| 4 | 社区死亡的可能性 |
| 3 | 多人死亡的可能性 |
| 2 | 可能造成严重伤害或一人死亡 |
| 1 | 可能发生轻伤 |

表2.4：基于结果的SIL分配[115]

•仅后果评估是一种SIL分配技术，仅基于后果的严重性，而忽略风险情景的可能性。因此，在不考虑其可能性的情况下，所有可能导致死亡的情景都将分配相同的SIL。这是最简单的技术，因为可能性通常很难估计。当历史数据受到限制时，这种技术是值得赞赏的[115]。SIL分配的表格决策示例如表2.4所示。

•风险矩阵是炼油、化工和石化公司最常用的技术之一[115]。与仅结果不同，该技术基于严重性和风险情景与SIL的可能性之间的相关性。为了成功应用该技术，必须充分了解过程、系统和相关风险，以便对可能性和严重性进行定性估计。SIL分配的风险矩阵示例如图2.3所示

•风险图是SIL的定性技术。在该技术中，SIL通常基于四个因素进行分配：后果或严重后果（C）；频率和



**可能**

图2.3:ANSI/ISA 84.00.01标准中SIL分配的风险矩阵

曝光时间（F）；避免危险事件的可能性（P）；以及意外发生的概率（W）[114]，如图2.4所示。最后三个因素的组合：F、P、W代表风险情景的可能性。换言之，SIL始终根据风险的性质进行分配：结果和可能性，然而，可能性由其贡献者参数（F、P、W）代替。

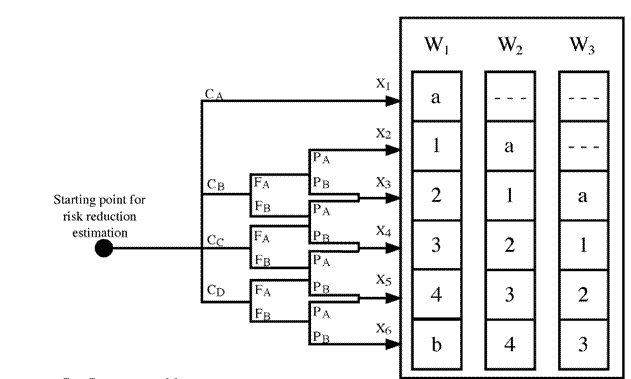
•定量评估：在该技术中，安全措施的SIL基于对相关事件可能性的定量估计而确定。该方法要求彻底了解事件的潜在原因以及每个潜在原因的估计概率。因此，该方法适用于事件历史信息非常有限的情况，因此定性确定可能性非常困难[115]。为确定所需SIL，可接受或可容忍的风险概率除以计算的工艺需求，如下所示：

可容忍风险概率

按需失效概率=

工艺需求

此时，我们可以发现SIL与2.3.2中提到的风险水平非常相似。这两个术语都与事件或风险情景的严重性和可能性相关，可用于风险评估活动。然而，这仍然是两件不同的事情。风险水平是可能性和严重性的组合，代表系统或流程的性质。当实施安全措施时，风险水平可能会发生变化（我们希望它降低到可接受的水平）。同时，SIL代表性能



a=无特殊安全要求，b=单一措施不充分，---=无需

图2.4:SIL分配的风险图[114]

安全措施的目标。当选择实施安全措施时，SIL不会改变，但会提出一个问题：“所选措施是否满足要求的SIL？”。

2.5.3故障树分析

故障树分析（FTA）是一种基于图形的系统安全分析技术。它最早由贝尔公司在20世纪60年代开发并应用于航空航天应用[86]，然后它变得流行并广泛应用于其他关键系统，如核电、汽车、医疗系统[116]。这种技术可以帮助分析员评估给定的系统，并理解和预防相关的风险。通过应用FTA，分析员可以创建一个可视化模型，说明设备故障和人为错误如何导致事故事件。根据该模型，分析员可以确定最危险的条件，并提出安全措施或建议。因此，FTA通常在系统开发期间执行，其结果通过预测和预防未来问题影响设计[93]。

FTA过程包括两个步骤。第一步是展示不同组件故障或特定环境条件如何组合导致给定系统故障。此步骤通过选择不希望出现的事件（UE）作为图的顶部节点开始。UE是被识别为令人反感和不想要的任何事件。然后，通过演绎推理，确定对UE有贡献的中间事件，并将其作为分支节点放置到图中。分支节点和顶部节点通过不同的逻辑门连接，如图2.5所示的OR、and、XOR。重复演绎推理过程，以确定已识别中间事件的原因，直到达到无法分解为较小事件的基本事件。在构建树图之后，布尔代数被应用于识别割集，割集是导致UE的必要和足够的基本事件的最小组合。第二步是基于割集中基本事件的概率来计算UE的概率。该步骤的结果不仅有助于分析员识别UE的全局可能性，而且有助于分析员识别故障树中所有事件对UE概率的贡献的重要性。

虽然传统的故障树方法非常成功并得到了广泛的应用，但它也存在局限性。传统的故障树分析方法在构建树状图的过程中无法对事件的时间序列进行建模。例如，如果我们有一个包含两个组件a和B的系统，并且有两种假设情况：“如果组件a在B出现故障之前出现故障，则系统不会出现故障”和“如果组件B在a出现故障之前出现故障，则系统不会出现故障”；FTA无法区分这些情况。为了克服这一限制，提出了不同的方法来创建动态故障树分析，如新的逻辑门[117]，基于贝叶斯网络的方法[118]，新的代数框架[119]，基于蒙特卡罗的方法[120]。作为另一个限制，传统的故障树分析无法克服基本事件故障数据的不确定性。对于许多复杂的大型系统，通常很难精确地确定所有基本事件的概率。这会导致不可靠的结果。为了克服这一限制，Tanaka等人[121]提出在FTA中使用模糊理论。然后，其他研究人员采用这一思想进一步发展了模糊故障树分析（FFTA）[122][123]，[124]。

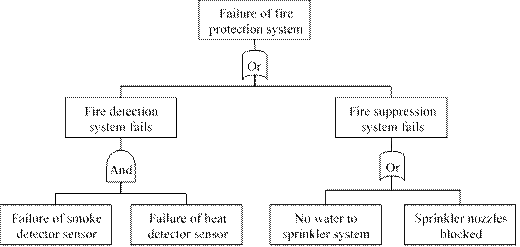


图2.5：故障树分析示例[125]

2.5.4事件树

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **即** |  | **安全措施** | |  | **结果** |
| 漏气 | 气体检测 | 隔离阀A关闭 | 隔离阀B关闭 | 排污阀打开 |  |
|  |  |  |  |  |  |

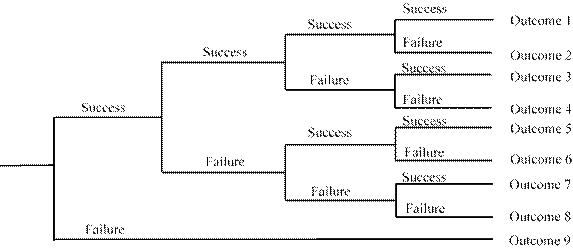


图2.6：事件树图示例[126]

事件树分析是另一种基于图形的分析技术，于20世纪70年代引入核反应堆项目[127]，随后被航空、化学等其他行业采用。该技术通常应用于系统设计和开发的早期阶段，以识别安全问题和设计安全措施，而不是在测试或事故后采取纠正措施[93]。它有助于对初始事件（IE）引发的潜在事故中的事件序列（或风险情景）进行归纳和定性评估。基于图形方法，该方法侧重于从逻辑和概率角度说明IE导致的事故与相关安全措施失效之间的关系。在偶数树图形中，事故场景（或风险场景）由三个元素建模：初始事件（IE）、轴心事件和结果。IE位于图形顶部，表示系统中的扰动（如火灾、气体泄漏、压力损失），需要操作员响应或安全系统响应，以避免意外后果。透视事件是图形树分支中IE之后的直接点（有时称为分支点）。枢轴事件表示安全系统在响应初始事件时的成功或失败。结果是树形图的终点，它表示某些类型的损失，例如人员的生命损失或伤害/疾病、设备或财产的损坏或损失、任务失败，其后果可能从轻微到严重不等。事件树的示例如图2.6所示。事件树图给出了可能结果的简短描述，并提供了估计其频率/概率的工具。初始事件和枢轴事件的概率可以从历史数据或其他分析（如故障树分析）的结果中发现[126]。通过将IE和pivot事件的概率相乘来计算结果概率。

2.5.5领结分析

蝴蝶结分析是一种基于图形的安全风险评估技术，在石油和天然气、航空、采矿等高风险行业已得到广泛应用[128]。该技术通过蝴蝶结形状的图形模拟安全事故。此图表的主要元素包括顶级事件、威胁、后果和障碍。顶部事件是领结的中心点，通常被定义为某种损失，如石油和天然气中的“安全壳损失”和航空中的“分离损失”[128]。威胁位于顶部事件的左侧，代表顶部事件的原因，而后果位于顶部事件的右侧，代表顶部事件的后果或事故的后果。每个领结图只有一个顶部，即使它是由多种威胁引起的，并导致多种后果。障碍在顶级赛事的两侧。它们说明了预防、控制或缓解事故的不同措施

[129].

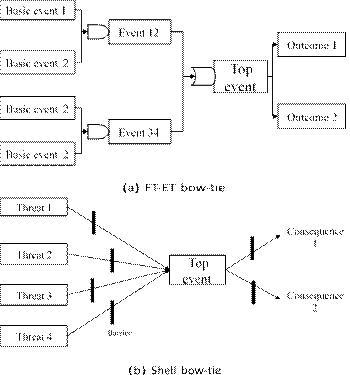


图2.7：领结图示例[128]

虽然领结很受欢迎，但它缺乏一致的方法[128]。至少，我们可以认识到至少两种在图形结构、目的和风险量化方面不同的方法，也被称为“蝴蝶结分析”。第一种方法是故障树和事件树的组合，如图2.7a所示。在这种方法中，领结图从故障树开始，在顶部事件中收敛，然后使用事件树发散。这种方法中的障碍通常不会直接在图表中显示，而是在安全措施的“失败/成功事件”形式下显示。利用故障树和事件树分析，这种方法允许分析员分解并详细分析可能发生的事故。因此，该方法用于计算后果概率[130]，[131]。在Salvi等人[132]的工作中，该方法的定量结果用于证明安全完整性水平（SIL）下安全措施的性能要求。另一方面，该方法与传统的FT和ET具有相同的困难，如数据不确定性[133]、非动态模型[134]、模型不确定性[135]。第二种方法是贝壳领结。这种方法提供了一个简单的蝴蝶结图，而不是FT和ET的组合，如图2.7b所示。图的左侧包括多个威胁，这些威胁本身可能导致顶部事件，而没有任何中间事件。然后，顶部事件在左侧造成单一后果。在这种方法中，屏障元素直接显示在图形的左侧和右侧。与基于FT-ET的图相比，shell-bow-tie图具有更高的抽象级别和更少的特定信息，因此计算后果概率的能力较弱。然而，贝壳蝴蝶结更容易理解。与基于FT-ET的图形相比，它的符号更少，并且更清楚地说明了安全屏障。这使得shell蝴蝶结成为沟通[128]、[136]（例如操作、用户、管理员）和“确保每个故障路径都有障碍或控制”的良好工具[137]。

2.5.6马尔可夫分析

马尔可夫分析或马尔可夫过程是一种基于图形的技术，用于建模系统的状态转换和计算（故障）状态发生。系统状态是子系统或组件（工作/故障）状态的组合。例如，一个系统有两个组件a和B；有不同的系统状态，例如（A-工作，B-工作），（A-故障，B-工作），（A-工作，B-故障），（A-故障，B-故障）。在马尔可夫分析中，假设系统状态随时间从一种状态持续变化到另一种状态，并且未来的系统状态仅取决于当前状态。这些状态转换由状态转换图建模。该图显示了系统的不同状态、过渡方向以及过渡速率，如图2.8所示。状态转移图用于建立一组一阶微分方程，表示不同状态概率随时间的关系。通过求解这组方程，我们得到了失效状态的概率。

与其他技术相比，马尔可夫分析既有优点也有缺点。它的优点是它可以考虑一些其他技术无法考虑的方面，如定时、修复活动、容错[93]。因此，它是进行精确定量分析的有力工具[138]。然而，这项技术学习起来相当复杂，需要分析师具备良好的数学知识。此外，当所考虑的系统变大时，图形可能会变大，难以读取和跟踪[93]。出于这些原因，2003年，Bouissou等人[139]提出了布尔驱动马尔可夫过程（BDMP）——一种故障树分析和马尔可夫分析的组合。这项技术具有两个优点：（1）易于理解，

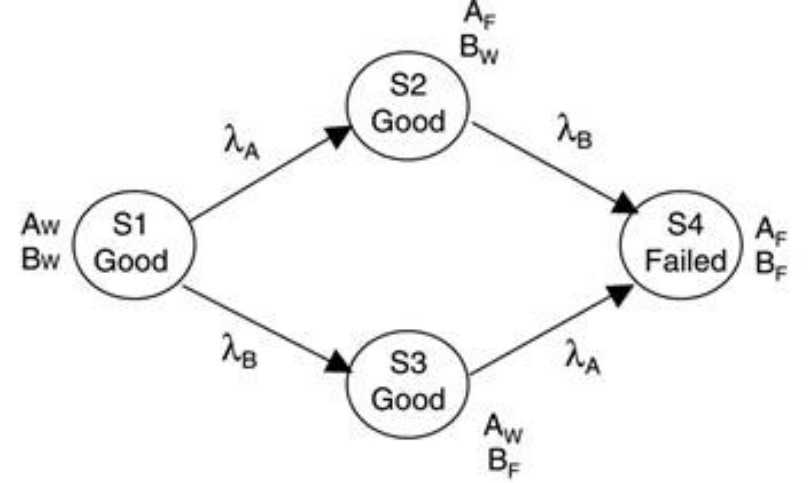


图2.8：状态转换图[93]

创建和跟踪（故障树），（2）精确量化（马尔可夫分析）。

2.5.7 Petri网

Petri网（PN）是一种分析技术，用于识别危险或事故场景，但不用于计算定量概率。为了识别危险，PN分析提供了一种工具，在广泛的抽象层次上以图形方式对系统进行建模。与马尔可夫模型一样，PN模型也可以说明不同的系统状态（包括故障状态），并处理定时、状态转换和修复活动。这些模型的优点在于，它们可以说明系统中硬件、软件和人为因素之间的联系。然而，由于PN分析的复杂性，其在系统安全分析中的应用不如Faul树或事件树等其他技术广泛。随着系统规模的增加，PN模型迅速变得庞大而复杂[93]。因此，其使用很少应用于大型系统，且仅限于检查软件控制系统。

2.5.8失效模式与影响分析

故障模式和影响分析（FMEA）是一种自下而上的技术，用于分析系统的安全性，并确定降低风险的优先措施。它最早于1949年由美国陆军引入，随后被广泛用于分析航空航天、汽车、核、机械和医疗等行业的安全[140]。在FMEA中，分析的重点是检查/识别所有组件故障及其对操作、系统和环境的影响。然后，组件故障率和影响严重性的组合解释了组件故障的风险，并指出了相关风险降低行动的优先级。Pierre等人[141]提出了一种解决方案，可以从用UML/SysML编写的系统设计中自动生成FMEA分析。此解决方案有助于改进系统设计和分析过程之间的交互。在被称为故障模式、影响和关键性分析（FMECA）的FMEA的更详细版本中，还考虑了检测部件故障能力的信息，以评估风险。由于需要部件信息（如故障模式、故障率），FMEA通常在系统详细设计可用或新详细设计变更时执行。这种技术的优点在于它相对容易理解，成本低廉，并能提供有意义的结果[93]。然而，它也有一个弱点。第一个是分析质量取决于用户的体验，因此结果可能是主观的，而不是稳健的[142]，[138]。第二个问题是FMEA无法识别所有风险情景。因为该技术着眼于单个部件故障，而事故可能由部件故障的组合引起[93]。

2.5.9摘要

|  |  |  |  |
| --- | --- | --- | --- |
| 技巧 |  | 风险评估 |  |
| 风险识别 | 风险分析 | 风险评估 |
| 危险品 | 基于引导词  表格  因果危害后果 | X  （来自其他来源） | 与标准进行比较，确定风险等级 |
| SIL分析 | X  （不是焦点） | X  （来自其他来源） | 多途径  确定措施的目标绩效 |
| 故障树 | 演绎推理，  图模型  基本事件顶级事件 | 定量概率传播 | X  （不是焦点） |
| 事件树 | 归纳推理图模型  顶级赛事结果 | 定量概率预测 | X  （不是焦点） |
| 领结 | FT，ET的组合  说明安全屏障。 | FT，ET的组合 | X  （不是焦点） |
| 马尔可夫过程 | X  （不是焦点） | 定量系统状态概率 | X  （不是焦点） |
| Petri网 | X  （不是焦点） | 定量系统状态概率 | X  （不是焦点） |
| FMEA | 归纳推理  表格  失效模式-效应 | X  （来自其他来源） | 与标准进行比较，确定风险等级 |

表2.5：风险评估技术比较

上面，我们介绍了广泛用于风险评估的八种基本技术。其中每一项都侧重于风险评估的一些任务（见表2.5）。对于风险识别任务，我们可以使用HAZOP、故障树、事件树、蝴蝶结和FMEA。对于风险分析任务，故障树、事件树、领结、马尔可夫过程、Petri网可以提供准确的定性结果。对于风险评估任务，Hazop、SIL分析和FMEA给出了比其他技术更详细的说明。此外，每种技术在不同方面都有优势，如沟通、推理和文档。因此，在对关键系统进行风险评估时，可以结合使用各种技术。例如，FMEA、故障树、Hazop可用于进行初步系统安全评估（PSSA）

2.6. 安全分析技术

-定义见ARP 4761航空电子系统标准[143]

2.6安全分析技术

2.6.1从SIL水平到SAL水平

与安全规程类似，安全规程涉及设计、实施和验证某种保护。因此，SIL概念在安全规程中可能很有用。然而，原始SIL分析在应用于安全规程[144]、[145]时存在局限性。SIL系数仅代表按需故障率方面的目标性能，而安全性通常要求对基于网络的攻击和可利用的软件或硬件条件具有弹性。基于SIL概念，Kube等人[144]提出了安全保证水平（SAL）的基本概念，该概念表示针对安全控制或设计功能的妥协的目标组件弹性。SAL的概念在ISA99/IEC62443[145]，[87]标准中得到采纳和进一步发展，该标准涉及组织运营技术（OT）领域中工业控制系统的网络安全。这些标准使用安全保证级别（SAL）来描述确保系统安全所需的保护。安全保护由七个基础要求来描述：（1）访问控制，（2）使用控制，（3）数据完整性，（4）数据机密性，（5）限制数据流，（6）及时响应事件，和（7）资源可用性。SAR定义为4个不同级别（1, 2, 3，4），随着表2.6中恢复的基础要求的严格性的增加。

|  |  |
| --- | --- |
| 萨尔 | 描述 |
| 萨尔1 | 防止因果或巧合侵权  偶然或巧合的违规行为通常是由于安全策略应用不严造成的 |
| 萨尔2 | 使用简单手段防止故意违规  这意味着攻击者不需要详细了解受攻击的安全性、域或特定系统 |
| 萨尔3 | 使用复杂手段防止故意违规  攻击者需要具备目标系统的安全和域操作方面的优势知识才能进行此类违规行为 |
| 萨尔4 | 使用扩展资源的复杂手段防止故意违规  与SAL 3类似，但攻击者拥有扩展的资源，如高性能计算机、延长的时间段 |

表2.6:IAS99/IEC62443[145]中的SAL

2.6.2安全方面的HAZOP

如上所述，危险与操作（HAZOP）的基本原理是，不安全情况是由系统的行为偏差引起的。为了使此技术适应安全规程，需要进行一些修改。Winther等人[146]提出了一种基于HAZOP的技术，用于识别与给定关键系统相关的不同安全威胁。安全威胁是根据新的指导词和安全属性（如披露、操纵、拒绝）的负面影响进行识别的。Wei等人[147]提出了另一种基于HAZOP的方法，专门用于嵌入式系统。该方法使用计算机应急响应团队（CERT）提出的攻击分类法作为新的指导词，并通过序列图模拟系统行为。Srivatanakul等人[148]和Daruwala等人[149]建议使用原始HAZOP和用例模型对软件和硬件进行安全分析，而不是修改或更改原始的指导词。在这种方法中，应更广泛地理解引导词的手段，并要求用户更具创造性。使用基于HAZOP的概念迫使分析员考虑异常情况。然而，与预定义的指导词列表相关的抽象级别也可能隐藏不被考虑的风险[68]。

2.6.3从故障树到攻击树

攻击树（FT）分析是一种基于树形图的技术，用于识别针对给定系统的可行攻击并确定安全对策的优先级。该技术被认为是对安全规程的安全技术故障树分析（FT）的改编[148][68]。AT分析的概念与FT分析的概念非常相似。攻击树作为树的顶部节点说明了攻击的目标。攻击者为达到攻击目标所需达到的中间目标由图的中间节点表示。该图以表示基本攻击动作的不同叶节点结束。节点仅由两个逻辑门（和/或）连接，而不是FT分析中的至少四个逻辑门。AT分析的概念由Schneier于1999年首次提出[150]，并在支付系统[68]、[151]的背景下进行了说明。在这项工作中，作者评估了风险，并根据定性估计的攻击成本确定了应对措施的优先级。自第一次演示以来，AT树已被采用并进一步扩展。这种方法通常用于许多不同的应用或工业领域，如汽车[152]、智能健康[153]、工业控制系统[154]、网上银行[155]。Ekstedt等人[156]，Kordy等人[157]将传统攻击树图扩展到攻击-防御树，以模拟安全对策。关于对策和风险评估，Jürgenson等人[158]建议使用不同的参数，如成本、攻击的可行性和攻击者所需的技能水平。还提出了模糊理论[159]和博弈论[160]来改进分析。

2.6. 安全分析技术

2.6.4基于FMEA的技术

失效模式影响分析是一种识别和理解可行失效模式影响的安全分析技术。由于其系统性、易于理解和“自我记录”，这项技术启发了安全学科的工作。文献中介绍了几项将FMEA应用于安全性的工作，并进行了一些修改。例如，Aagedal等人[161]在CORAS欧洲项目的安全背景下使用FMEV；Gorbenko等人[162]提出了用于Web服务分析的入侵模式和影响分析（IMEA）；Schmittner等人[163]将FMEA用于汽车安全；Bowles等人[164]提出了用于软件分析的威胁效应分析（TEA）。这些工作的原则是，他们不关注故障模式，而是关注可行的威胁/攻击模式及其对给定系统和操作的影响。威胁/攻击模式通常与安全属性（机密性、完整性和可用性）的丢失有关，并由此推断。Schmittner等人[73]提出了故障模式、脆弱性和影响分析（FMVEA）技术，以实现系统的联合分析方法（安全和安保）。作者提供了安全风险场景的可视化模型，以及进行安全和安全分析的FMEA的详细过程。

2.6.5领结安全性分析

蝴蝶结（BT）分析是一个强大的工具，可以直观地对风险情景进行建模，并在不同的利益相关者之间进行沟通。因此，采用这种技术进行安全分析可能会很有趣。SANS Institute company[165]的一份报告认为，安全分析可以采用与安全分析相同的方式进行BT分析，而不会改变任何概念。美国海岸警卫队还发布了关于如何应用BT技术识别和应对针对海上运输系统的网络攻击的指南[166]。在本指南中，网络攻击被高度抽象地提到，如黑客活动主义者、内部威胁。为了软件系统的网络安全，来自PI Square的Harry[167]使用Shell蝴蝶结对攻击路径和防御措施进行可视化建模。然而，与其他安全分析技术相比，蝴蝶结分析在安全学科中的适用性非常有限，尤其是在学术领域。通过使用谷歌学者工具，我们发现很少有针对这一主题的作品。Abdo等人和Bernsmed等人完成了与该主题相关的最重要的工作[168]。Abdo等人[169]将FT-et领结与AT结合起来，对工业控制系统进行安全-安保联合分析。这种方法的优点在于，它允许考虑由安全问题和安全问题之间的耦合引起的风险场景。Bernsmed等人[168]通过使用通用的外壳BT图，可视化了恶意活动、随机故障、安全对策和安全屏障。作者还提出了一种基于威胁可能性和后果严重性的风险量化方法。

2.6.6安全的马尔可夫过程

马尔可夫过程（BDMP）是安全规程中使用的精确风险量化工具。这种技术也用于安全规程中。Ye等人[170]使用马尔可夫过程观察和分析计算机和网络系统的网络安全风险。本文的工作成果用于构建一个实时网络攻击检测系统。晓林等[171]提出了一种基于马尔可夫博弈论的网络信息系统风险评估模型。该模型包括两个马尔可夫链。一个是对威胁传播进行建模并发现隐藏的风险，另一个是对系统管理员实施的修复过程进行建模。该评估结果用于构建自动工具生成防御方案。Lakhno等人[172]也采用了马尔可夫过程和博弈论之间的耦合来检验智能城市概念的网络安全。与安全规程一样，马尔可夫过程的局限性在于难以读取、跟踪和建模复杂系统。出于这些原因，Piètre Cambacédès等人[173]将布尔逻辑驱动的马尔可夫过程（BDMP）概念从安全域改编为安全域。安全BDMP将马尔可夫过程与攻击树相结合，而不是故障树。攻击树本质上是静态的，只能在不考虑时间的情况下检查独立事件，而BDMP是动态的，可以检查简单的依赖关系。BDMP允许对攻击序列进行建模，但也允许对攻击检测等安全对策进行建模[174]。

2.6.7安全性的Petri网

McDermott在[175]中首次介绍了Petri网在安全分析中的应用。在这项工作中，作者建议在渗透测试的背景下使用Petri网对网络安全风险进行建模，并认为Petri网可以结合一些缺陷对复杂的攻击进行建模，这对于其他基于图的技术（如攻击树）来说是困难的。在McDermott的工作之后，基于Petri网的安全规程技术在多个方向和各个工业领域得到了进一步发展。为了减少Petri网在复杂性和时间消耗方面的缺点，Zhou等人[176]提出了一种在Internet入侵分析环境下将攻击树覆盖到Petri网的方法。这种方法允许利用攻击树技术（降低建模成本）和Petri网技术（允许模型安全措施）。Fu等人[177]建议将Petri网与大数据分析相结合，以评估网络物理系统的网络安全性。然而，由于复杂性，这种方法仍然需要专家参与数据挖掘，以提高评估的准确性。Jianfeng等人[178]提出了一种基于Petri网的方法来分析化学过程中的网络安全。在这种方法中，Petri网技术被扩展以检查攻击时间（例如，时刻、持续时间）。

2.7. 安全和安保综合办法



2.7安全和安保综合方法

如前几节所述，安全和安保有许多相互作用。首先，这些术语的定义非常接近。它们都涉及到系统的保护。失去安全保护可能导致失去安全。Lisova等人[179]认为，“一个连接的安全关键系统如果不安全就不安全”。其次，安全和安保领域在风险、风险评估和风险管理方面有着相同的概念。许多安全评估技术起源于安全领域中使用的技术。最后，安全和安保是系统开发和运行中的基本问题。因此，自然需要将安全和安保方面整合到一个综合风险评估方法中。在学术界，有一些作品与这一主题有关。例如，Reichenbach等人[180]介绍了一种基于安全完整性等级（SIL）的威胁脆弱性和风险评估（TVRA）技术的综合方法。该方法允许解决安全问题对安全的影响。Plósz等人[181]提出了一种将FMEA技术与STERE模型相结合的方法——一种安全威胁分类（欺骗、篡改、否认、数据泄漏、拒绝服务、特权提升）。通过同时考虑安全评估和安全风险评估的共性，这种综合方法可以减少时间和精力。Fovino等人[182]提出在风险评估方法中结合攻击树和故障树。为此，作者提出了一种将攻击树集成到预构建故障树中的技术，以扩展传统风险分析结果的可用性，同时考虑潜在的恶意攻击。同样，Abdo[169]使用攻击故障树来共同分析安全性。然而，作者认为，不应基于相同的概率尺度来处理安全情景和安全情景。因为决策者不知道不可接受的风险是由安全相关原因还是安全相关原因产生的。因此，作者建议基于两个术语可能性部分来评估风险水平：一个用于安全，一个用于安全。Puys等人[183]提出了一种基于安全风险评估的工业控制系统网络安全评估方法。在这种方法中，安全风险评估提供了对网络安全攻击场景建模的功能。这种方法利用了一个事实，即工业系统通常在安全方面得到很好的分析。

在行业中，安全和安保综合方法才刚刚开始吸引人们的注意。例如，DO-326标准于2015年制定，旨在将ARP4761标准中定义的基于安全的流程扩展到网络安全。另一个例子是IEC 61508-IEC 63187标准的演变，该标准的制定是为了更好地适应当前的技术发展，并考虑到网络安全方面。

2.8结论

本章讨论两个不同的术语：安全和安全/网络安全。安全是指意外事件，而安全/网络安全是指攻击（恶意意图）。为了解决系统设计或运行中的安全问题，从业者和研究人员通常使用一个基本概念：风险——场景的可能性和严重性的组合。我们在文献中发现了不同的评估安全相关风险的方法。过去，安全和安保是通过单独的方法来考虑的。自上世纪初以来，安全方法已经发展起来。安全（网络安全）方法自20世纪80年代计算机和网络变得更加流行以来就已经发展起来。许多安全/网络安全方法是在安全领域现有方法的基础上制定的。由于安全和安保之间的相互作用，综合方法目前是一个有趣的课题。对于我们的重点应用-无人驾驶飞机系统（UAS），安全和网络安全现在都被公众所考虑。存在专门用于此应用的风险评估方法：特定操作风险评估。然而，这种风险评估方法只考虑安全，而不考虑网络安全方面。在航空航天行业，DO-326A标准中提到了安全风险评估方法。然而，这种方法似乎太大，成本太高，无法应用于商业UAS。因此，本文旨在开发适用于无人机的安全风险评估方法。第三章介绍了基于系统的安全风险管理。第四章介绍了我们基于操作的安全风险评估。

第三章

系统网络安全风险管理



目录

|  |  |
| --- | --- |
| 3.1导言。 | 46 |
| 3.2拟议方法。 | 46 |
| 3.2.1背景建立。 | 47 |
| 3.2.2风险识别。 | 49 |
| 3.2.3风险分析和评估。 | 51 |
| 3.2.4治疗。 | 53 |
| 3.3案例研究。 | 53 |
| 3.3.1结果分析。 | 57 |
| 3.4结论。 | 60 |

45

3.1导言

如第2章所述，网络安全在系统开发过程中起着关键作用。因此，学术界和工业界都引入了许多风险管理方法。然而，对于过度增长的UAS部门，没有适当的方法。这是我们开发和引入专门用于无人机系统（UAS）的网络安全风险管理方法的动机之一。此外，通过本研究，我们旨在将网络安全方面添加到SOGILIS公司（我们的工业合作伙伴）的发展过程中。风险管理的输出用作开发过程的输入，如图3.1所示

|  |  |  |
| --- | --- | --- |
| |  | | --- | | 风险管理方法  （本研究的重点） | |  |
| |  | | --- | | DO-178C标准 | |

图3.1：一般方法

3.2拟议方法

通过启发其他领域现有的风险管理方法，我们开发了一种简单的方法，包括四项主要活动。它们是“背景建立”、“风险识别”、“风险分析和评估”和“处理”，如图3.2所示。在建立活动的背景下，我们提出了一种收集和整理受保护系统状况的所有信息的方法，定义了风险管理的范围。对于风险识别活动，我们提出了一种基于攻击树方法和故障分析的方法来识别可能的安全风险。风险分析和评估活动旨在确定每个已定义风险的优先级。具有最高优先级的风险需要首先采用稳健的解决方案进行处理。在最后一个单处理活动中，我们定义了用于设计、验证安全解决方案的安全需求。这些活动将在本节剩余部分进行更详细的描述。

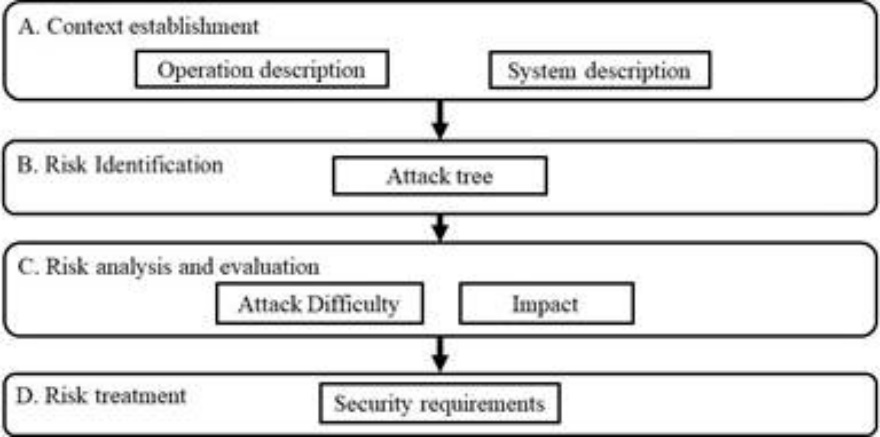


图3.2：拟议方法的工作流程

3.2.1背景建立

在该方法中，背景建立（活动A）旨在为其他风险评估活动做好准备。此活动包括以下步骤：

•操作说明

•考虑中的系统描述

3.2.1.1操作说明

该步骤旨在从操作员的角度尽可能详细地描述部署系统需要实现的目标和过程。为此，我们利用JARUS-SORA[184]的指南收集和呈现如下操作信息：

•包含所有信息的详细说明，以了解无人机部署的方式、地点以及限制或条件。

•飞行期间操作类型（如可视视线或超出可视视线）、操作员参与和系统自动化水平的详细说明。

•关于系统部署和维护过程以及这些过程中涉及的人员的详细说明

•应急程序的详细说明（例如，电池耗尽、连接中断时）。

•考虑中系统的若干网络安全假设，该环境允许减少分析范围并忽略几种攻击，例如，“所有员工都是可信的，因此内部员工故意发起的所有攻击都被忽略”。

注1：从该描述中，我们可以提取更多信息，如系统需要执行的功能（例如，遵循特定轨迹，将视频发送回地面控制站-地面军事系统），用于分析影响严重性的参考因素（例如，无人驾驶飞机飞越人群时的死亡人数，无人驾驶飞机运输货物时的经济损失）。

注2：需要仔细确定网络安全假设；如果不确定，则可以忽略潜在的攻击。

3.2.1.2考虑中的系统描述

本步骤的目的是获取有关受保护系统的必要知识。本步骤重点收集几种信息：体系结构、网络安全环境、接口、功能。

•体系结构：系统可分解为子系统。它们包括基本子系统（自动驾驶仪、ESC等）和附加子系统（摄像机、有效载荷等）。应确定这些元件及其相互连接。

•环境：所有人、可与所考虑系统交互的外部系统。例如，UAS环境可能由维护人员、制造商、互联网、运营商等组成。对于环境的每个要素，需要详细说明其访问能力和角色。

•接口：环境元素可以与系统交互的所有入口点。例如，在无人机的情况下，地面控制站通过射频通信向无人机发送命令数据。因此，射频通信是无人机的接口。

•功能：实现系统目标所需的所有离散动作（用动作动词描述）。有关系统功能的信息可以从体系结构描述中提供的系统操作信息中推断出来。例如，系统功能可以遵循预先确定的轨迹，录制视频并将其传输回地面站。在功能描述中，还应详细说明此功能的要求。例如，对于“将视频发送回地面站”功能，应详细说明视频的预期质量、视频数据保密性等。

每个组件或子系统也有自己的体系结构、功能、接口和环境。因此，所有提到的信息都应该在许多抽象层次上收集。例如，除了UAS的架构、接口、功能、网络安全环境外，我们还需要了解自动驾驶仪、射频模块、摄像头等。

注：根据开发过程（设计、测试、文档）和系统状态（正在开发或准备使用），此信息可能存在（文档化）或不存在。如果它们不存在，则应以确保信息完整性的方式从现有信息中推断它们

3.2.2风险识别

在风险识别步骤中，我们的目标是实现三个目标。第一个目标是尽可能全面地识别风险。第二个目标是揭示风险的性质及其演变（包括攻击者的基本行为、不同抽象级别的组件故障以及系统级别的故障）。最后一个是为了方便安全需求的选择。为此，此方法为此步骤采用了新版本的攻击树。构建攻击树的过程如图3.3所示。

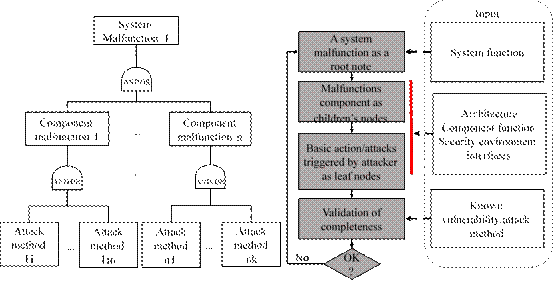


图3.3：攻击树构建工作流程

首先，每个攻击树从最高抽象级别的系统故障开始，作为表示攻击目标的根节点（例如，“无人机坠毁”或“视频被披露”）。这些故障可以直接从上下文建立中确定的系统所需功能推断出来。每个故障都被视为三个安全属性（机密性、完整性、可用性）中的一个的丢失，见表3.1。

*例如，如果无人驾驶飞机自动飞行跟随预定轨迹，我们可以考虑“飞行并遵循预定轨迹”作为系统功能。我们可以确定无人机的两个相关故障：（1）“坠毁”（失去可用性）和（2）“偏离预定轨迹-遵循攻击者定义的轨迹”（失去完整性）。*

接下来，推断出导致根本故障的部件中的故障，并将其表示为攻击树的子节点（例如，自动驾驶仪向电机提供错误的指令）。为了推断部件的故障，我们使用部件功能列表

表3.1：安全属性丢失导致的故障

|  |  |
| --- | --- |
| 安全属性 | 故障描述 |
| 可利用性 | 出现拒绝访问功能的故障 |
| 诚实正直 | 表示功能误用或校正不正确的故障 |
| 保密性 | 显示信息/数据披露的故障 |

和体系结构作为输入。

*例如，我们认为“无人机崩溃”作为根节点。该系统故障与前一示例中提到的“按照预定轨迹飞行”系统功能有关。该功能是基于不同组件的协作实现的。他们是：*

• *自动驾驶仪，估计飞行状态并提供发动机指令*

• *GPS，提供位置数据*

• *惯性测量单元（IMU），提供姿态数据。*

*我们使用三个网络安全属性关键字（机密性、完整性、可用性）确定每个组件及以上组件可能出现的故障。它们可能是“GPS提供错误的位置数据”、“GPS无法提供位置数据”、“自动驾驶仪无法控制飞机”等。我们将这些故障作为子节点添加到攻击树中。*

然后，我们重复此过程，以确定组件的原因（视为子系统），直到达到最低级别的元素（无法获得进一步分析的信息）。最后，攻击树以叶节点结束，叶节点表示攻击者可能发起的恶意操作或攻击方法，以触发攻击。我们可以从有关UAS环境的信息推断出这些恶意行为。

攻击树为我们提供了与系统功能完成后相关的风险的可视化演示。从叶节点到根节点的每条路径都表示攻击者可以执行的攻击场景。每个攻击场景都是网络安全风险，我们需要在下一步中对其进行评估。由于构建攻击树的过程是演绎的，因此结果或多或少受到执行分析的人员的能力的影响。因此，最后，需要通过检查攻击树中是否识别了所有记录的攻击方法来验证结果的完整性。

注：然而，在扣除过程中，一些故障/漏洞被认为很难发生。如果它们与更高级别的故障/恶意操作之间的链接符合逻辑，则应将它们保留在攻击树上。例如，“通过USB端口闪烁带有恶意软件的GPS”很难发生，但可能发生，因此需要在攻击树中显示。

3.2.3风险分析与评估

此步骤旨在确定需要考虑哪些攻击场景，哪些可以忽略。该步骤的基本思想与安全分析中的基本思想类似，其中风险水平由两个因素表征：影响的可能性和严重性。然而，由于缺乏反馈，很难确定攻击的可能性。我们评估攻击难度（DOA），而不是可能性。DOA表示攻击者成功实施攻击所需的全部努力。这些攻击很容易执行，但可能产生重大影响，应首先处理。难以执行的攻击可能影响较小，可以忽略或以低优先级处理。表3.2显示了用于确定每个攻击场景的风险水平的机制（L、M、H表示代表性的低、中、高风险水平）。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| DOA | 没有一个 | L | M | M | H | H |
| 基本的 | L | L | M | M | H |
| 适度的 | L | L | L | M | M |
| 高的 | L | L | L | L | M |
| 很高 | L | L | L | L | L |
|  | 无影响 | 低的 | 中等的 | 高的 | 很高 |
|  |  | 攻击的严重性 | | |  |  |

表3.2：风险水平

在这种方法中，一次攻击的难度和严重程度由多人定性评估。攻击的严重性可以从上下文建立活动中收集的操作信息推断出来。攻击的难度可根据必要设备的性质（例如，便宜或昂贵、知名或不知名）、实施攻击所需的攻击技术和系统知识进行评估。

我们采用ED202A/DO326标准中提出的指南-载人飞机的网络安全难度。在本标准中，每个场景的难度根据三个标准确定：“准备手段”、“执行手段”和“机会之窗”。“准备手段”表示准备攻击的资源、时间和知识方面的困难（例如，发现漏洞和发现目标特征）。“执行平均数”表示执行攻击所需的资源、时间和知识（例如，破坏加密算法的时间）。“机会之窗”表示与攻击时刻相关的难度（例如，如果可能，仅在系统重新启动期间很难发起攻击）。使用ED202A/DO326标准中提供的量表对这些标准进行评估（见表3.3、表3.4和表3.5）。分配给这些标准的点的总和就是场景的总难度点。

然后将该点与5个难度级别（无、基本、中等、高和非常高）中的一个匹配，如表3.6所示。

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | 知识 |  |
| 设备 | 无/公开信息，无准备时间 | 非受控信息和无意义准备时间 | 内部知识或大量准备时间 |
| 无/标准[1] | 0 | 2 | 6 |
| 特殊胶辊[2] | 0 | 2 | 6 |
| 特别报告[3] | 不适用 | 4 | 6 |
| 定制[4] | 不适用 | 5 | 6 |

表3.3：准备方法

|  |  |
| --- | --- |
| 要点 | 描述 |
| 0 | 攻击可以在任何时候进行 |
| 1 | 攻击可以在常规巡航飞行期间进行。 |
| 2 | 当飞机在地面上时，攻击向量是可用的。 |
| 3 | 限制机会窗口的强制性操作程序的最大有效性。 |
| 6 | 攻击向量只能在受限的时间段中使用，例如在维护模式下在地面上可用。 |
| 8 | 攻击只能在独立于飞行阶段的非常有限的时间段内执行（例如，在系统重新启动期间）。 |

表3.4：机会之窗

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | 专业知识 | |  |  |
| 设备 |  | 外行 | 精通的 | 专家 | 多专家 |
| 无/标准 | 0 | 4 | 6 | 10 |
| 特殊胶辊 | 4 | 4 | 6 | 10 |
| 特殊的 | 不适用 | 6 | 8 | 12 |
| 定制 | 不适用 | 不适用 | 10 | 12 |

表3.5：执行方式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 从0到6 | 从7点到12点 | 从13岁到18岁 | 从19岁到24岁 | 超过24 |
| 没有一个 | 基本的 | 适度的 | 高的 | 很高 |

表3.6：攻击难度量表

3.2.4治疗

对于上一步选择处理的每个威胁场景，应制定一套网络安全要求。网络安全要求不是一项具体的安全措施，但它只是一项需要实现的安全目标，以确保系统的网络安全。对于每个网络安全要求，可以考虑一个或多个安全措施。在选择布线系统要求之前，需要对其进行测试/模拟和评估（成本、有效性）。

在该方法中，我们采用ED202A/DO326A[185]中提到的安全要求分类如下：

•预防：目的是阻止恶意用户造成故障

•威慑：目的是防止发生故障

•检测：目的是检测并报告攻击者的故障或恶意行为。

•纠正：目的是在故障发生时作出反应

•恢复性：目的是在发生故障后将系统恢复到正常状态

3.3案例研究

在本节中，我们将介绍我们的方法在案例研究中的应用：“基于无人机的公路观测”——SOGILIS公司的一个实际应用。在本案例研究中，UAS用于在自动飞行模式下观察高速公路。无人机捕获的视频和飞行信息被发送到地面，并在地面控制站（GCS）计算机的屏幕上显示给操作员。在操作过程中，无人机将沿公路飞行并遵循预定轨迹。从飞行开始到结束，无人机在操作员的超视距（BVLOS）观察下始终以自动模式飞行。操作员可以使用三个简单的命令：启动航班、结束航班（返回待机模式）和回家。该UAS的架构如图3.4所示。为了简化案例研究，我们假设该UAS是在没有任何网络安全注意的情况下开发的。这意味着在应用我们的方法之前，没有保护UAS的措施。

从系统操作的描述中，我们定义了三个需要保护的系统功能：

•功能1：按照预先确定的轨迹自动驾驶飞行器：无人机必须遵循制造商预先确定并嵌入自动驾驶仪的飞行计划。飞行计划包含多个航路点。每个航路点都包含有关坐标、海平面高度或地面高度的信息。

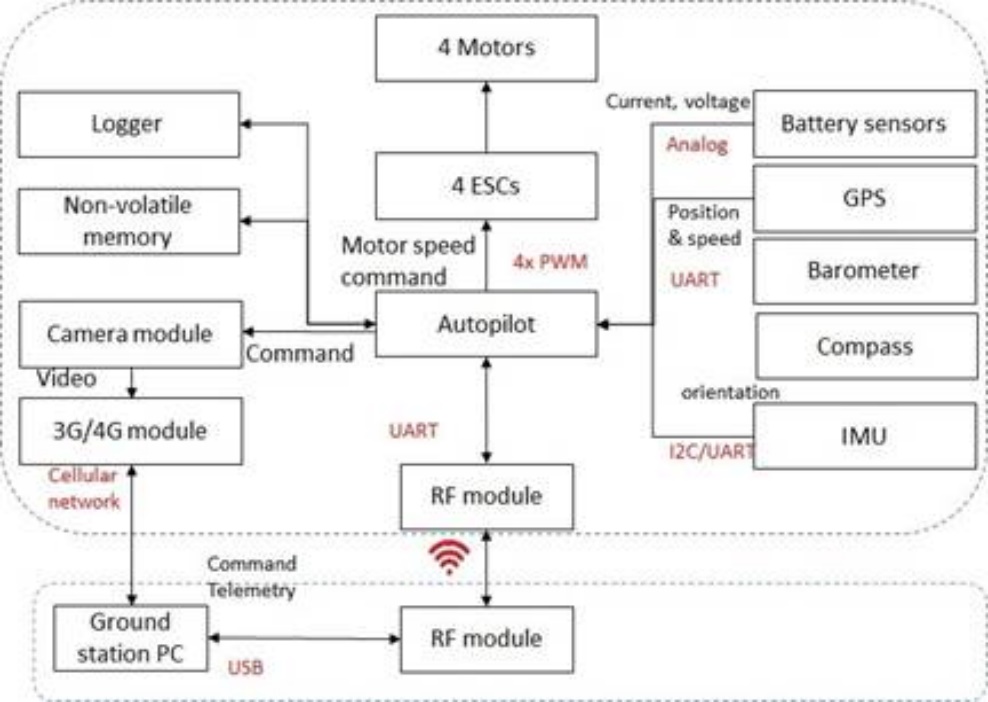


图3.4：无人机的体系结构。

•功能2：向操作员提供飞行信息：所有状态信息，如姿态、位置、预定轨迹、电池信息将发送至地面，并显示在地面军事系统计算机屏幕上。只有负责的操作员才有权访问此信息。

•功能3：向操作员提供观察视频：摄像机捕获的视频被发送到地面并显示在地面军事系统计算机上。只有负责的操作员才有权访问此信息。

基于上述系统功能，我们定义了攻击者想要触发的故障。每个故障都与系统功能的一个网络安全属性（完整性、可用性、机密性）的丢失有关。故障列表如下所示：

•故障1-可用性-无人机坠毁：由于恶意行为，无人机失去姿态并坠毁。由于飞越高速公路，无人机坠毁可能导致致命事故。因此，我们将该故障的严重性定为非常高的级别。

•故障1-完整性-偏离预定轨迹：在攻击下，UAV偏离其轨迹并按照攻击者定义的轨迹飞行。通过操纵无人机的轨迹，攻击者可以劫持车辆。在最坏的情况下，攻击者可能会造成故意的致命事故。因此，我们将该故障的严重程度定为非常高的级别。

•故障1-保密性-无相关信息。

•故障2-可用性-飞行信息不可用：在攻击下，飞行信息不再可用，操作员无法识别情况。此故障可能帮助攻击者发起其他攻击或取消操作。我们为该故障指定了中等严重程度。

•故障2-完整性-假飞行信息：假飞行信息：在受到攻击时，假飞行信息被提供给操作员，这使他们做出错误的决定，例如触发故障安全功能。我们为该故障指定了中等严重程度

•故障2-机密性-泄露航班信息：在攻击下，攻击者可能获得对航班信息的未经授权访问，这可能有助于攻击者发起其他攻击。我们为该故障指定了中等严重程度

•故障3-可用性-视频不可用：在攻击下，操作员无法访问观察视频。我们为该故障指定了较低的严重程度。

•故障3-完整性-假视频：在受到攻击时，操作员收到攻击者制作的假观察视频。该故障不会直接影响操作的安全性。我们为该故障指定了较低的严重程度

•故障3-机密性-视频泄露：在攻击下，攻击者可能获得对观察视频的未经授权访问，从而影响被观察者的隐私。我们指定了高级别的严重性

对于每个系统故障，我们建立一个攻击树。对于这项任务，我们使用ADTool[186]——一种开源软件来绘制具有相关需求的攻击树。例如，图3.5显示了与故障2-完整性相关的攻击树。在本章的下一部分中，我们将重点分析故障2-完整性“假飞行信息”。其他故障分析（包括攻击树、风险评估、要求）见附录C。通过图3.5所示的攻击树，我们可以确定以下五种可能的攻击场景：

•场景2-integrity-1：在此场景中，对手通过射频通信信道攻击UAS。如果射频通信信道没有得到足够的保护，敌方可能会在地面创建并向射频模块发送虚假信息，并用故障信息欺骗地面军事系统和飞行员。因此，RF模块应验证每个接收包在时间、有效载荷和来源方面的完整性（要求14-见附录C.2），以抵御该攻击。

•场景2-integrity-2：该场景与第一个场景类似，其中RF模块接收假消息。不同之处在于，对手不会创建虚假消息，而只是复制传输的消息，然后重新发送。这次攻击的结果是飞行员被时间方面的故障信息欺骗。在里面

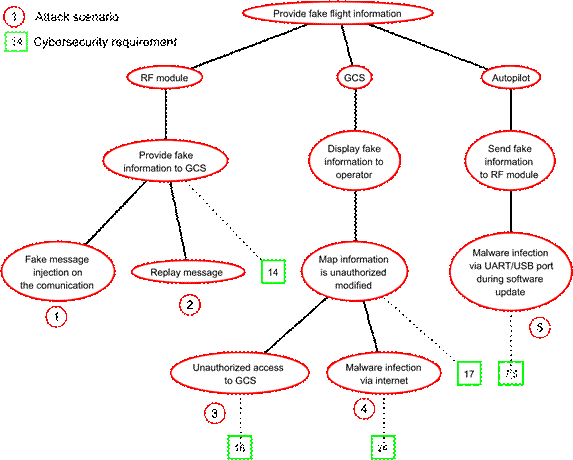


图3.5：与故障2-完整性相关的完整攻击树

在这种情况下，对手不必知道消息的结构或使用的加密方案（如果可用）。为了防御这种攻击，RF模块应根据过渡时间/顺序验证每个接收包的完整性（要求14-见附录C.2）。

•场景2-integrity-3：在此场景中，对手通过地面军事系统攻击无人机。如果敌方能够到达地面控制站（GCS），他们可以修改地面控制站存储的地图。有了故障地图，驾驶员将被车辆位置上的故障信息欺骗。对于成功的攻击，攻击者不必具备高技术知识水平，但她/他必须有机会访问地面军事系统（例如，不满的工作人员）。这种攻击的合适对策可能是访问控制机制，允许授权人员访问地面军事系统（要求16-见附录C.2）。

•场景2-integrity-4：在此场景中，地面军事系统计算机通过互联网感染恶意软件，该软件可能会修改存储的地图信息，而不会被检测到。到

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 脚本 | DOA | | | | 严重程度 | 风险水平 |
| 准备手段 | 机会之窗 | 执行手段 | 全部的 |
| 2-完整性-1 | 2 | 1 | 6 | 9（基本） | 中等的 | 中等的 |
| 2-完整性-2 | 2 | 1 | 6 | 9（基本） | 中等的 | 中等的 |
| 2-完整性-3 | 6 | 6 | 10 | 22  （高） | 中等的 | 低的 |
| 2-4 | 6 | 6 | 10 | 22  （高） | 中等的 | 低的 |
| 2-5 | 6 | 6 | 10 | 22  （高） | 中等的 | 低的 |

表3.7：与故障2-完整性相关的攻击场景的风险评估

如果成功进行此攻击，攻击者必须具备恶意软件和目标地面军事系统的良好技术知识。为了抵御这种情况，需要控制互联网和地面军事系统之间的数据流。只有制造商定义的数据类型才能达到地面军事系统从互联网发送或由地面军事系统发送至互联网（要求24-见附录

C.2）。

•场景2-integrity-5：在此场景中，自动驾驶仪应在软件更新期间感染恶意软件。由于安装了恶意软件，自动驾驶仪在飞行期间（通过RF模块）向地面军事系统发送虚假信息。这种情况要求攻击者对恶意软件和目标自动驾驶仪有很好的了解。对于此类攻击，自动驾驶仪应能够验证固件的完整性，以确保其由制造商创建（要求7-见附录C.2）。此外，可以设置访问控制机制，仅允许制造商修改/更新固件（要求8-见附录C.2）。

如表3.7所示，对上述攻击场景的风险级别进行了评估。

3.3.1结果分析

基于攻击树，我们确定了49种可能的攻击场景，包括9种高风险场景、28种中风险场景和12种低风险场景。这些场景涉及UAS的不同组件。图3.6所示的图表显示了攻击场景到各种目标组件的分布情况。根据该图，攻击场景中最受攻击的组件是自动驾驶仪（11种场景）、地面控制站或地面军事系统（10种场景）、射频链路（7种场景）和3G/4G链路（7种场景）。这一论点是合乎逻辑的，因为自动驾驶仪、地面军事系统和通信链路涉及UAS的所有功能。在这一点上，我们可能想知道场景是否与这些相关

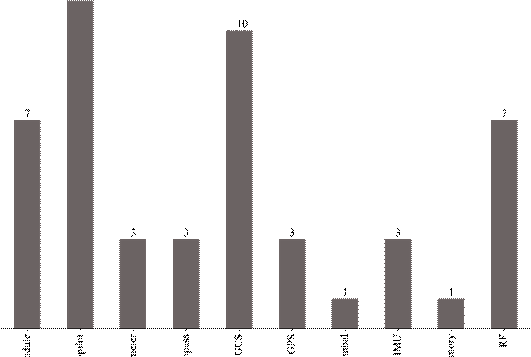
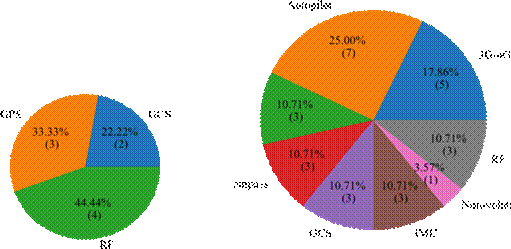


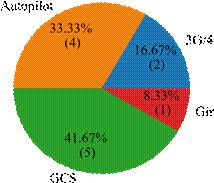
图3.6：不同目标组件的攻击场景分布

在风险处理步骤中，最应该考虑的是组件。答案是“不确定”。特别是根据我们的方法和总体风险管理的一般精神，在治疗步骤中，治疗步骤中场景的优先级取决于其风险水平。图3.7所示的图表显示了高风险场景在不同组件中的分布情况。

如图3.7所示，高风险场景仅涉及三个组件：地面军事系统、GPS模块和RF模块。射频模块和GPS模块都基于某种无线通信。通过将目标对准RF模块和GPS模块，攻击者可以远程发起攻击。同时，地面军事系统提供了一台完整的人机，可以轻松控制车辆。这意味着在到达地面军事系统时，对手可能会在没有太多技术知识的情况下干扰飞行器的飞行。此外，所有这些部件都涉及UAS的基本功能：保持车辆安全地沿着预定轨道飞行。对于另一个关键组件——自动驾驶仪，我们仅将相关风险场景分配到中等风险级别或低风险级别。攻击者没有太多机会实际到达自动驾驶仪。此外，它需要复杂的工具和有关自动驾驶仪软件/硬件的知识，才能发动成功的攻击。



（a） 高风险情景 （b）中等风险情景



（c） 低风险情景

图3.7：不同目标组件和风险级别的风险场景分布

此外在自动驾驶仪中，我们还将涉及传感器（气压计、指南针、IMU）和有效载荷组件（万向节、3G/4G模块）的风险场景分配到低或中等级别。我们认为基于传感器的攻击场景几乎是不可能的，因为这些攻击的有效范围受到限制，如第1.5节所述。同时，万向节和3G/4G模块仅涉及非关键功能（采集和传输视频数据）。基于上述分析，我们应首先处理与地面军事系统、GPS和RF模块相关的风险（如GPS欺骗、数据泄露、反认证）。然而，该结论仅适用于该预期操作和架构，该架构是在“无网络安全注意”假设下开发的。

3.4结论

本章介绍了我们解决现有（或设计）UAS网络安全问题的风险管理方法。我们的方法包括四个步骤：（1）背景建立，（2）风险识别，（3）风险分析和评估，（4）风险处理。在第一步-上下文建立中，我们收集有关系统架构和操作的信息，这些信息应该尽可能详细。在第二步-风险识别中，我们识别可能的网络安全攻击场景。攻击场景是根据第一步收集的系统信息（功能、组件、环境）推断出来的。在这一步中，我们使用攻击树图来支持推理过程并可视化场景。在第三步-风险分析和评估中，我们根据每个已识别攻击场景的影响严重程度和难度级别评估其风险级别。为了估计难度水平，我们采用DO326标准中定义的量表。在最后一步-风险处理中，我们确定了防御攻击场景的安全需求。这些要求是根据相关攻击的风险等级顺序制定/实施的。为了说明这种方法，我们提供了一个简单的案例研究，其中使用无人机对公路进行观测。在风险识别步骤中，我们总共识别了49种不同的风险场景。这些场景涵盖了文献中提到的所有可能的攻击方法（真实攻击、测试或模拟）。在风险分析和评估中，我们将7个场景分配给高风险级别，28个场景分配给中等风险级别，12个场景分配给低风险级别。这一步在很大程度上取决于直观判断，尽管这一步是基于航空标准DO326A中定义的分类尺度执行的。通过结合不同专家的判断，可以提高该步骤的稳健性。在最后一步中，我们确定了需要考虑的24项网络安全要求。这些都是技术要求。其中一些需要对系统架构进行重大更改。架构更改可能会影响开发过程在时间、财务和工作量方面的成本效益。因此，我们认为，在设计架构之前，应该考虑网络安全。这一论点是我们在第4章中工作的基础

第四章

运营风险评估：从安全到网络安全



目录

|  |  |
| --- | --- |
| 4.1导言。 | 62 |
| 4.2 SORA方法的解释。 | 62 |
| 4.2.1风险模型。 | 62 |
| 4.2.2评估过程。 | 64 |
| 4.3将SORA方法扩展到网络安全的解决方案。 | 67 |
| 4.4损害扩展：SORA与隐私损害。 | 69 |
| 4.4.1侵犯隐私的可能性。 | 70 |
| 4.4.2隐私风险等级确定步骤。 | 72 |
| 4.4.3新帆的确定。 | 73 |
| 4.5威胁扩展：SORA面临新的网络安全威胁。 | 74 |
| 4.5.1网络安全分类和风险模型扩展。 | 74 |
| 4.5.2 OCSL的确定。 | 76 |
| 4.5.3 OCSO稳健性测定。 | 79 |
| 4.6用于风险评估的扩展SORA网络工具。 | 79 |
| 4.6.1说明和目的。 | 79 |
| 4.6.2设计和实施。 | 80 |
| 4.7结论。 | 81 |

61

4.1导言

在上一节中，我们介绍了一种加强现有UAS网络安全的方法。由于系统修改的成本，这种方法对于网络安全问题可能不具有成本效益。因此，我们的目标是开发一种方法，以尽早考虑网络安全方面，在系统设计的开始。为此，我们将现有的安全方法-特定操作风险评估（SORA）扩展到网络安全。SORA是UAS行业中一种著名的评估方法。该方法侧重于评估与操作安全相关的风险，但未考虑网络安全。本章的剩余部分组织如下。SORA方法的概念见第4.2节。第4.3节给出了扩展该方法的方法。第4.4节和第4.5节给出了SORA方法的两个扩展。第4.6节介绍了我们开发的基于网络的风险评估工具，可远程访问。我们在第4.7节中总结了我们的工作。

4.2 SORA方法的解释

具体操作风险评估（SORA）是一种以操作为中心的整体方法[187]，由国家航空管理局-无人系统规则制定联合管理局（JARUS）[188]，[189]的专家组提出。该方法用于分析UAS运行的安全性，并确定需要实现的安全目标。这些目标涉及操作的许多方面，如培训、系统性能、操作员组织、系统开发。这种方法对不同类型的利益相关者可能有用。运营商（操作无人机的运营商）和航空当局可以使用该方法作为遵守欧盟法规的手段。制造商（设计和开发UAS）可以使用SORA方法来确定其设计需要达到的特定类别下目标操作的安全特性。本节解释了该方法的一般概念，包括两部分：风险模型、评估过程。

4.2.1风险模型

SORA方法使用蝴蝶结模型来说明考虑中的风险情景。该模型在方法SORA[103]的第一版中有详细介绍，但在第二版[104]中没有明确提及。然而，该方法仍以该模型为基础。因此，有必要了解模型以了解方法论的基本原理。该模型的主要要素包括（1）危害、（2）威胁、（3）危害和（4）障碍。

1.    危险是领结图的中心点。指在操作员意图之外进行操作的情况（例如飞机飞到外部

4.2.SORA方法的解释

在目视视线操作中对飞行员进行目视观察）。

2.    威胁位于危险的左侧，分为不同的类别。它们是造成危险的可能原因。由于SORA方法仅考虑安全方面，领结图仅说明了一些意外威胁类别，如图4.1所示。

3.    危害位于危害的右侧，代表危害的可能后果或场景的最终结果。目前，SORA方法只考虑了与人的生命相关的两种伤害：“地面第三方致命伤害”、“空中第三方致命伤害”（见图4.1）。为了缓解风险情景，可以采用几种屏障（或缓解手段）。

4.    有两种壁垒：威胁壁垒和伤害壁垒。危害屏障防止危害发生后发生危害。威胁屏障可防止危险发生。对于每种类型的威胁，将在风险评估结束时以运行安全目标（OSO）的形式确定不同的威胁屏障。每个OSO在三个健壮性级别（低、中、高）进行了详细说明。OSO#4就是一个例子——“UAS是按照权威机构认可的设计标准开发的”。在本OSO的低稳健性水平下，申请人应仅声明达到了要求的标准。同时，在高稳健性水平上，申请人必须提供支持证据（如分析、模拟），这些证据将由有能力的第三方进行验证。本方法提供的OSO清单见本文件附件E。

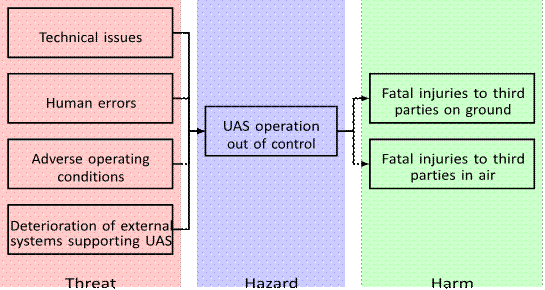


图4.1：以蝴蝶结图表示的SORA方法的风险模型

在下一部分中，我们将从定量和定性两方面解释基于上述风险模型的SORA方法的评估过程。

4.2.2评估过程

4.2.2.1定量方法

传统上，风险被定义为可能性和严重性的组合。然而，SORA方法中的风险仅与可能性参数相关[103]，因为该方法基本上只关注对人的生命造成伤害的风险。这些危害的严重程度可以认为是极其严重的。换句话说，将确定安全目标，以将每次伤害的可能性保持在可接受值（10）以下−每飞行小时造成6人死亡，相当于载人飞机操作[103]）。如图4.2所示，这些危害的可能性分解为单独的成分。

|  |
| --- |
| 对地面第三方造成致命伤害的可能性 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 拥有无人机的可能性  操作失控  (1) | x | 如果操作失控，被UA击中的可能性  (2) | x | 被击中人员死亡的可能性  (3) |

=

|  |
| --- |
| 如果被击中，另一个  飞机不能  继续安全飞行  (3) |

|  |  |  |
| --- | --- | --- |
| 拥有无人机的可能性  操作失控  (1) | x | 其他飞机被撞击的可能性  UA，如果操作失控  (2) |

|  |
| --- |
| 空中对第三方造成致命伤害的可能性 |

=x

图4.2：根据SORA，地面和空中发生致命伤害的可能性[103]

每个等式的组成部分（1）“无人机运行失控的可能性”主要受威胁和威胁屏障的影响[103]。每个等式中的组件（2）和组件（3）的组合表示在无人机运行失控的情况下发生危害的可能性，可通过分析考虑中的运行性质（例如位置、高度、运行类型、设置的危害屏障）来评估。根据上述假设，定量方法中该方法的一般概念可解释如下：

•目标：考虑到UAS操作，我们需要将每次伤害的可能性保持在可接受的值以下：10−每飞行小时造成6人死亡。

•首先，我们收集无人机的预期操作信息，如操作区域、操作模式、飞行员、无人机重量。该活动称为作战概念（CONOPS）描述。SORA方法附录a中提供了CONCOPS说明的形式。

•其次，我们根据收集到的信息（如10）估计“UAS运行失控”情况下发生危害的可能性−每种危险在地面上造成4人死亡，10人受伤−每种危险在空气中造成3人死亡）。

•第三，根据上述估计值，我们计算出UAS运行失控可能性的可接受值（10−从第一个方程式开始，每飞行小时2次危险，10次−从第二次飞行开始，每飞行小时3次危险）。更关键的

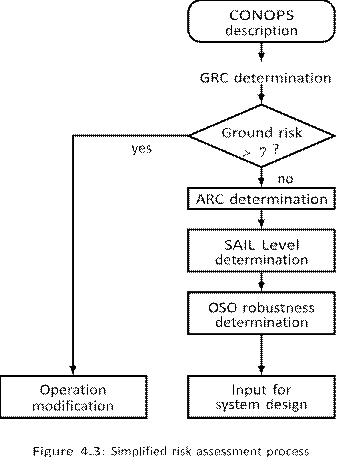
4.2. SORA方法的解释

将选择值作为需要达到的目标（例如10−每飞行小时3次危险）。

•最后，基于“无人机运行失控的可能性”的目标值，将定义具有相应鲁棒性的安全目标。

4.2.2.2定性方法

由于缺乏实际数据，上述定性方法通常不现实。因此，SORA方法基于图4.3所示的定量方法的主要思想，提出了一种定性方法。定性方法可解释如下：



•目标：考虑到UAS操作，我们需要将每次伤害的可能性保持在可接受的水平。

•首先，我们收集有关预期操作的信息（CONOPS说明）

•其次，我们确定两个定性因素：地面风险等级（GRC）和空气风险等级（ARC）。这些因素定性地代表了在UAS运行失控的情况下发生危害的可能性。GRC和ARC是根据操作的固有特性确定的，例如操作区域、姿态、飞机重量和伤害屏障的可用性。

•第三，我们确定了两个具体的保证和完整性水平（SAIL）值，它们表示UAS运营将保持在控制之下的信心水平。一个SAIL值对应于GRC，另一个对应于ARC[103]。SAIL值的范围从I到VI。然后，将选择较高的SAIL值作为与UAS操作相对应的置信水平或SAIL。该值被视为推动所需安全目标的目标。在SORA方法的最新版本中，通过使用表4.1简化了这些活动。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 航海决心 | | | |  |
|  | 弧 | | |  |
| GRC | a（\*\*） | B | C | D |
| ≤ 2 (\*) | 我 | 二, | 四, | v |
| 3 | 二, | 二, | 四, | v |
| 4 | 三, | 三, | 四, | v |
| 5 | 四, | 四, | 四, | v |
| 6 | v | v | v | v |
| 7 | 不及物动词 | 不及物动词 | 不及物动词 | 不及物动词 |

表4.1:SORA方法的确定[104]

*表4.1的说明：第一条值线（\*）包含对应于弧值的SAIL值。它们也可以理解为GRC可忽略不计的操作的SAIL值。第一个值列（\*\*）显示与GRC对应的SAIL值。它们也可以理解为ARC可忽略不计的操作的风帆值。其他SAIL值是GRC对应的SAIL值和ARC对应的SAIL值中的最大值。*

•最后，我们选择了操作安全目标（OSO）及其与操作航行水平相对应的鲁棒性水平。SORA[98]附件E中提供了所有可能的OSO列表。

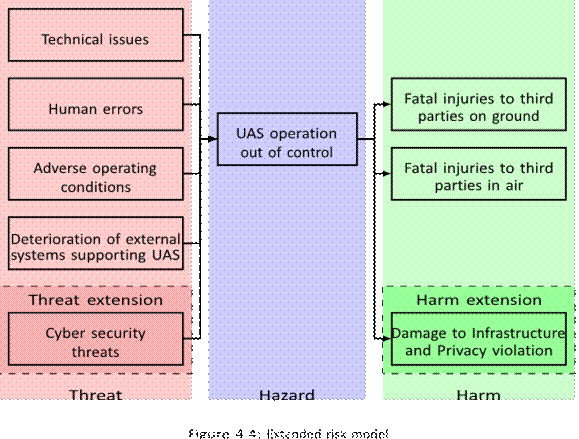
在本节中，我们解释了SORA方法的原始概念。可恢复为（1）首先，根据“UAS操作失控”情况下的危害可能性评估UAS操作的临界水平，（2）然后确定与操作临界水平对应的威胁屏障。在下一节中，我们将提出一个解决方案，将此方法扩展到基于此概念的网络安全方面。

4.3. 将SORA方法扩展到网络安全的解决方案



4.3将SORA方法扩展到网络安全的解决方案

我们提出的解决方案包括两部分，即伤害扩展和威胁扩展。危害扩展利用新危害扩展考虑中的风险情景；并完成对给定UAS操作的关键级别的评估。威胁扩展使用新的网络安全威胁扩展考虑中的场景；并确定给定UAS操作的相应威胁屏障。



在危害扩展中，我们关注风险模型的危害方面（见图4.4）。最初的SORA方法只涉及对人的生命的伤害。然而，除了对人的生命造成伤害外，公众还关注其他伤害[103]、[189]–[191]，例如：

•侵犯隐私：UAS可能具有小尺寸、长操作范围和高性能机载传感器；因此，它可以侵入私人场所并收集信息[192]。这侵犯了主人的隐私。侵犯隐私可能由网络攻击或系统错误引起。例如，警察操作的无人机在前往作战区的途中可能会经常穿越私人财产。在下面

如果发生网络攻击，则可能会泄露财产上录制的视频，进而侵犯业主的隐私权。

•对基础设施的物理破坏：假设UA可能因网络攻击或事故而坠落在公路、电力线、核电厂等关键基础设施上。这种危害仅与无人机在关键基础设施附近或上方飞行的某些特定操作有关。

•基础设施的数字破坏：据推测，无人机可能成为关键基础设施的安全漏洞。例如，攻击者接管了UAS的控制权，并通过UAS和基础设施之间的连接使用它来攻击基础设施。

因此，这些新的危害成为扩展方法中应该考虑的重要问题。在Harm Extension中，我们应对新危害的策略包括以下四个步骤：

1.    选择了需要解决的新危害

2.    确定影响所选伤害可能性的UAS操作因素/特征。

3.    建立公式或表格，根据确定的因素定性评估可能性

4.    扩展“确定航行”步骤，以涵盖新危害的可能性。

在威胁扩展中，我们将关注风险模型的威胁方面。需要确定潜在的网络安全威胁，并将其分为新的威胁类别。换句话说，这就需要对与无人机操作相关的网络安全威胁进行分类。为了说明新的场景，新的威胁类别将添加到风险模型的威胁端，如图4.4所示。根据每个新的威胁类别，还将建立一份可能的威胁屏障列表。给定UAS操作的详细威胁屏障将根据SAIL因子的值从建议列表中选择。我们开发该扩展的策略可以描述如下：

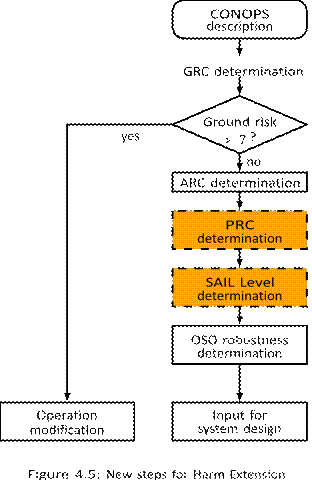
1.    根据文献回顾，创建网络安全威胁的分类。网络安全威胁将被添加到SORA风险模型的威胁端。

2.    为定义的分类法中的每个威胁类别建立通用威胁屏障列表。根据SORA方法，每个屏障将定义为三个鲁棒性级别（低、中、高）。这项工作也是基于“封闭”领域的网络安全对策的最新进展，如智能车辆、机器人技术。。。

3.    确定为给定UAS操作选择网络安全威胁屏障稳健性的机制。

伤害扩展和威胁扩展可以单独开发，然后可以集成到一个完整的方法中。第4.4节详细介绍了与隐私相关的危害扩展，第4.5节介绍了威胁扩展。

4.4危害扩展：SORA与隐私危害



如今，隐私侵犯是公众接受UAS应用程序时最关心的问题之一[103]、[191]、[193]。因此，我们认为这是一个重要的问题，并在我们的作品中首先提出。然而，一般隐私是一个非常大的术语。很难准确地定义[194]这一术语，也很难笼统地处理这一术语，因此我们只关注这一危害的三个方面：（1）个人信息的披露；（2） 非法人身监视；（3）侵入私人场所。第一个方面在Li等人[195]的著作中进行了说明。作者试验了一种基于无人机捕获视频的密码窃取攻击。第二个方面在[196]-[198]中提到。在这些论文中，作者研究了监视UAS应用程序如何影响地面人员的隐私。此外，Park et al.[197]和Babiceanu et al.[199]提出了基于捕获图像/视频质量判断UAS操作隐私侵权的标准。最后一个方面由Blank等人[200]提出。作者提出了一种机制，在创建飞行路径时识别私人空间，并确保UAs不会飞越这些私人空间。

接下来，我们首先分析侵犯隐私的可能性，以确定与此伤害相关的可能因素，这些因素可用于评估（见4.4.1）。然后，我们建议对评估过程进行扩展：（4.4.2）一个名为“隐私风险等级（PRC）确定”的新步骤，以评估“UAS运行失控”情况下的这种损害的可能性；（4.4.3）扩展“航行确定”步骤（见图4.5）。

4.4.1侵犯隐私的可能性

考虑到隐私损害，风险评估的目标被扩展，以保持隐私损害的可能性也在一定的可接受水平之下。与对人的生命造成伤害的可能性类似，隐私伤害之一可以分解为图4.6所示。该等式的两个组成部分（2）和（3）的组合表示“UAS运行失控”后第三方隐私受到侵犯的可能性。

对于给定的操作，人员暴露于UA（传感范围内或UA下方）的可能性取决于操作区域的性质（城市区域与农村区域）和操作类型（视线外与视线下）。在城市地区，人口密度和私人场所的数量高于农村地区。因此，城市地区的个人或私人场所暴露于UA的可能性可能高于农村地区。在超视距（BVLOS）操作中，无人驾驶飞机的操作范围大于视距（VLOS）操作。因此，BVLOS操作中UA下方或附近的人数可能高于VLOS操作中的人数。这就是为什么在BVLOS操作中，个人或私人场所暴露于UA的可能性高于VLOS操作的可能性。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 侵犯隐私的可能性 | = | 拥有无人机的可能性  操作失控  (1) | x | 在以下情况下，受UA影响的人员的可能性：  操作失控  (2) | x | 可能，如果暴露，隐私  人身侵犯  (3) |

图4.6：侵犯隐私的可能性

对于暴露在UA中的人员，侵犯隐私的可能性取决于车载摄像机拍摄的图像的详细程度。例如，如果UAS拍摄的照片分辨率太低，则此人的图像不够详细，无法识别其面部，因此侵犯隐私的可能性很小。图像的细节水平可以通过像素密度来评估，像素密度是指拍摄图像中代表地面上一米的像素数。为了简化计算，我们假设地面是平的。因此，对于UAS操作，当相机方向垂直于地面时，像素密度达到最高值，如图4.7所示。在这种情况下，像素密度是UA（h）的离地高度、相机的分辨率和相机的最小视角（）的函数，如下所示：*α*

水平像素数

*PD*=

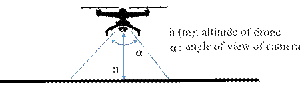


图4.7：最大像素密度位置

由于UAS应用程序和闭路电视（CCTV）应用程序[191]、[197]、[198]之间存在隐私问题的共同点，我们采用了英国安全工业协会（BSIA）为CCTV应用程序引入的图像细节级别分类，如表4.2所示。

|  |  |
| --- | --- |
| 质量水平 | 描述 |
| 监视器（12.5像素/米） | 如果知道人员的存在，可以查看人员移动的方向和速度。 |
| 检测（25像素/米） | 启用以确定是否有人在场 |
| 观察（62.5像素/米） | 能够描述个人的一些细节 |
| 识别（125像素/米） | 启用以确定显示的个人是否与他们以前见过的人相同 |
| 标识（250像素/米） | 能够在合理怀疑的情况下识别个人。 |
| 检查（1000像素/米） | 启用个人身份 |

表4.2：图像细节分类[201]

基于这一分析，我们定义了UAS操作的三个内在特征，以评估“UAS操作失控”情况下侵犯隐私的可能性：

•作业区密度：城市区与农村区

•操作类型：超视距飞行物与超视距飞行物

•拍摄图像的详细程度。

与原始方法中引入的危害类似，可以通过应用一些危害屏障来降低隐私危害的可能性。在此扩展中，我们解决了三种类型的损害壁垒，以减轻隐私损害：

•隐私保护过滤器：这些算法减少了视频/图像中可能侵犯个人隐私的不必要信息，如模糊、像素化、掩蔽、扭曲[198]

•对私人空间的限制：运营商避免穿越私人空间的飞行路径[200]

•向公众发布运行感知公告：应向观察到UAS运行的公众通报。

在本文的下一部分中，我们将提供PRC确定步骤和SAIL确定步骤的详细信息。

4.4.2隐私风险等级确定步骤

在此步骤中，“UAS操作失控”情况下隐私侵犯的可能性由隐私风险等级（PRC）值定性表示。我们根据运营的内在特征和应用的危害屏障确定运营的PRC。如4.4.1所述，考虑的内在特征包括作业区域（农村与城市）、作业类型（VLO与BVLO）和图像详细程度。如表4.3所示，这些特征的组合表达了操作的固有PRC。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类型  活动 | 农村地区，  VLOS | 农村地区，  BVLOS | 市区，  VLOS | 市区，  BVLOS |
| 图像细节级别 |  |  |  |  |
| 班长 | A. | B | C | C |
| 发现 | B | B | C | C |
| 看到 | B | C | D | D |
| 认出 | C | C | D | D |
| 识别 | C | D | E | E |
| 检查 | C | D | E | F |

表4.3：固有PRC测定

然后，确定的固有PRC可以通过伤害壁垒来降低：“隐私保护过滤器”、“私人空间限制”和“向公众发布运营意识公告”。

每个伤害屏障使用表4.4所示的折减系数修正固有PRC。

|  |  |  |
| --- | --- | --- |
| 伤害屏障 | PRC修正系数 | |
| 不适用 | 应用 |
| 隐私保护过滤器 | 0 | -1 |
| 对私人空间的限制 | 0 | -1 |
| 行动通告 | 0 | -1 |

表4.4：伤害屏障的PRC修正系数

例如，无人驾驶飞机配备1920 x 1080分辨率和10度视角（）的摄像机；以超视距飞行模式飞行，离地150米。在该操作中，最大像素密度为36像素/m，对应于检测级别（见表4.2）。根据表4.3，固有PRC为C级。在对隐私问题进行分析后，运营商决定使用数字滤波器升级车载摄像头，该数字滤波器会使人的图像模糊且无法识别。在这种情况下，PRC从C级降至B级（见表4.4）。*α*

4.4.3新帆的确定

在这个扩展中，UAS操作的帆是三个因素的组合：GRC、ARC和PRC。为了区分新的SAIL值与根据原始方法确定的值，我们将新的值称为3D-SAIL，将旧的SAIL值称为2D-SAIL。我们确定3D-SAIL的方式与确定2D-SAIL的方式类似。首先，我们选择三个对应于给定操作的GRC、ARC和PRC值的SAIL值。目前，我们建议使用表4.5来确定与GRC值相对应的帆。相应的SAIL值仅与PRC值成比例。然后，给定操作的3D-SAIL值是三个确定的SAIL值中的最高值。3D-SAIL确定步骤描述如下：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 中华人民共和国 | A. | B | C | D | E | F |
| 对应帆 | 我 | 二, | 三, | 四, | v | 不及物动词 |

表4.5：与PRC值对应的SAIL值

1.    对于给定的操作，确定对应于ARC和GRC的SAIL值的最高值。该值为2D-SAIL。我们可以使用原始SORA方法提供的表格（见4.1）。

2.    确定与PRC值相对应的风帆值（见表4.5）。

3.    在2D-SAIL值和PRC对应值之间选择更高的SAIL值（更关键），作为3D-SAIL或操作对应的最终SAIL（见表4.6）。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 2D-SAIL | |  |  |
| 中华人民共和国 | 我 | 二, | 三, | 四, | v | 不及物动词 |
| A. | 我 | 二, | 三, | 四, | v | 不及物动词 |
| B | 二, | 二, | 三, | 四, | v | 不及物动词 |
| C | 三, | 三, | 三, | 四, | v | 不及物动词 |
| D | 四, | 四, | 四, | 四, | v | 不及物动词 |
| E | v | v | v | v | v | 不及物动词 |
| F | 不及物动词 | 不及物动词 | 不及物动词 | 不及物动词 | 不及物动词 | 不及物动词 |

表4.6:3D-SAIL测定

上面提到的2D-SAIL和3D-SAIL是两个不同的值。2D-SAIL是GRC和ARC的组合，不考虑PRC（隐私损害）。同时3D-SAIL也考虑了隐私的危害。但这两项都代表了需要实现的“无人机操作将保持在控制之下”的信心水平。因此，在3D-SAIL和2D-SAIL的值相同的情况下，基于2D-SAIL和3D-SAIL确定的OSO鲁棒性水平是相似的。

例如，UAS操作被分配为GRC的6级、ARC的b级和PRC的b级。基于ARC因子和GRC因子，我们获得2D-SAIL因子的V值（见表4.1-原始方法）。然后，基于PRC系数和2D-SAIL系数，我们获得3D-SAIL的相同值：V级（见表4.6-扩展方法）。在这种情况下，由扩展方法（3D-SAIL）确定的OSO稳健性水平与由原始方法（2D-SAIL）确定的稳健性水平相似。这就是为什么在Harm扩展中，我们保持步骤“OSO鲁棒性确定”不变的原因。然而，我们认为，原始的OSOS清单是不够的，以保护UAS操作的网络安全。因为最初的OSO只处理无意的威胁（例如开发错误、飞行员的错误行为）。同时，故意威胁被忽略（如网络攻击），这可能会损害隐私和人的生命。第4.5节中提出的威胁扩展弥补了这一差距

4.5威胁扩展：SORA面临新的网络安全威胁

在上一节课中，我们将SORA方法的“蝴蝶结”风险模型的左侧扩展为新类型的伤害。接下来，我们用一种新的威胁——网络安全威胁来扩展这个模型的右侧。

4.5.1网络安全分类和风险模型扩展

根据第1.5节中的文献综述，我们提出了一种网络安全威胁分类法，分为三类（见表4.7）。一是"攻击"

4.5.威胁扩展：SORA面临新的网络安全威胁

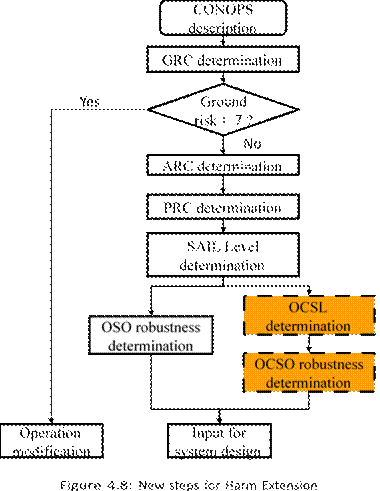


“软件/硬件体系结构”类别，代表所有可能的攻击，重点是利用自动驾驶仪和地面控制站（GCS）的软件和硬件。第二类是“通信攻击”，涵盖了针对通信领域网络安全漏洞的所有可能威胁。第三类是“对传感器的攻击”。该类别是所有网络物理系统（如UAS）的典型类型，其中传感器为系统提供感知物理环境的能力。然而，传感器也允许攻击者用虚假数据欺骗系统。由于我们的分类法是建立在文献综述的基础上的，因此建议的分类只能涵盖在现实生活或模拟中已被证实的网络安全威胁。这种分类法将来可以扩展到未发现的威胁。

|  |  |
| --- | --- |
| 描述 | 类别 |
| 加载到自动驾驶仪中的未经授权修改航路点[61] | 对软件的攻击 |
| 地面军事系统上的病毒[2] |
| 未经授权修改源代码[152] |
| 未经授权访问软件[152] |
| 视频重放攻击[3] | 攻击通信 |
| 对通信的反身份验证攻击[4] |
| 通过干扰通信控制无人机[57] |
| 视频数据公开[202] |
| GPS干扰欺骗[49]，[50] | 对传感器的攻击 |
| 摄像头欺骗[203] |
| IMU欺骗[51]–[53] |

表4.7：网络安全威胁类别

利用建议的分类法，我们将SORA风险模型的威胁端扩展为网络安全威胁类别，如图3.8所示。与经典SORA方法论的想法类似，网络安全威胁造成的“操作失控”危害可以通过威胁屏障加以预防或缓解。我们将这些障碍称为网络安全操作目标（OCSO），相当于原始方法的操作安全目标（OSO）。根据MEHARI方法指南和IEC62443基本安全服务清单，我们提出了三个新网络安全类别的OCSO清单（见附录a）。该列表由13个OCSO组成。从1号到7号的OCSo提供了保护软件的目标（包括存储数据、源代码、访问授权）。8号至12号OCSo旨在保护通信通道内数据的可用性、完整性和机密性。最后一个OCSO编号13是指与传感器提供的数据相关的保护。与原始方法的OSO类似，每个OCSO都有三个健壮性级别（低、中、高）的详细定义。对于每项操作，OCSO的稳健性水平取决于（1）UAS操作将保持在控制（或航行）下所需的置信水平和（2）操作对网络安全攻击的敏感性。例如，对于必须始终处于控制之下（高度航行）且非常容易受到网络安全攻击的操作，需要高鲁棒性OCSO。我们通过一个新的因素来描述操作敏感性：操作网络安全敏感性水平（OCSL）。



为了适应扩展的风险模型，我们在风险评估过程中提出了两个新步骤：OCSL确定和OCSO稳健性确定（见图4.8）。接下来，我们将详细讨论这些步骤。

4.5.2 OCSL测定

给定操作对网络安全攻击的敏感性取决于操作的内在特征。第一个特征是用于UAS操作的通信解决方案的性质。隔离的通信通道越多，攻击者到达UAS的机会就越少（用于发现、利用漏洞）。因此，该行动不易受到网络攻击。例如，使用专用/专用/军用通信解决方案的操作比使用互联网通信解决方案的操作更难实现。然而，在这一点上，应该清楚的是，我们并没有将“孤立”称为一种威胁

4.5. 威胁扩展：SORA面临新的网络安全威胁



针对网络安全攻击的保护解决方案，但这只是UAS操作的一个特征。第二种运行的特点是运行类型（VLO与BVLO）。在BVLOS操作中，车辆在相当长的距离内运行，超出驾驶员的视觉观察范围。因此，攻击者有更多机会发起攻击而不被发现，并且车辆的异常行为可能被隐藏（例如，在GPS欺骗的情况下）。同时，在VLOS操作中，由于网络安全攻击，车辆的异常行为可以被目视检测到。因此，我们认为BVLOS操作比VLOS操作更容易受到网络攻击。我们考虑的第三个特点是飞行员在操作过程中的监控。与未经持续监控的无人机相比，攻击者对在飞行员持续监控下飞行的无人机发动成功攻击的机会更小。最后一个操作的特征与第三方服务/设备有关。为了实现操作，UAS的运营商可以使用第三方提供的服务（如维护、飞行员、导航等）或补充设备（摄像头、计算机、通信模块）。未经UAS建造商（或制造商）认证的第三方服务/设备可能存在未知漏洞或后门。该攻击可利用/利用这些漏洞/后门对该行动发起网络攻击。例如，第三方公司的维护人员可以合法到达UAS并非法修改UAS的参数。当完整的U形空间概念可用时，该特性将更加重要（见1.4）。此时，许多与操作相关的任务和设备将由第三方提供商提供。

在OCSL确定步骤中，我们通过分析上述四个特征来评估操作敏感性：通信、操作类型、监控级别和第三方（可靠性）。我们使用表4.8为每个特征分配点。操作的OCSL是点的总和。

例如，一家公司使用无人机观察高速公路。在此操作中，车辆将在驾驶员的持续监控下从远离公路的地面站自动飞行。为了维持车辆与地面控制站之间的远程通信，UAS使用互联网（通过3G/4G移动网络）作为主要通信解决方案。公司使用由专业无人机建造商提供的完整无人机（包括所有材料和维护服务）。根据表4.8，该操作的评估如下：

•沟通：由于运营使用互联网来维持沟通，我们将2分配给该特征。

•操作类型：由于BVLOS，我们为该特性指定1。

•监控级别：由于飞行员持续监控操作，因此我们为该特性指定0。

•第三方可靠性：操作不使用任何第三方服务/设备，因此该特性分配为0。

•最后，运营网络安全敏感度等级或OCSL为3。

|  |  |  |  |
| --- | --- | --- | --- |
| 表达 | 类型  活动 | 监测水平 | 第三方（\*） |
| -2分  使用公共网络，如互联网。 | -1分  BVLOS | -1分  如果不是连续监测 | -2分  如果是不受信任的第三方服务/设备  用于UAS操作 |
| -1分  使用共享网络  例如，公司的内部网络  用于其他活动 | -0分  VLOS | -0分  如果连续监测 | -1分  如果UAS操作仅使用受信任的第三方服务/设备 |
| -0分  使用专用网络 |  |  | -0分  如果未使用第三方服务/设备 |
| （\*）：受信任的第三方是由UAS制造商验证/培训或认证的第三方 | | | |

表4.8：与CS相关的操作特征

4.6. 用于风险评估的扩展SORA基于Web的工具

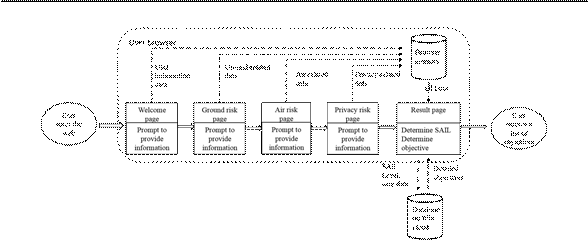


图4.9：应用程序概述

4.5.3 OCSO稳健性测定

作战网络安全目标（OCSO）的必要稳健性水平由作战行动的SAIL和OCSL通过表4.9确定。根据获得的OCSL，我们可以通过查阅附录A中的OCSO列表来确定详细的网络安全目标。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| OCSL | 6 | 中等的 | 中等的 | 高的 | 高的 | 高的 | 高的 |
| 5 | 中等的 | 中等的 | 中等的 | 高的 | 高的 | 高的 |
| 4 | 中等的 | 中等的 | 中等的 | 中等的 | 高的 | 高的 |
| 3 | 低的 | 中等的 | 中等的 | 中等的 | 中等的 | 高的 |
| 2 | 低的 | 低的 | 中等的 | 中等的 | 中等的 | 中等的 |
| 1 | 低的 | 低的 | 低的 | 中等的 | 中等的 | 中等的 |
|  |  | 我 | 二, | 三, | 四, | v | 不及物动词 |
|  |  | 帆 | |  |  |

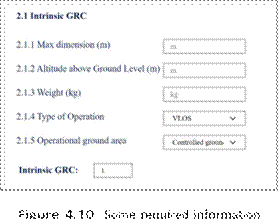
表4.9：OCSO测定

4.6用于风险评估的扩展SORA网络工具

4.6.1           说明和目的

该工具帮助用户根据SORA方法及其扩展自动进行风险评估。首先提示用户提供有关扩展操作的输入信息。基于此信息，我们的工具将自动确定与此类操作和相关安全目标相对应的航行高度。该工具是为具有不同目的的不同用户开发的：（1）操作员可以快速确定与预期操作相关的目标；（2） 运营商可以配置预期的运营，并平衡运营绩效与满足目标的成本；（3） UAS制造商/建造商可以快速预测与其客户特定运营相关的目标；（4） 管理局还可以使用此工具快速验证请求授权的操作。此外，开发该工具的目的是为了方便将来扩展SORA方法的新扩展工具，例如考虑新危害和新威胁。

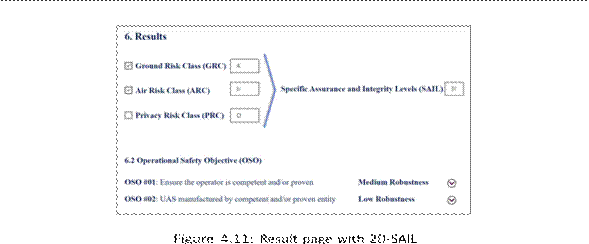
4.6.2           设计与实现



该工具是基于Wix平台开发的web应用程序。该平台提供了快速创建网站所需的工具/服务，并支持Java脚本语言创建定制功能。应用程序的结构如图4.9所示。我们的网站由五个页面组成，用户将在风险评估期间逐个浏览。在第一页中，提示用户提供一般用户信息（姓名、联系人、角色、用途）。在第二页上，用户必须提供与地面风险相关的信息，如飞机尺寸、作业区域和缓解措施（页面的一部分如图4.10所示）。对于一些“是/否”选项，用户可以解释如何满足这些选项。此类解释将用于在风险评估结束时创建最终报告。同样，第三和第四页提示用户提供与空气风险和隐私风险相关的信息。每个页面上提供的所有信息都存储在用户浏览器的内存中。根据这些信息，最后一页运行风险评估。首先，页面决定了帆的高度。此页面允许用户选择在确定航行高度时考虑哪些风险（见图4.11），例如地面风险和空气风险（原始SORA）或各种风险（扩展SORA）。然后，页面向Wix云上的数据库发送请求，以获取与确定的SAIL级别相关联的详细目标。此外，所有用户提供的信息也被发送到wix云上的数据库并存储在该数据库中。最后，向用户显示与预期操作相对应的所有所需目标。本应用程序的手册见附录B。

根据目前的设计，我们的工具可以很容易地扩展到采用其他SORA方法-

4.7. 结论



医学扩展。对于一个新的伤害扩展，我们只需要添加一个新页面来提示用户提供与这种伤害相关的信息，并稍微修改结果页面。同时，我们只需添加一个新页面，提示用户提供与此类威胁相关的信息，并将新目标添加到数据库中，以进行新的威胁扩展。

4.7结论

在这项工作中，我们旨在将原始SORA方法扩展到网络安全方面。SORA方法的当前文档仅解释了如何使用它，但没有解释它是如何工作的。因此，我们根据现有文件和我们关于风险评估的知识来描述方法的概念。然后基于这个概念，我们提出了一种扩展方法。该方法由两部分组成。第一个（危害扩展）是考虑网络安全/安全问题可能导致的新危害。目前，我们关注的是“侵犯隐私”的危害，这是公众接受无人机操作的一个基本问题。但我们也可以使用相同的策略将SORA方法扩展到其他类型的危害，如金融危害、材料破坏、关键设施等。第二部分（威胁扩展）是考虑网络安全威胁（或攻击）（与原始方法涵盖的意外威胁相比）以及相关的网络安全缓解措施。之后，我们以基于web的应用程序的形式提出了一个风险评估工具。该工具旨在简化风险评估任务，并快速适应其他拟议的SORA扩展。在本文的下一章中，我们将用不同的案例研究来说明我们的方法。

第五章

扩展SORA方法说明



目录

|  |  |
| --- | --- |
| 5.1导言。 | 84 |
| 5.2我们的方法与MULTIDRONE项目中使用的方法的比较。 | 84 |
| 5.2.1 CONOPS说明。 | 84 |
| 5.2.2 GRC测定。 | 85 |
| 5.2.3电弧测定。 | 86 |
| 5.2.4中华人民共和国的决定。 | 86 |
| 5.2.5帆的确定。 | 87 |
| 5.2.6 OSO稳健性测定。 | 88 |
| 5.2.7 OCSL的确定。 | 89 |
| 5.2.8 OCSO稳健性测定。 | 89 |
| 5.2.9结果讨论。 | 89 |
| 5.3其他案例研究的应用。 | 90 |
| 5.3.1“市区交付无人机”操作。 | 91 |
| 5.3.2工业现场监测。 | 94 |
| 5.4系统开发扩展SORA方法的使用。 | 97 |
| 5.4.1初始操作说明。 | 98 |
| 5.4.2扩展SORA分析。99                          5.4.3最终操作说明。101                          5.4.4系统说明。104                 5.5结论。107 | |

83

84第5章。扩展SORA方法说明



5.1导言

在上一章中，我们介绍了SORA方法的扩展版本，该方法考虑了网络安全方面。在本章中，我们使用此方法评估不同的操作。根据风险评估结果，我们讨论了我们方法的不同方面，并提出了一些改进。此外，SORA方法最初被设计为运营商和管理部门之间在行政过程中的沟通工具。这意味着使用SORA方法的主要目的是验证已定义的UAS操作和系统是否可以获得批准。但它也可以用于开发目的。本章说明了扩展SORA方法在UAS开发过程中的地位。本章的其余部分组织如下。首先，我们将我们的方法应用于实际操作，使用第5.2节文献中的原始方法进行评估。然后，我们考虑在第5.3节中市场所涉及的两个其他操作。接下来，我们将在第5.4节的开发过程中说明使用从扩展SORA获得的评估结果的方法。我们在第5.5节中总结了我们的工作

5.2我们的方法与MULTIDRONE项目中使用的方法的比较

在本节中，我们将对欧盟资助项目“多无人机”中引入的无人机操作进行风险评估。在这次行动中，一个无人机被部署到农村地区，与一些公众一起拍摄一场划船比赛。Captián等人的工作中介绍了该手术的风险评估[204]。在这项工作中，作者使用原始SORA方法进行了风险评估。在本案例研究中，我们使用扩展的SORA方法进行风险评估。我们将在案例研究结束时比较结果。

5.2.1 CONOPS说明

操作的完整描述非常长（如SORA方法附录A所述）。因此，我们仅提供一些必要信息的概述，以便在此步骤中进行风险评估。更多详细信息见[204]，

[205].

在这次行动中，无人机将跟随船只飞行拍照。由于该行动是在大范围内进行的（赛道为15公里），无人机将超越飞行员的视觉视线（BVLOS）并以自主模式飞行。该行动发生在人口密度较低的农村地区。据推测，河流两岸可能有许多观众，无人驾驶飞机不会飞越他们。表5.1总结了预期操作的基本信息。

|  |  |
| --- | --- |
| 主要无人机和操作规范 | |
| 框架 | DJI S1000+ |
| 自动驾驶仪 | 皮克斯霍克2.1 |
| 表达 | 泰雷兹LTE/Wi-Fi通信模块 |
| 降落伞 | 银河GRS 10/350 |
| 照相机 | BMMC+松下Lumix Vario镜头 |
| 大小 | 1,45米 |
| 重量 | 11公斤 |
| 海拔高度 | 10米 |
| 飞行模式 | 自主的 |
| 操作类型 | BVLOS |

表5.1：无人机和操作规范（来自多无人机项目）

5.2.2 GRC测定

我们首先确定作业的固有GRC，即在不考虑安全措施的情况下对地面人员的固有风险。由于无人机在农村地区飞行，不会飞越观众，因此我们将地面作业区划分为人口稀少的环境。根据有关操作区域和车辆尺寸（小于3m）的信息，我们为固有GRC分配了4个，如表5.2所示。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 固有地面风险等级 | | | | |
| 最大车辆尺寸 | 1米 | 3米 | 8米 | *>*8米 |
| 操作场景 |  |  |  |  |
| 受控地面区域上的VLO/BVLOS | 1 | 2 | 3 | 4 |
| 人口稀少环境中的VLO | 2 | 3 | 4 | 5 |
| 人口稀少环境中的BVLOS | 3 | 4 | 5 | 6 |
| 人口密集环境中的VLO | 4 | 5 | 6 | 8 |
| 人口环境中的BVLOS | 5 | 6 | 8 | 10 |
| VLO超过了人的聚集 | 7 | 没有 | | |
| B.过度聚集人群 | 9 |

表5.2:SORA方法的内在GRC表

然后，我们研究了行动的危害障碍，包括应急响应计划、战略缓解措施和减少地面影响。预期操作未实施任何应急响应计划，也未提及地面风险的任何战略缓解措施。这导致GRC增加（见表5.3）。操作员仅使用降落伞作为伤害屏障，以减少地面撞击。我们假设制造商测试了该降落伞，并且降落伞在不利激活情况下不会影响操作安全。因此，该伤害屏障处于中等稳健水平，有助于降低GRC（见表5.3）。手术的最终GRC保持在4。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 健壮性 | |  |
| 危害屏障 | 低/无 | 中等的 | 高的 |
| 地面风险的战略缓解 | 0 | -2 | -4 |
| 减少地面撞击的影响 | 0 | -1 | -2 |
| 应急响应计划 | 1 | 0 | -1 |
| 总相互作用 | 0 |  |  |

表5.3：最终GRC确定的缓解措施

5.2.3电弧测定

由于飞机在高于地面10米的高度飞行，在农村地区和不受控制的空域，与其他飞机碰撞的风险很低。因此，预期操作的初始弧为b，广义飞行密度为1（在5级[104]的范围内）。为降低作业的空气风险，运营商实施边界缓解措施，作为限制作业量的伤害屏障。然而，在这种情况下，根据SORA方法，伤害屏障没有用处，因为初始碰撞概率太低，无法降低。因此，最终电弧保持在b级。

5.2.4中华人民共和国的确定

正如我们在提案中提到的，我们分析了UAS的一些特征和操作，以确定隐私风险等级（PRC）。表5.1中提供了该步骤的大部分输入数据，但摄像机最小视角（AOV）的数据/信息除外。操作说明没有提供AOV的信息，但我们可以根据摄像机规格手动计算。摄像机规格如表5.4所示。

|  |  |
| --- | --- |
| BMMC相机，配备松下Lumix Vario镜头 | |
| 决议 | 2432x1366 |
| 传感器尺寸 | 16.64毫米x14.04毫米 |
| 焦距 | 从14毫米到42毫米 |

表5.4：摄像机规格（来自多无人机项目）

摄像机的最小AOV计算如下：



然后，我们得到无人机捕获的图像的最大像素密度如下：水平像素数



因此，图像细节处于“检查”级别（见表4.2）。此外，UA以BVLOS模式飞行，飞越农村地区。因此，我们为该操作分配了D的固有PRC（见表5.5）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类型  活动 | 农村地区，  VLOS | 农村地区，  BVLOS | 市区，  VLOS | 市区，  BVLOS |
| 图像细节级别 |  |  |  |  |
| 班长 | A. | B | C | C |
| 发现 | B | B | C | C |
| 看到 | B | C | D | D |
| 认出 | C | C | D | D |
| 识别 | C | D | E | E |
| 检查 | C | D | E | F |

表5.5：固有PRC测定

操作的最终PRC是初始PRC减去伤害屏障提供的风险降低。然而，操作说明并未提及任何损害地面人员隐私的障碍。因此，我们假设运营商没有应用任何伤害壁垒，最终PRC仍然是D。

5.2.5风帆测定

该操作分配给b弧和4 GRC。因此，2D-SAIL的值（考虑到ARC和GRC）为III（见表5.6）。2D-SAIL为III，PRC为D，3D-SAIL的值（考虑ARC、GRC、PRC）为IV（见表5.7）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 航海决心 | | | | |
|  | 弧 | | | |
| GRC | A. | B | C | D |
| ≤ 2. | 我 | 二, | 四, | v |
| 3 | 二, | 二, | 四, | v |
| 4 | 三, | 三, | 四, | v |
| 5 | 四, | 四, | 四, | v |
| 6 | v | v | v | v |
| 7 | 不及物动词 | 不及物动词 | 不及物动词 | 不及物动词 |

表5.6：风帆测定[104]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 2D-SAIL | |  |  |
| 中华人民共和国 | 我 | 二, | 三, | 四, | v | 不及物动词 |
| A. | 我 | 二, | 三, | 四, | v | 不及物动词 |
| B | 二, | 二, | 三, | 四, | v | 不及物动词 |
| C | 三, | 三, | 三, | 四, | v | 不及物动词 |
| D | 四, | 四, | 四, | 四, | v | 不及物动词 |
| E | v | v | v | v | v | 不及物动词 |
| F | 不及物动词 | 不及物动词 | 不及物动词 | 不及物动词 | 不及物动词 | 不及物动词 |

表5.7:3D-SAIL测定

5.2.6 OSO稳健性测定

利用IV的最终SAIL值（3D-SAIL），我们可以确定每个OSO的稳健性级别，然后确定需要实现的详细目标。详细目标如附录E所示。由于SORA方法旨在支持无人机操作授权申请，因此一些目标与操作员而非制造商有关（如评估天气条件和操作员能力）。因此，在本案例研究中，从制造商的角度出发，我们讨论了一些关键的OSO，这些OSO可被视为UAS开发过程的输入，用于预期操作：

•OSO#04的稳健性水平较低。它要求UAS必须按照主管当局认为适当的标准进行开发。应以较低的完整性水平应用这些标准（用这些标准定义）。制造商不必提供支持证据，只需声明符合标准即可。然而，目前还没有任何专门用于UAS开发的标准。或者，制造商可以应用航空领域广泛接受的一些安全标准，如DO178C、DO256。制造商还必须考虑与隐私和数据保护相关的标准。

•OSO#06处于中等稳健水平。它要求通信链路的特性适合操作。由于无人驾驶飞机在不受控制的空域飞行，飞行员不必与空中交通管制（ATC）保持通信，因此通信链路仅用于控制车辆。UAS可以使用未经许可的频段进行通信，如2.4GHz。然而，UAS需要向飞行员提供监控通信链路的手段（例如信号强度、丢包率）。与隐私问题相关，通信链路必须能够保护交换数据的机密性。UA的这些保护功能必须由合格的第三方进行验证。

•OSO#18处于中等稳健水平。它要求UAS能够检测并防止导致UA超过其飞行性能的错误飞行员输入（例如，飞行员让UA下降过快）。飞行包线的自动保护已发展到主管当局认为适当的标准。

5.2.7 OCSL测定

在这一步中，我们分析了四个特征：通信、操作类型、监控级别和第三方。对于通信，UAS配备了泰雷兹LTE/wifi通信模块。我们没有关于此通信模块的任何技术信息。我们认为这是一个专门的和高质量的UAS。在此操作中，车辆以BVLOS模式飞行，并在飞行员的持续监控下飞行。所考虑的UAS是建立在一些开源组件（如自动驾驶仪）的基础上的，我们认为这是一个不可信的第三方设备。基于此分析，我们将此操作的OCSL分配为3（见表5.8）。

|  |  |  |
| --- | --- | --- |
| 特征 | 描述 | 要点 |
| 表达 | 专用解决方案 | 0 |
| 操作类型 | BVLOS | 1 |
| 监测水平 | 由飞行员持续监控 | 0 |
| 第三方 | 不受信任的设备 | 2 |
| OCSL |  | 3 |

表5.8：OCSL测定结果

5.2.8 OCSO稳健性测定

最终航行为IV，OCSL为3，对于该操作，所有OCSO应满足中等鲁棒性水平（见表4.9）。例如：

•OCSO#1-防止非授权人员实施恶意行为。在中等鲁棒性水平上，该OCSO需要验证试图访问地面控制站（GCS）或自动驾驶仪的人员身份的机制。但是，目前，这些功能不适用于此操作中使用的自动驾驶仪。

•OCSO#13-检测传感器数据的异常。在中等鲁棒性水平上，OCSO需要通过两种方法验证传感器数据。第一个是检查来自传感器的数据是否超过合理的阈值。该操作中使用的自动驾驶仪软件目前采用这种方法。第二种方法是检查不同传感器之间的交叉一致性。对于此操作中使用的自动驾驶仪，我们没有关于此机制的任何信息。

5.2.9结果讨论

在本案例研究中，我们使用扩展的SORA方法对欧盟资助的多无人机项目中提到的UAS操作进行了风险评估。如上所述，Captián等人[204]根据原始SORA方法对同一手术进行了风险评估。表5.9总结了这些结果。

|  |  |  |
| --- | --- | --- |
|  | Capitán等人的评估[204] | 我们的评估 |
| 方法论 | 索拉 | 扩展囊泡 |
| GRC | 2 | 4 |
| 弧 | A. | B |
| 中华人民共和国 | 不适用 | D |
| 最后航行 | 我 | 四, |
| OCSL | 不适用 | 3 |

表5.9：结果比较

根据上表，我们的风险评估给出的SAIL临界值比Captán等人给出的更高（第四版SAIL与第一版SAIL）。因此，我们的评估要求安全目标（OSO）具有更高的稳健性水平。例如，在我们的评估中，无人机的设计必须能够确定可能的故障并将其发生率降至最低。同时，在Captián等人的评估中，这一目标不是必需的。造成这种差异的原因有两个。第一个是Captián等人使用了原始SORA方法的旧版本，该方法在评估时仍处于开发阶段，缺乏明确的说明。这导致高估伤害屏障的鲁棒性水平（如降落伞）。第二个原因是，我们的评估考虑了对地面人员的隐私伤害。在该操作中，隐私损害是一个重要方面，因为UAS配备了高性能摄像头，并且操作发生在拥挤的事件中。此外，与Captaán等人的工作相比，我们的工作更进一步，考虑了新的网络安全威胁，并确定了与网络安全相关的目标。某些已确定的网络安全目标未在所考虑的操作中实现。为了实现这些目标，需要大幅改变操作和UAS。这一变化可能使该行动更加安全，但也可能影响该行动的成本效益。

5.3适用于其他案例研究

在上一节中，我们将我们提出的方法应用于一个真实的UAS操作，该操作在一个欧洲研究项目中得到了很好的证明。在本节中，我们将介绍另外两个案例研究：“城区无人驾驶飞机交付”和“工业现场监控”，以进一步分析我们提出的方法。这些操作代表了UAS应用市场非常关注的两种UAS操作。

5.3.1“市区交付无人机”操作

5.3.1.1操作说明

在此操作中，电子商务公司将使用UAS将货物从其仓库运输到城市中的客户。为了优化运营的成本效益，运营商（电子商务公司）将在市中心建立仓库，并在仓库周围6公里范围内向客户提供服务。因此，飞机完全在市中心（城区）飞行。

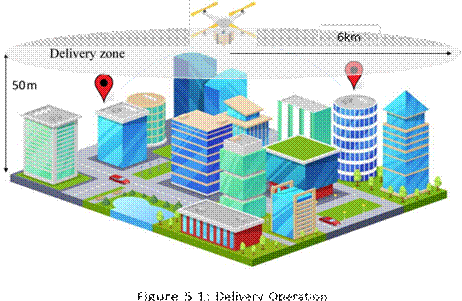
飞行计划在40米的高度进行，并超出飞行员的可视范围（BVLOS模式）。对于每次交付，飞机将根据客户的位置遵循不同的轨迹。因此，飞行员应在运行前准备飞行计划并上传至UAS。在操作过程中，飞机在飞行员的监控下按照预定的飞行计划自动飞行。因此，飞行员需要执行的主要任务是：准备飞行计划、开始和结束飞行、监控飞行、解决异常情况。该飞机将配备一个小型RGB摄像机，以帮助飞行员监控交付情况。该相机的分辨率为1920x1080像素，视角为40。我们假设摄像机能够检测地面上的人，并自动模糊他们的图像以保护他们的隐私（隐私保护过滤器）。◦

运营商计划使用最大尺寸为1.5 m、最大重量为10 kg的无人驾驶飞机。因为飞行是在人的上方进行的，所以飞机配备了降落伞。我们假设运营商将制定应急响应计划（ERP）以应对紧急情况。本操作文件明确了紧急情况下每个机组成员的任务和角色。据推测，降落伞和ERP都符合当局采用的标准。

5.3.1.2扩展的SORA分析

我们根据扩展方法进行风险评估，以确定安全目标（OSO）和网络安全目标（OCSO）。

1.    首先，我们确定预期操作的地面风险等级（GRC）。由于飞行发生在市区的BVLOS模式下，且飞机尺寸小于3m，因此固有GRC被指定为7。GRC可以通过两个伤害屏障来减少：应急响应计划（ERP）和降落伞。根据操作说明，这些屏障将处于中等鲁棒性水平，有助于将GRC降低1分。因此，此操作的最终GRC为6。



2.    我们确定预期操作的空气风险等级（ARC）。飞机将在市中心上空飞行，高度低于150米，远离机场。因此，根据SORA方法，该操作的ARC为c。

3.    结合c的弧和6的GRC，我们得到了V的2D-SAIL（见表4.1）。

4.    我们确定预期操作的隐私风险等级（PRC）。根据相机规格（1920x1080分辨率，40视角）和飞行高度，我们计算拍摄图像的像素密度。每米65.9像素，相当于“观察者”的详细程度（见表4.2）。由于飞行发生在市区，且处于BLVOS模式，因此我们指定了D的固有PRC。此外，摄像机可以自动检测并模糊人的图像。此功能有助于保护地面人员的隐私，并将PRC降低1个百分点。因此，运营的最终PRC为C。◦

5.    结合V的2D-SAIL和C的PRC，我们获得了V的SAIL 3D。使用该SAIL值，操作应在高鲁棒性水平上满足OSOs的要求。详细目标见SORA方法[98]附件E。

6.    我们评估预期操作的网络安全敏感性（OCSL）。我们假设UAS将使用移动网络（4G）来维持飞机与地面站之间的通信。数据将通过可信第三方服务提供的云传输。因此，我们将操作分配为OCSL 4，如表5.10所示。

7.    3D-SAIL为V，OCSL为4，操作应满足高鲁棒性水平的OCSOs。OCSO详见附件A。

|  |  |  |
| --- | --- | --- |
| 特征 | 描述 | 要点 |
| 表达 | 公共网络 | 2 |
| 操作类型 | BVLOS | 1 |
| 监测水平 | 由飞行员持续监控 | 0 |
| 第三方 | 仅受信任的设备 | 1 |
| OCSL |  | 4 |

表5.10：OCSL测定结果

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 分析 | | | |  | 分析 | | | |
| GRC | 6 | 2D-SAIL | v | GRC | 6 | 3D-SAIL | v |
| 弧 | C | 3D-SAIL | v | 弧 | C | 3D-SAIL | v |
| 中华人民共和国 | C | OCSL | 4 | 中华人民共和国 | D | OCSL | 4 |

                 （a） 带隐私保护过滤器（b）不带隐私保护过滤器

表5.11：交付操作的分析结果

5.3.1.3结果讨论

分析结果如表5.11a所示。根据分析，根据上述操作说明，运营商必须以高鲁棒性水平（20/24目标）满足大多数操作安全目标，并以高鲁棒性水平满足所有操作网络安全目标。据我们所知，目前市场上没有能够满足这些目标的系统（V型或VI型帆）[5]。一方面，我们发现这项行动的成本非常高。因为它需要很多资源来实施复杂的网络安全解决方案，并符合不同的标准（开发、设计、维护等）。另一方面，我们仍然可以为这次手术降低一点手术成本。在操作说明中，假设摄像机能够识别地面上的人的图像，并将其从视频中删除。这种相机可能比没有这种功能的标准相机更贵。如果删除此功能（隐私保护过滤器），会发生什么情况。在这种情况下，操作的PRC将是D而不是C。新的分析如表5.11b所示。我们有相同的3D-SAIL值，然后是相同的OCSOs和OSOs。因为在这次行动中，飞机飞得太高，相机的分辨率太低，不会影响地面上人们的隐私。因此，在这次行动中，我们可以使用标准摄像机来降低行动成本，而不会增加OCSO和OSO的复杂性。

让我们考虑相同的案例研究，但具有较低的高度（20米）和更高性能的相机（分辨率为400x3000像素，最小视角为11）。分析结果如表5.12a和5.12b所示。在操作说明中，如果未提及隐私保护过滤器，3D-SAIL将从V增加到VI，我们必须以高鲁棒性水平满足所有OSO（而不是仅满足20/24个目标）。这使得运营成本增加。◦

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 分析 | | | |  | 分析 | | | |
| GRC | 6 | 2D-SAIL | v | GRC | 6 | 2D-SAIL | v |
| 弧 | C | 3D-SAIL | v | 弧 | C | 3D-SAIL | 不及物动词 |
| 中华人民共和国 | E | OCSL | 4 | 中华人民共和国 | F | OCSL | 4 |

                 （a） 带隐私保护过滤器（b）不带隐私保护过滤器

表5.12：改进交付操作的分析结果

通过这些讨论，我们认为应以优化运营成本的方式使用SORA方法（扩展或原始版本）。具体而言，如果可能，我们可以调整操作描述的一些参数，以获得鲁棒性级别较低的OCSO和OSO。这一论点对操作员和制造商尤其有用。因此，当我们在开发过程中使用扩展的SORA方法时，我们会考虑这一论点（见5.4）。

5.3.2工业现场监测

5.3.2.1操作说明

在此操作中，一家工业公司将使用UAS监控其工业现场。假设该场地远离居民区和机场。因此，我们可以认为飞机在农村上空飞行。飞机重量约为20公斤，最大尺寸为2米宽。

飞机将沿着预先确定的轨道在30米的高度绕工厂飞行。飞机不允许飞越工厂区。由于工业场地非常大，飞机将飞出飞行员的可视范围并自动运行。在飞行过程中，飞行员根据飞机的飞行信息对飞机进行观察。飞行信息通过专用无线连接传输到地面控制站。

发生故障时，公司希望尽快确定运行区域内的航班（内部无人）。此外，降落伞不会用来防止飞机坠落到工厂。

该飞机将配备RGB摄像机，用于监控工业现场。该相机的分辨率为1920 x 1080像素，最小视角为20◦

5.3.2.2扩展的SORA分析

我们根据扩展方法进行风险评估，以确定安全性

目标（OSO）和网络安全目标（OCSo）。

1.    首先，我们确定预期操作的地面风险等级（GRC）。由于飞行在农村地区（人口稀少环境）的BVLOS模式下进行，且飞机尺寸小于3m，因此将固有GRC分配给

4.

2.    我们确定预期操作的空气风险等级（ARC）。飞机将在农村地区上空飞行，高度低于150米，远离机场。因此，根据SORA方法，该操作的弧为b。

3.    结合b的弧和4的GRC，我们得到了III的2D-SAIL（见表4.1）。

4.    我们确定预期操作的隐私风险等级（PRC）。根据相机规格（1920x1080分辨率，20视角）和飞行高度，我们计算拍摄图像的像素密度。它是每米181像素，相当于“识别”的详细程度（见表4.2）。由于航班发生在农村地区，且处于BLVOS模式，因此我们将固有PRC指定为C。由于UAS用于监控站点，因此未应用隐私保护。因此，操作的最终PRC保持在C级。◦

5.    结合III的2D-SAIL和C的PRC，我们得到III的SAIL 3D。使用该SAIL值，操作应满足低或中等鲁棒性水平的OSOs。详细目标见SORA方法[98]附件E。

6.    我们评估了预期操作的网络安全敏感性（OCSL），如表5.13所示。该操作的OCSL为2。

|  |  |  |
| --- | --- | --- |
| 特征 | 描述 | 要点 |
| 表达 | 专用解决方案 | 0 |
| 操作类型 | BVLOS | 1 |
| 监测水平 | 由飞行员持续监控 | 0 |
| 第三方 | 仅受信任的设备 | 1 |
| OCSL |  | 2 |

表5.13：OCSL测定结果

7.    3D-SAIL为III，OCSL为2，操作应满足中等鲁棒性水平的OCSOs。OCSO详见附件A。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 分析 | |  |
| GRC | 4 | 2D-SAIL | 三, |
| 弧 | B | 3D-SAIL | 三, |
| 中华人民共和国 | C | OCSL | 2 |

表5.14：带有隐私保护过滤器

5.3.2.3结果讨论

分析结果如表5.14所示。根据该结果，操作员必须仅以低或中等鲁棒性水平（相对于交付操作中的高鲁棒性水平）满足目标。该结果是“工业现场监控”操作的典型结果。工业用地通常分布在大片区域，远离住宅区，远离机场。因此，“工业现场监控”作业具有一些共同特征，如农村作业区、BLVOS、低活动密度空域。根据SORA方法，具有这些特征的操作通常并不重要。这是不合理的。例如，考虑到“核电厂监测”、“太阳能发电计划监测”和“a现场监测”三项业务，我们得到了相同的结果。原因是（原始或扩展）的当前版本只考虑了对人类的直接伤害（生命或隐私的损失）。尚未发现对基础设施或工业场地的危害。事实上，这一主题非常复杂，因为不同工业领域的危害评估可能是多种多样的。

目前，我们提出了解决上述问题的临时解决方案。对于“工业现场监控”操作，我们将在3DSAIL中添加“补充点”。这些观点部分反映了工业场地的关键性质。将根据两个问题对分数进行评估：（1）“工业现场是否生产或储存危险产品（如有毒、汽油、辐射材料）”，（2）“该现场是否储存敏感信息？”（见表5.15）。

|  |  |  |
| --- | --- | --- |
| 补充要点 | |  |
| 工业用地类型 | 没有敏感信息 | 敏感信息 |
| 无危险品 | 0 | 2 |
| 危险品 | 1 | 3 |

表5.15：“补充点”评估

将此解决方案用于上述三个操作，我们得到了新的结果，如表5.16所示。核电站是最关键的基础设施之一。因此，VI的3D-SAIL和最高鲁棒性级别的OSOs是合适的。如果我们不考虑可能的“金融”危害，太阳能计划权的运作与一个领域的运作具有相同的临界水平。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 监控操作 | |  |
|  | 核电厂 | 太阳能发电厂 | 田地 |
| 补充要点 | 3 | 0 | 不适用 |
| 最终3D-SAIL | 不及物动词 | 三, | 三, |

表5.16：应用补充点后三种监测操作的比较

5.4利用扩展的SORA方法进行系统开发

扩展的SORA方法需要一些关于预期操作（如操作区域、操作类型）的简单信息来执行风险评估。该评估的结果是一份安全和网络安全目标清单。当我们定义操作的详细特征（如组织、操作程序、培训）和系统规范时，这些目标可以得到满足。这意味着我们可以使用扩展的SORA分析来细化操作描述和系统描述。因此，当客户的需求转化为系统描述时，我们建议将扩展的SORA分析集成到开发过程的早期阶段。图5.2显示了我们的建议。该提案的详细解释如下：

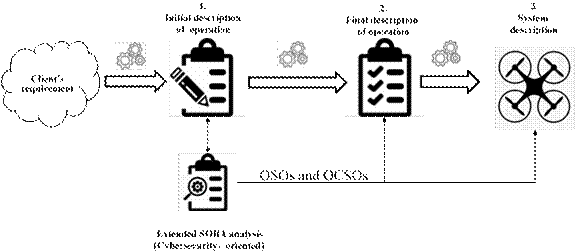


图5.2：将扩展SORA分析集成到开发过程中的拟议方法

1.    初始操作描述：在开发过程开始时，我们假设客户机只能提供所需操作的简单信息。这些信息可能是客户的需求或关于操作的想法。例如，客户需要一个UAS来监控数千公顷的土地或交付小包裹。该信息不够详细，无法执行扩展的SORA分析。因此

我们首先建立初始操作描述。本文件包括执行扩展SORA分析的输入信息（例如，操作目的、VLOS操作或BLVOS操作、操作区域、飞机尺寸、伤害屏障等）。这些是扩展SORA方法中评估的操作参数。我们可以在与客户讨论其需求的基础上收集、推理或选择这些参数。

2.    扩展SORA分析：根据初始操作描述，我们执行扩展SORA方法。因此，我们获得了“作战”安全目标（OSO）和“作战”网络安全目标（OCSO）。在这一步中，我们可以灵活地应用方法来优化运营成本，正如我们之前的结论（见5.3.1.3）。例如，我们可以增加新的伤害壁垒，并在较低的鲁棒性水平上满足目标；或者移除一些伤害障碍，但满足相同级别的目标。

3.    最终操作说明：在此步骤中，我们根据JARUS在[184]中提供的表格建立最终操作说明。最终操作说明应符合安全/网络安全目标和上一步中定义的初始说明。此外，本说明应尽可能澄清如何使用UAS。

4.    系统描述最后，我们描述了满足最终操作描述、安全和网络安全目标的系统架构。

接下来，我们将在“工业现场监控”案例研究中说明上述方法。

5.4.1初始操作说明

为了监控高灵敏度的工业工厂（如核电站、化工厂），业主公司将部署一个配备热摄像机的无人机。UAS将部署在位于农村地区的工厂周围进行飞行。飞行计划由业主公司确定，并对所有航班进行重复。根据飞行计划，无人机不飞越核电站，与核电站保持200米的距离。检查区域附近没有机场。无人机重量为20千克，最大尺寸为2米宽；其设计为在超视距（BVLOS）下自动飞行，整个运行期间的高度为地面以上30m。

在飞行过程中，飞行员通过地面军事系统计算机实时观察无人机的状态无人机和高速公路。飞行员只需要执行三个简单的动作：开始飞行、结束飞行（返回待机模式）、回家。地面军事系统和飞机之间交换的数据通过无线通信信道传输。

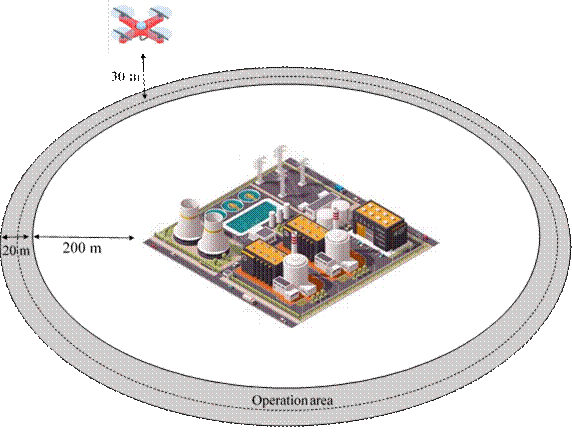


图5.3：无人机操作

飞机配备有摄像机，其特点如下：

•分辨率：1920 x 1080

•最小视角：10度。

5.4.2扩展的SORA分析

通过执行扩展SORA分析，我们获得了给定操作的VI 3D-SAIL和OCSL（操作网络安全敏感级别）2。该分析的详细内容见5.3.2。根据该方法，我们应该满足最高鲁棒性级别的OSO和中等级别的OCSO。这些OSO见原始SORA方法的附录E（读者可在本论文的附录E中找到），OCSO的详细信息见表5.17。

|  |  |
| --- | --- |
| 名称 | 描述 |
| OCSO#01 | -            定义识别和验证试图访问地面军事系统和自动驾驶仪的人员的流程/机制。  -            定义创建/修改/删除个人身份的流程/机制 |
| OCSO#02 | -定义组织中每个人的权利，这些人可以与自动驾驶仪和地面军事系统交互。  -定义分配/修改/撤销每个人权利的流程/机制 |
| OCSO#03 | -定义流程/机制，以限制一个人可以作为其分配权利执行的行动 |
| OCSO#04 | -定义安全机制，以保护储存在地面军事系统和自动驾驶仪中的飞行计划、飞行参数（PID参数、滤波卡尔曼参数、传感器校准等）和记录数据（视频数据、日志数据）的完整性。 |
| OCSO#05 | -定义安全机制，以保护存储在地面军事系统和自动驾驶仪中的数据/信息的机密性 |
| OCSO#06 | -分析飞行后软件/硬件上的异常行为，以检测飞行后检查中的异常行为。 |
| OCSO#07 | -将软件/硬件体系结构划分为具有不同临界级别的不同“区域”。一些硬件/软件可能比其他硬件/软件更容易受到网络攻击，但它们提供的功能不如其他硬件/软件那么重要 |
| OCSO#08 | -定义确保通过通信设备传输的每个数据的机密性的机制。 |
| OCSO#09 | -定义机制以确保通过通信设备传输的每个数据包/消息的完整性 |
| OCSO#10 | -            定义用于测量通信信道性能的参数。  -            地面军事系统向飞行员显示定义的参数  -            建立一个安全指令，飞行员可以用它来检测通信信道性能的下降 |
| 奥克索#11 | -定义在通信性能下降的情况下重新建立通信或维护几个基本服务的机制。 |
| 奥克索#12 | -            定义用于在每次飞行后诊断通信信道性能的参数。这些参数将记录在自动驾驶仪和地面军事系统上。  -            制定安全说明，飞行员或维修人员可通过检查日志来检测异常情况 |
| 奥克索#13 | -根据传输数据的关键性级别和脆弱性级别，将通信系统划分为不同的信道。 |
| 奥克索#14 | -通过分析来自不同传感器的数据之间的一致性和一致性，定义检测异常传感器数据的机制。 |
| 奥克索#15 | -定义保护传感器免受环境干扰的解决方案  （攻击者可以利用共振频率的干扰来操纵加速器传感器的输出） |



表5.17：中等稳健性水平的OCSO定义

5.4.3最终操作说明

我们可以根据定义的OCSO和OSO以及初始操作说明，建立最终操作说明。根据JARUS[184]提供的表格，该描述包括组织结构、操作程序、培训、制造商、开发标准等多种信息。针对本论文的主题——网络安全，我们在此仅提及与网络安全方面相关的信息。

5.4.3.1操作员

我们打算让UAS由三人操作：一名运营经理、一名主驾驶员和一名副驾驶员。运行经理负责整个运行并管理飞行员。主驾驶员负责观察和控制飞机。副驾驶员负责操作摄像机，观察工厂。根据各成员的角色，其权利定义如下：

•运营经理可以创建/修改/删除试点账户

•为了控制和观察飞行，主驾驶员可以：

–从地面军事系统向飞行器发送命令（起飞、着陆、按计划飞行、飞行终止）。

–访问飞行信息（高度、位置、姿态、电池信息、通信状态）。

–控制和指挥车辆。

–访问摄像头捕获的视频。

–访问记录的文件以执行飞行后分析。

•为了控制摄像机并观察工业现场，副驾驶员可以：

–访问摄像头捕获的视频控制和命令摄像机。

通过定义每个成员的具体权利，我们满足OCSO#2。

5.4.3.2操作程序说明

操作程序包含飞行员执行的逐步任务，以有效应对不同情况。操作程序包括正常情况、应急情况和紧急情况。这些情况根据空域而有所不同

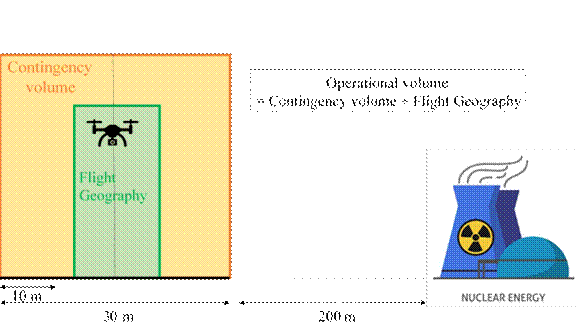


图5.4：运营量

飞机定位的体积。我们在空间和时间上将运行量分为两个空域量：飞行地理和应急量，如图5.4所示。飞行地理是指飞机正常运行并采用正常程序的空域容量。在该操作中，飞行地理是一条10 m宽的走廊，沿着并覆盖预定轨迹。这意味着在该操作中，我们接受飞机位置5 m的公差。应急量是飞行地理以外的空域容量，我们认为该操作处于异常情况，但仍在控制中。当运行处于异常情况时，飞行员应遵循应急程序，恢复控制下的运行。如果飞机超出应急容量，则视为失去控制或处于紧急情况。当操作失控时，飞行员应遵守应急程序，以限制升级影响。操作程序的细节如下所示。

（a） 正常飞行程序

当UAS按照运营商的意图正常运行时，正常程序已到位。飞机自动飞行，飞行员只需在地面站观察飞行

（b） 应急程序

当飞机运行异常并超出飞行地理范围时，我们启动应急程序，并进入应急容量。我们假设作业区是空的（没有人、没有建筑物、没有设施等），并且受到保护。因此，当飞机超出飞行地理范围时，我们打算取消飞行，并尽快将车辆降落在作业区内。因为如果飞机继续飞行，它可能会飞出操作范围，撞到核电站上。它应该自动进入着陆模式并为飞行员加热。这一要求可以通过地理围栏解决方案来实现（将飞行限制在定义边界内）。假设飞机在着陆时仍倾向于超出应急容量。在这种情况下，主驾驶员接管以手动控制飞机，并将其降落在操作范围内。在这种情况下，UAS应将可能的原因告知飞行员并使其暖和起来。应考虑以下原因：

•导航数据退化（来自GPSs、IMU）：在这种情况下，导航数据不够精确，无法保持飞机跟踪预定轨迹，但足够精确，无法保持飞机飞行。

•机械部件（电机、叶片、机身）退化。

•电池耗尽

•通信中断：在这种情况下，飞行员无法识别情况，无法接管飞机。飞机应进入着陆模式并自动着陆。

•恶劣的天气条件。

（c） 应急程序

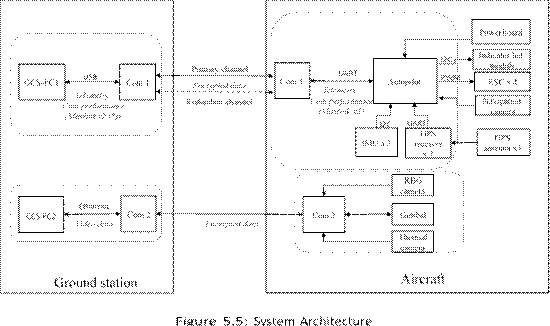
当飞机超出应急容量时，我们认为操作失控。它要求航班终止。土工围栏机构应关闭所有电机，并让飞机自动降落。如果自动飞行终止失败，主驾驶员应手动激活飞行终止。副驾驶员应在紧急情况下为经理和地面人员保暖。

（d） 飞行后

在这个阶段，飞行员寻找飞机行为和通信链路的任何异常情况（例如，丢包率、包失效、信号强度）。这些异常可能表明飞行过程中发生的故障或网络攻击。例如，飞机的轻微振动可能表明GPS性能下降或IMU可能受到攻击。飞行员在飞行过程中很难立即发现这个问题。然而，通过观察和分析整个数据，飞行员可以在飞行后阶段轻松识别振动。必须记录任何异常情况，并向制造商报告。飞行后程序允许我们满足OCSO#06、OCSO#10和OCSO#14中提到的与飞行后分析中异常检测相关的目标。

5.4.4系统说明

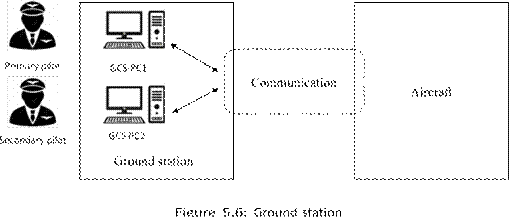
通过分析已定义的网络安全目标和操作描述，我们提出了一个UAS架构，如图5.5所示。在本节的剩余部分中，我们将解释选择此系统的原因。



5.4.4.1地面站

地面站为飞行员提供与系统交互的人机界面。如（5.4.3.1）所述，两名飞行员（一级飞行员和二级飞行员）直接参与操作具有不同属性任务的无人机。为确保飞行员只能执行为其角色定义的动作（OCSO#03），地面站应为他们提供不同的接口。将有两个单独的接口。我们称之为主引导接口和辅助引导接口。主飞行员界面允许主飞行员识别飞行状态（位置、高度、姿态、电池状态）。该界面还允许主飞行员使用不同的屏幕按钮操纵飞行：防护（启动）、解除防护（停止电机）、起飞、着陆、回家、故障保护。当飞行员点击这些按钮时，相关命令被发送到飞机。辅助界面显示摄像头的视频、车辆位置、地理地图和摄像头的方向。副驾驶员可以通过操纵杆控制摄像机的移动。

主飞行员界面和辅助飞行员界面为飞行员提供不同关键级别的功能。主飞行员界面提供控制和指挥飞机的功能，这对操作安全至关重要。同时,



辅助飞行员界面几乎与控制、命令摄像机的功能有关。这些功能被认为是实现运营目标（监控工业现场）的必要功能，但对飞行来说并不重要。例如，假设对手操纵辅助飞行员界面。在这种情况下，飞行仍然可以控制，不会对车辆和工厂造成任何重大影响。因此，根据OCSO#07（软件/硬件划分），我们将地面控制段分解为两个独立的部分，如5.6所示。第一部分包括地面控制站计算机（GCS-PC1）和相关软件，用于控制和指挥飞机（主飞行员界面）。第二部分由另一台计算机和相关软件组成，用于控制和命令摄像机（辅助飞行员界面）。地面军事系统PCs的使用应严格限于指定的飞行员，以避免误用或破坏。为此，地面军事系统PC应识别和验证试图访问的用户，如OCSO#01（用户识别和验证）所述。飞行员将被提示提供其飞行员账户信息，包括访问GCS-PCs时的账户id和密码。如5.4.3.1所述，运营经理将管理飞行员账户。因此，我们建议两个GCSPC向运营经理提供一个特定的界面，用于创建、修改或删除试点账户。只能使用管理员帐户访问此界面。

为支持飞行后分析（见5.4.3.2），GCS-PC1应记录并存储飞机的飞行信息，GCS-PC2应记录飞行期间摄像机捕获的视频。正如OCSO#04和OCSO#05中提到的，我们应该保护存储数据的完整性和机密性。为此，我们可以使用加密哈希算法（如SHA-224、SHA-256、SHA-384等）来保护数据的完整性，并使用加密算法（如AES-128、AES-256）来保护数据的机密性。

5.4.4.2飞机段

（a） 自动驾驶仪

在正常情况下，飞机将自动飞行，无需飞行员的交互。自动驾驶仪应按照预定轨迹驾驶飞机。轨迹是重复的，所有飞行的机身都不会改变。因此，我们可以将飞行计划、操作体积边界（在5.4.3.2中提到）和飞行控制参数嵌入自动驾驶仪固件（对于某些商用自动驾驶仪，这些参数是可调的，并存储在闪存中）。这有助于防止对手非法访问和修改这些参数。此配置符合OCSO#04和OCSO#05（数据完整性和机密性保护）。为了提供更高的保护级别，我们还可以考虑保护固件完整性的机制，例如，在[206 ] -（208）中提到的那些机制。

如飞行后程序（见5.4.3.2）所述，飞行员在每次飞行后进行飞行后分析。对于该活动，自动驾驶仪应将飞行信息记录并存储为加密数据，并伴有加密散列。有助于保护数据机密性和数据完整性（根据OCSO 04和OCSO 05的要求）

（b） IMU和GPS

IMU（加速计、陀螺仪和指南针）和GPS接收器是为自动驾驶仪提供导航数据的基本传感器。如OCSO#15所述，传感器冗余应到位。冗余有两种形式：组件冗余和数据冗余。组件冗余提供三重IMU和三重GPS接收机。如果其中一个GPS（或IMU）发生故障，自动驾驶仪应根据剩余的GPS（或IMU）检测故障，并向地面站发送警报。对于数据冗余，飞机将配备嵌入式摄像头模块，该模块提供除GPSs和IMU之外的第三个导航数据源。自动驾驶仪应检测三个数据源之一是否不可靠。这些冗余使得通过传感器进行攻击（尤其是GPS欺骗）更加困难。

（c） 有效载荷

飞机配备了一个摄像头模块，包括一个RGB摄像头、一个用于拍摄监控现场的热摄像头，以及一个用于稳定和控制摄像头方向的万向节。如5.4.4.1所述，我们认为与视频记录相关的功能不如与航班相关的功能那么重要。根据OCSO#07（软件/硬件划分），摄像机模块应独立于自动驾驶仪。

5.4.4.3通信段

通信系统应确保地面控制段和飞机段之间的数据流。有两种传输数据：地面军事系统和自动驾驶仪之间的遥测数据（飞行状态和飞行员指令）；地面军事系统与地面军事系统之间的摄像机数据

5.5. 结论107

摄像头模块。根据OCSO#08和OCSO#09，应实施加密方案，以保护传输数据的完整性和机密性。然而，每种数据的加密机制可能会因其不同的性能要求而有所不同。对于遥测数据，需要低延迟传输，但可以接受低带宽。而对于摄像机数据，虽然不严格要求低传输延迟，但需要高带宽。此外，我们认为遥测数据比摄像机数据对操作的安全性更为关键。因此，根据OCSO#13（通信分区），此类数据应在两个独立的通信链路内传输：Com 1（遥测数据）和Com 2（摄像机数据）。

由于遥测数据对控制和指挥飞行至关重要，Com 1链路应提供冗余机制，以确保数据的可用性和可靠性（如OCSO 11所述）。例如，数据可以在两个不同的频带上传输。一个频率始终处于激活状态，如果第一个频率上的通信性能下降，另一个频率将激活。

为支持飞行后程序（见5.4.3.2）并满足OCSO#12的要求，应估计通信链路性能，并将其存储在地面军事系统PC和自动驾驶仪上。我们提出了三个参数来评估链路性能：包丢失百分比、信号强度、延迟时间。

5.5结论

为了说明和讨论我们提出的扩展SORA方法，我们对不同的UAS操作进行了风险评估。第一个是“农村地区航空摄影”行动——这是一个在欧洲资助的项目中得到充分记录的真实行动。另一种是“市区无人机交付”和“工业现场监控”业务，我们根据市场需求建立。分析结果，我们有以下几个论点：

•扩展方法要求安全目标比原始方法更加稳健。一方面，这意味着使用扩展的方法，UAS操作可以达到更高的安全和安保水平。另一方面，为了满足更高的安全级别，它可能需要更多的资源，并影响UAS操作的成本效益。

•SORA方法（扩展版或原始版）可灵活用于优化运营成本。这一论点对操作员和制造商尤其有用。

•SORA方法（扩展版或原始版）目前不适用于与工业区相关的操作。我们引入了一个简单的解决方案来评估工业区，并改进了此类操作的SORA方法，以解决此问题。

除了用我们提出的方法说明风险评估外，本章还定位了评估结果在开发过程中的使用。我们建议使用这种风险评估考虑网络安全（也安全）方面时，客户的需求转化为系统描述。根据客户的要求，我们首先制定操作说明，然后制定符合规定网络安全目标的系统说明。我们通过“工业现场监控”案例研究来证明这一建议。请记住，本提案的目的不是引入完整的开发过程。这只是一个将网络安全纳入发展过程的想法。

全球结论和展望

结论

本文介绍了我们在无人机系统网络安全方面的工作。网络安全问题是阻碍公众接受UAS应用程序的问题之一。在这项工作中，我们专注于为UAS开发网络安全风险评估方法。风险评估（包括风险分析和进一步的风险管理）是确保系统网络安全的决策过程的关键部分。此外，应将风险评估视为系统开发过程的一部分。我们的工作有两个主要贡献：

•管理无人机网络安全风险的方法（第3章）。风险管理是一个比风险评估更大的术语。除风险评估外，风险管理还包括其他活动：环境建立、处理，以及利益相关者之间可能的沟通活动。但我们方法的重点是风险评估。在该方法中，风险评估包括风险识别和风险分析/评估。风险识别一般不侧重于识别针对UAS的新类型攻击。但它侧重于列出针对所考虑的UAS的可能攻击，并在攻击树图上显示它们。风险分析/评估旨在根据攻击的难度和影响评估攻击的严重性。评估有助于确定应首先考虑或处理的攻击，以及应稍后考虑或忽略的攻击。这项工作为读者提供了一个工具来系统地评估网络安全风险，并为UAS制定网络安全要求。方法应用的结果取决于用户的主动性判断和他们的知识。因此，不同专家的参与可以提高结果的覆盖面。我们可以在UAS体系结构定义之后和开发过程中的实现之前使用这种方法。这种方法的弱点是成本效益。实施由此产生的网络安全要求可能需要大幅修改系统架构；这可能很昂贵。

•基于SORA方法的综合网络安全风险评估方法（第4章和第5章）。SORA方法最初是一种专门用于操作安全的风险评估方法。原始方法考虑了一组安全风险，这些风险由蝴蝶结模型建模。该模型包括威胁、危险、危害和障碍。最初的方法只注重安全性；因此，它只考虑对人类生命的意外或“非故意”威胁和伤害。通过提供的评估表，用户可以评估风险并确定安全目标。为了将SORA方法扩展到网络安全，我们首先将风险模型扩展为三种新的“故意”威胁和隐私损害。然后，我们介绍了我们的评估机制，它符合

109

全球结论和展望



用哲学的原始方法论。基于此机制，用户可以评估风险并确定安全和网络安全目标。我们提出的策略可用于扩展该方法，以涵盖其他未知威胁和其他危害。最初的方法主要设计用于管理过程中的UAS操作验证，而不是开发过程。因此，我们介绍了将扩展SORA评估集成到开发过程中的方法。这种方法从客户的需求开始，以系统架构结束。我们提出的解决方案的优点是：（1）执行风险评估非常容易（尤其是使用我们的基于web的工具），（2）在早期（在系统架构设计之前）考虑网络安全问题。然而，它也有一个弱点。该方法仅考虑了风险模型中呈现的一组有限风险以及所提供列表中列出的目标。因此，很难考虑日新月异的新攻击技术。

态度

作为我们工作的视角，我们考虑以下工作：

|  |
| --- |
| 实施 |

|  |
| --- |
| 系统  描述 |

1.    SORA方法的进一步扩展：目前，我们扩展的SORA方法只考虑对人类生命和隐私的损害。因此，它不适用于与基础设施或工业现场相关的UAS操作，在这些基础设施或工业现场，攻击或事故的后果可能是设施损坏或敏感信息泄露。在我们的工作中，我们为这个默认值提出了一个简单的解决方案。然而，这应被视为一种临时解决办法。在未来，它需要更深入地分析这种操作，并创造一种新的危害（例如“工业基础设施损害”）。

图5.7：开发过程中提出的两种方法

2.    在开发过程中结合提出的方法：我们提出了两种不同的方法。一个可以在开发过程中早期使用，但它不足以考虑新的攻击技术。另一个可以在开发过程中使用，并且足够灵活地考虑新的攻击（取决于用户的专业知识）。因此，我们可以在相同的开发过程中使用这两种方法，如图5.7所示。这使我们能够作出全球性的结论和展望



在开发过程中考虑网络安全方面。目前，我们不验证这一想法。

3.    基于Web的工具：目前，我们只有一个用于扩展SORA方法的基于Web的工具。未来，它需要为另一种方法开发另一种工具。

4.    反馈：我们通过一些案例研究对我们提出的方法进行了测试和评估。然而，为了得到客观的评估和改进我们的工作，这些方法应该被工业专家推广、测试和评论。

附录A

运营网络安全目标



113

**A.与软件/硬件架构攻击相关的OCSo**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **描述** |  | **诚信水平** | | |
|  | **低的** | **中等的** | **高的** |
| **OCSO#1#U软件/硬件**  识别并验证试图访问地面军事系统和自动驾驶仪的实体（\*）  关键词：识别和认证    *注意：实体可以是人，也可以是组件*  *（硬件/软件）* | 可选择的 |  | -          定义识别和验证试图访问地面军事系统和自动驾驶仪的人员的流程/机制。  -          定义流程/机制，以  创建/修改/删除个人身份  这些活动应与OSO#02保持一致，OSO#02要求定义运营商人员的职责 | -和中号一样 |
|  |  | **实例**  -密码用于验证用户的身份  当有人试图访问  地面军事系统/自动驾驶仪 |  |
| **OCSO#2#U软件/硬件**  管理实体的授权。    关键词：授权管理    *注1：该目标侧重于定义/分配/修改/撤销实体授权的操作程序。*    *注2：实体可以是人，也可以是组件*  *（硬件/软件）* | 可选择的 |  | -          定义组织中每个人的权利，这些人可以与自动驾驶仪和地面军事系统交互。  -          定义分配/修改/撤销每个人权利的流程/机制。 | -和中号一样 |
|  |  | **实例**  每个人的授权定义如下：  -          经理  -          飞行员可以进入地面军事系统监控车辆。  -          维修人员可以在飞行前后访问自动驾驶仪并下载数据。  为了获得维护人员的权利，一个人必须向经理索取这些权利。 |  |
| **OCSO#3#U软件/硬件**  对于访问地面军事系统或自动驾驶仪的每个实体（\*），确保其只能执行授权行动。  关键词：访问控制  *注意：实体可以是人，也可以是组件*  *（硬件/软件）* | 可选择的 |  | -          定义流程/机制，以限制一个人可以作为其分配权利执行的行动。  -          这些活动应与OSO#02保持一致，OSO#02要求定义运营商人员的职责 | -          和中号一样  另外  -          定义流程/机制，将其他组件可以执行的操作限制在其权限范围内 |
|  |  | 实例  -根据用户的角色，地面军事系统可以提供特定的人机界面，让用户执行授权操作 | 实例  -自动驾驶仪的连接端口允许GPS模块仅向自动驾驶仪发送位置数据，而不发送其他类型的数据 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **OCSO#4#U软件/硬件**  检测未经授权的实体（\*）修改地面军事系统和自动驾驶仪中存储的数据/信息。  关键词：诚信    *注1：该目标是指绕过OCSO#3中定义的保护机制的情况*  *注2：实体可以是人，也可以是组件*  *（硬件/软件）* | 可选择的 | | -定义安全机制，以保护储存在地面军事系统和自动驾驶仪中的飞行计划、飞行参数（PID参数、滤波卡尔曼参数、传感器校准等）和记录数据（视频数据、日志数据）的完整性。 | -          和中号一样  另外  -          定义安全机制以保护源代码的完整性  自动驾驶仪和地面军事系统 |
|  |  | | **实例**  -自动驾驶仪和地面军事系统生成加密的散列，以保护飞行计划的完整性。 | **实例**  -自动驾驶仪可以在引导时检查软件的完整性 |
| **OCSO#5#U软件/硬件**  防止未经授权的实体（\*）访问存储在地面军事系统和自动驾驶仪中的数据/信息。  关键词：保密性    *注1：该目标是指绕过OCSO#3中定义的保护机制的情况*    *注2：实体可以是人，也可以是组件*  *（硬件/软件）* | 可选择的 | | -定义安全机制，以保护存储在地面军事系统和自动驾驶仪中的数据/信息的机密性 | -和中号一样 |
|  | | **实例**  -采用AES算法对系统进行保护  飞行计划的保密性 |  |
| **OCSO#6#U软件/硬件**  飞行后分析软件/硬件上的异常行为（飞行后检查）  关键词：异常检测 | 分析飞行后软件/硬件上的异常行为，以检测飞行后检查中的异常行为。  *注：该活动应与SORA方法的OSO#6保持一致，该方法要求定义飞行后检查程序。* | | -同低 | -同低 |
| 实例  -          飞行结束后，飞行员应对飞行过程中记录的飞行数据和飞行指令进行分析。  -          为支持上述活动，自动驾驶仪和地面军事系统应记录飞行期间的数据和事件。 | |  |  |
| **OCSO#7#U软件/硬件**  将软件/硬件体系结构划分为具有不同临界级别的不同“区域”。    关键词：硬件/软件  **隔断** | 可选择的 |  | -将软件/硬件体系结构划分为具有不同临界级别的不同“区域”。一些硬件/软件可能比其他硬件/软件更容易受到网络攻击，但它们提供的功能不如其他硬件/软件那么重要。 | -和中号一样 |
|  | . | **实例**  -地面军事系统包括2台带有两种不同软件的电脑。一台PC用于控制和观察飞机。这台电脑对UAS至关重要。另一个用于控制有效载荷。此功能不太重要。 |  |

**B.与通信攻击相关的OCSO：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **描述** | **诚实正直** |  | **水平** |  |
| **低的** |  | **中等的** | **高的** |
| **OCSO#8 u通信**  防止非授权实体（\*）访问地面军事系统和飞机之间通信中的数据/信息  关键词：保密性    *注意：实体可以是人，也可以是组件*  *（硬件/软件）* | -定义确保通过通信设备传输的每个数据的机密性的机制。 | -同低 |  | -         同低  另外  -         定义确保地面军事系统软件和自动驾驶仪软件之间传输的每条信息保密的机制。（应用程序级别） |
| **实例**  -在一个简单的情况下，地面军事系统和自动驾驶仪通过一对无线电模块进行通信。该模块提供的加密算法和跳频机制保护了数据的机密性。 |  |  | **实例**  -地面军事系统软件和自动驾驶仪软件有各自的机制来保护它们之间传输的信息的机密性。 |
| **OCSO#9\_u通信** | -定义确保每个数据包/消息完整性的机制 | 同低 |  | -同低 |

|  |  |  |  |
| --- | --- | --- | --- |
| **描述** | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| 防止非授权实体修改地面军事系统和飞机之间通信中的数据/信息  关键词：诚信    *注意：这是为了确保数据在内容、时间（防止重播攻击）和来源方面没有被修改。* | 通过通信设备传输。 |  | 另外  -定义确保GCS软件和自动驾驶仪软件之间传输的每条信息完整性的机制。（应用程序之间的通信） |
| **实例**  -在一个简单的情况下，地面军事系统和自动驾驶仪通过一对无线电模块进行通信。基于此模块提供的加密算法保护数据的完整性。 |  | **实例**  -地面军事系统软件和自动驾驶仪软件有各自的机制来保护它们之间传输的信息的机密性。 |
| **OCSO#10 u通信**  **检测异常**在操作期间，地面军事系统与飞机之间的通信信道中  关键词：异常检测 | -          定义用于测量通信信道性能的参数。  -          地面军事系统显示定义的参数  -          建立安全指令，飞行员可以通过观察通信信道来检测通信信道性能的下降  "地位。  在低水平上，异常仅指通信性能的下降。  这些活动应与OSO#6保持一致，OSO#6要求操作员识别通信特征 | -同低 | -          同低  另外  -          定义在通信信道中自动检测异常的机制  在这个级别上，异常指的是通信性能的下降以及通过通信信道传输的消息/分组的内容。 |
| **实例**  用于评估通信质量的参数是信号强度、丢包率和比特率。这些参数将显示给飞行员。 |  | **实例**  **-** 如果UAS的通信基于用于其他应用程序、操作或系统的复杂网络，则使用防火墙 |
| **OCSO#11 u通信**  保持最低限度  通信性能    关键词：可用性 | -一种计划或程序，允许  用户，飞行员，在发现通信性能下降的情况下，重新建立通信或维持若干基本服务。 | -定义在通信性能下降的情况下重新建立通信或维护几个基本服务的机制。 | -和中号一样 |
| **实例**  -如果通信性能下降，飞行员应改变通信频率。 | **实例**  -如果通信性能下降，通信模块应发送重要信息/消息/数据包（如位置、姿态）  信息和飞行员命令信息）优先。 |  |
| **描述** | **诚实正直** | **水平** |  |
| **低的** | **中等的** | **高的** |
| **OCSO#12 u通信**  飞行后分析通信通道中的异常情况（飞行后检查）    关键词：异常检测 | -          定义用于在每次飞行后诊断通信信道性能的参数。这些参数将记录在自动驾驶仪和地面军事系统上。  -          制定安全说明，飞行员或维修人员可通过检查日志来检测异常情况。 | -同低 | -同低 |
|  | **实例**  -          自动驾驶仪和地面军事系统记录参数：包丢失百分比、信号强度、延迟时间。  -          地面军事系统提供一个接口，允许飞行员/工作人员分析记录的数据。 |  |  |
| **OCSO#13 u通信**  将通信系统划分为不同的信道。    关键词：通信分区 | 可选择的 | 根据传输数据的关键性级别和脆弱性级别，将通信系统划分为不同的信道。 | 和中号一样 |
|  | **实例**  -通信系统分为两个通道。一个用于传输飞行数据，这是至关重要的。另一个用于传输不太重要的视频数据。 |  |

**C.与传感器攻击相关的OCSO**

|  |  |  |  |
| --- | --- | --- | --- |
| **描述** | **诚信水平** | |  |
|  | **低的** | **中等的** | **高的** |
| **OCSO#14#U传感器**  检测由于攻击而导致的传感器异常行为  关键词：异常检测 | -定义传感器的特性（关于输出值、采样频率、噪声）及其可接受阈值。超过这些阈值被视为异常行为。 | -          和中号一样  另外  -          通过分析来自不同传感器的数据之间的一致性和一致性，定义检测异常传感器数据的机制。 | 和中号一样 |
| **实例**  -加速度计数据的可接受阈值，如+-3m/s2。超出此范围的数据可视为可能的攻击。 | **实例**  -将来自GPS的位置数据与来自IMU和立体相机的数据进行比较，以检测GPS欺骗 |  |
| **OCSO#15#U传感器**  确保受到攻击的传感器数据的可用性。    关键词：可用性 | -定义保护传感器免受环境干扰的解决方案（攻击者可以通过在谐振频率下使用干扰来操纵加速计传感器的输出） | -            同低  另外  -            定义提供传感器数据冗余的机制或体系结构 | 和中号一样 |
|  | **实例**  -加速计（IMU）装在一个金属盒内，以防止共振频率下的干扰 | **实例**  **-** 在GPS不可靠的情况下，来自摄像机的数据可以交替提供位置数据 |  |

 .

附录B

网络工具手册



B.1一般信息页

这是我们申请的第一步。在此步骤中，将提示用户提供有关预期UAS操作的某些类型的一般信息。提供的信息不用于风险评估，但有助于我们改进应用程序。一般资料包括：



•申请人（或用户）姓名

•电子邮件

•组织类型。有三种选择，如下所示：

–制造商，如果用户是制造商的成员。

–操作员，如果用户是操作员的成员管理员，如果用户是管理员。

121

•无人机操作目的：无人机的部署目的是什么？例如：观察一条公路，运输良好。

•本风险评估的目的。有两种选择，如下所示：

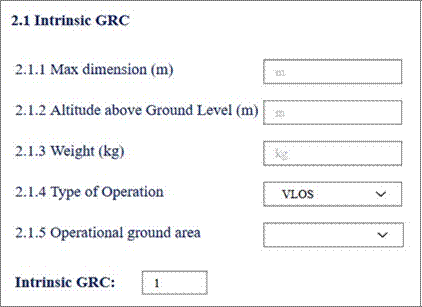
–验证现有UAS操作。在这种情况下，我们假设拟定的操作已制定并得到充分记录。如果该操作涵盖了风险评估产生的所有安全和安保目标，则认为该操作有效。

–开发新的无人机操作。在这种情况下，在风险评估开始时，我们只有一些关于预期操作的基本信息（例如，目的、海拔、位置）。然后，风险评估（目标）的结果将用于完善和完成操作说明。

要开始风险评估过程，请单击“创建新评估”按钮。

B.2地面风险等级（GRC）的确定

我们应用的这一步骤对应于SORA方法的两个步骤：内在GRC测定和最终GRC测定。



图B.2：计算固有GRC的信息

为了确定预期操作的固有GRC，系统会提示用户提供以下信息：

B.2。地面风险等级（GRC）的确定

•飞机的最大尺寸（单位：米）。

•运行期间飞机地面以上的高度（单位：米）。

•飞机重量（单位：kg）。

•操作类型。此信息有两个选项：

–VLOS或可视视线，如果飞机在飞行员的可视范围内运行。

–BVLOS或视野之外，如果飞机在驾驶员视野之外运行。

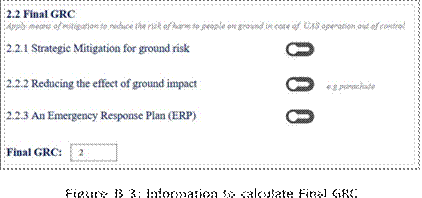
•操作地面区域。此信息有四个选项：

–控制地面区域，前提是只有直接参与操作区域内操作的积极参与者。

–人口稀少的环境

–居住环境

–如果飞机飞越人群，聚集人员。



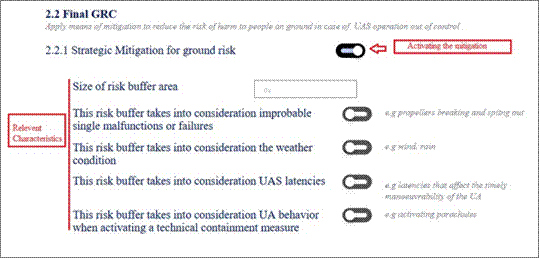
为确定预期运行的最终GRC，提示用户提供有关在“UAS运行失控”情况下减轻地面致命伤害可能性的措施的信息。有三种可能的缓解措施：

•地面风险的战略缓解。这有助于降低在UAS运行失控时，人员进入危险区域的可能性。

•减少地面撞击的影响。这有助于降低在地面人员不幸被飞机（如降落伞）击中时发生致命伤害的可能性。

•应急响应计划。针对紧急事件以特定顺序或方式实施的行动计划。

如果在预期操作中提到或考虑了缓解措施，用户可以通过单击/切换相应按钮来激活呈现的缓解措施。一旦激活缓解措施，将显示该缓解措施的相关特征。然后，用户可以选择激活预期操作中提到或考虑的特性。基于激活特征，应用程序可以估计缓解的鲁棒性。



图B.4：战略缓解的相关特征

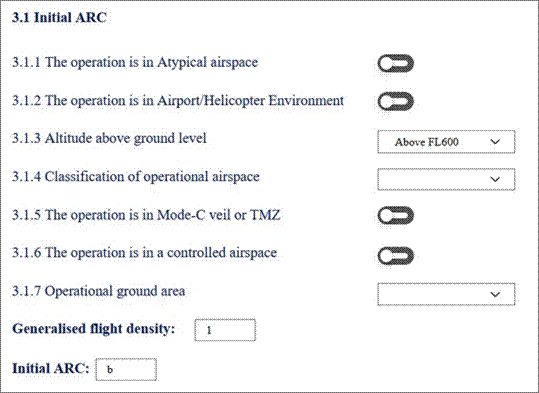
对于每个激活的特性，用户可以提供更多关于在预期操作中如何提及或考虑相关特性的信息。该信息将用于生成最终报告，但不用于风险评估。

根据固有GRC和适用缓解措施的信息，在页面底部计算最终GRC。

B.3空气风险等级（ARC）的确定

我们应用的这一步对应于SORA方法的两个步骤：初始电弧确定和最终电弧确定。初始ARC提供了无人机在特定空域环境中遭遇载人飞机的速率的广义定性分类。假设申请人认为分配的广义初始弧对于局部操作体积条件来说过高。在这种情况下，可以考虑采取缓解措施来降低初始电弧值。如果初始圆弧不正确，则最终圆弧等于初始圆弧。

B.3。空气风险等级（ARC）的确定



图B.5：计算初始弧的信息

为了确定预期操作的初始弧，根据预期操作的描述，用户将回答以下问题：

•飞机是否在非典型空域内飞行？非典型空域的定义如下：

–受限空域或危险区域；

–正常载人飞机无法飞行的空域（例如，建筑物或构筑物100英尺范围内的空域）；

–在运行期间，载人飞机的遭遇率低于每飞行小时1E-6的空域特征；

•飞机是否在机场/直升机环境中飞行？

•飞机在地面以上的哪个高度运行？有三个可用选项：

-高于FL600水平面（地面以上18000米）

–海拔500英尺（周围150米）及600英尺以上

–500英尺以下

•飞机在哪个空域级别运行？有三种选择：

–A级或E级

–B、C或D类

–F级或G级

这些等级由国家航空管理局根据飞行规则和飞机与空中交通管制（ATC）之间的相互作用进行定义。它们可能因国家当局而异。

•飞机是否在模式C或TMZ下运行？

•飞机是否在受控空域运行？

应用程序可以根据提供的信息计算相关空域的初始弧和相应的“广义飞行密度”水平。



为了减少初始电弧，可以考虑两种缓解措施。他们是：

•通过操作限制缓解

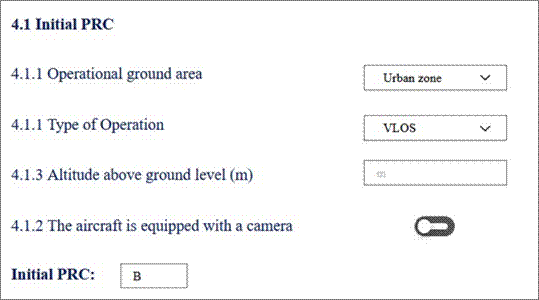
•通过共同结构和规则进行缓解

根据初始ARC和应用缓解措施的信息，在页面底部计算最终ARC。

B.4。隐私风险等级（PRC）确定

B.4隐私风险等级（PRC）的确定

我们的应用程序的这一步骤与我们的SORA方法的扩展版本有关，其中考虑了隐私侵犯风险。



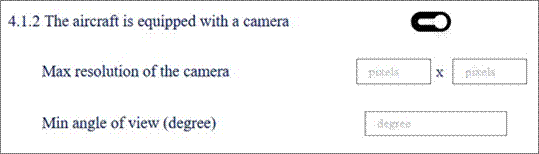
图B.7：计算初始PRC的信息

首先，要求用户提供以下信息以计算操作的初始PRC值：

•操作地面区域：城市区域与农村区域。

•操作类型：VLOS与BVLOS

•飞机是否配备了摄像头？如果是，请切换此选项的按钮，并提供有关分辨率和最小视角的更多信息。



图B.8：摄像机特性

然后提示用户提供有关在“UAS操作失控”情况下降低隐私侵犯可能性的措施的信息。在此，我们提出三种缓解措施：

•隐私保护过滤器。

•私人空间限制

•向公众发布运营意识公告

对于每个选择的缓解措施，用户可以提供更多关于如何在预期操作中提及或考虑缓解措施的信息。该信息仅用于生成最终报告，而不用于风险评估。

根据固有PRC和适用缓解措施的信息，在页面底部计算最终PRC。

B.5运营网络安全敏感等级（OCSL）的确定

我们应用程序的这一步骤与我们的扩展SORA方法有关，其中考虑了网络安全威胁。

在此步骤中，将提示用户提供有关预期操作的某些特征的信息，这有助于评估预期操作的漏洞。他们是：

•通信链路的性质。有三种选择：

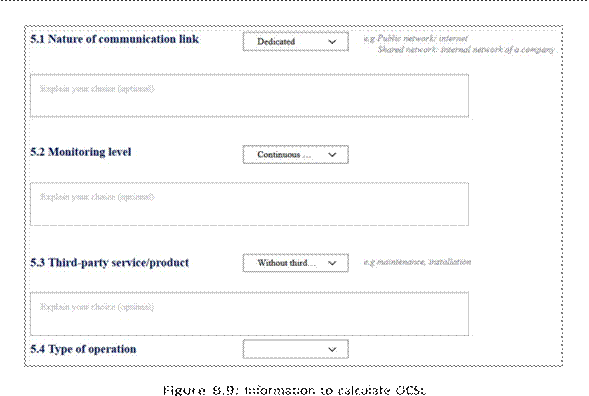
–专用通信链路：地面控制站通过仅用于UAS操作的通信链路与飞机通信（例如，RF模块）

–共享网络：地面控制站通过运营商组织的内部网络与飞机通信。除了UAS操作之外，该网络还可以服务于该组织的其他活动。

–公共网络：地面控制站通过与外部组织或个人共享的网络与飞机通信。（例如互联网连接、云服务）。

•监测水平。有三种选择：

B.5。运营网络安全敏感等级（OCSL）的确定



–持续监控：地面控制站和飞机在运行期间频繁通信。数据以实时或几乎实时的方式传输。

–没有持续监控。地面控制站和飞机在运行期间定期通信。数据不是实时或几乎实时传输的。

•系统是否使用第三方提供的服务？（例如，维护服务、安装服务）：

–没有第三方：如果没有使用第三方服务/设备。

–受信任的第三方：如果UAS操作仅使用受信任的第三方服务/设备。

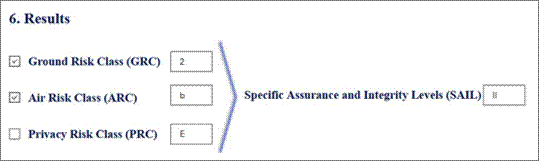
–不受信任的第三方：如果UAS操作使用了不受信任的第三方服务/设备。

•操作类型：VLOS与BVLOS。

根据提供的信息，在页面底部计算OCSL。

B.6结果

本页将显示预期操作的风险评估结果。



图B.10：基于GRC和ARC值计算的帆

首先，计算与所提供的信息相对应的SAIL值。在经典SORA方法中，SAIL值是GRC值和ARC值的组合。同时，在我们扩展的SORA方法中，根据GRC、ARC和PRC值计算SAIL值。要选择用于计算SAIL值的参数，用户可以单击参数左侧的复选框。

显示了基于SAIL级别确定鲁棒性级别的不同OSO和OCSO。要详细查看目标，请单击fletch按钮。

附录C

风险管理结果



C.1故障

在本文档中，我介绍了我的24项安全要求，这些要求可用于确保UAS操作的安全。这些要求用于处理或减轻以下系统故障的影响。

1.    无人机坠毁：由于恶意行为，无人机失去姿态并坠毁。由于飞越高速公路，无人机的现金可能导致致命事故。（失去可用性）

2.    偏离轨迹：在攻击下，无人机偏离其轨迹并按照攻击者定义的轨迹飞行。（诚信缺失）

3.    航班信息不可用：在攻击下，操作员无法访问航班信息。（失去可用性）。

4.    假飞行信息：在攻击下，假飞行信息被提供给操作员，使他们做出错误的决定。（诚信缺失）

5.    航班信息披露：在攻击下，攻击者可能获得对航班信息的未经授权访问，这可能有助于攻击者发起其他攻击。（失去保密性）

6.    假视频：在攻击下，操作员收到攻击者制作的假观察视频。该故障不会直接影响操作的安全性，但会使操作目标完全失效。（诚信缺失）

7.    视频不可用：在攻击下，操作员无法访问观察视频。（失去可用性）

8.    视频披露：在攻击下，攻击者可能未经授权访问观察视频，从而影响被观察者的隐私。（失去保密性）

131

C.2网络安全要求

C.2.1安全要求1

（自动防故障）

目标：如果GPS模块不可用，自动驾驶仪需要检测此问题，并根据可用传感器的数据使车辆着陆。相关故障：1

C.2.2安全要求2

目标：自动驾驶仪需要验证GPS模块提供的位置数据的完整性。如果检测到不正确的数据，自动驾驶仪需要向操作员报告并使车辆着陆。

相关故障：1、2

C.2.3安全要求3

（故障模式）

目标：如果IMU模块不可用，自动驾驶仪需要检测故障并终止飞行

相关故障：1

C.2.4安全要求4

目标：每当从IMU模块接收原始加速度和角速度数据时，自动驾驶仪需要验证该数据的完整性。当检测到不正确的数据时，自动驾驶仪需要终止与飞行相关的故障：1、2

C.2.5安全要求5

目标：自动驾驶仪需要验证导航数据的完整性。需要检测伪造的数据。

C.2。网络安全要求

相关故障：1、2

C.2.6安全要求6

目标：在操作开始时，自动驾驶仪需要确认飞行计划、飞行控制参数、导航参数没有被未经授权的人员修改。相关故障：1、2

C.2.7安全要求7

对象：自动驾驶仪需要验证固件是否未根据内容和来源进行修改。

相关故障：1、2、3、4、5、7

C.2.8安全要求8

目标：自动驾驶仪需要访问控制机制，该机制只允许授权方访问自动驾驶仪，并将操作作为其属性权利实施（例如，只有制造商可以修改固件，操作员可以启动/停止任务等）。每个参与方的角色需要详细定义。相关故障：1、2、3、4、5、7

C.2.9安全要求9

（自动防故障）

目标：如果气压计模块不可用，应根据其他可用传感器的数据估计车辆的高度，以使车辆着陆。相关故障：1

C.2.10安全要求10

目标：每当从气压计模块接收气压数据时，自动驾驶仪应验证该数据的完整性。当检测到不正确的数据时，自动驾驶仪应使车辆着陆。

相关故障：1,2

C.2.11安全要求11

（自动防故障）

目标：如果罗盘模块不可用，自动驾驶仪需要检测此问题，并根据来自可用传感器的数据使车辆着陆。相关故障：1

C.2.12安全要求12

目标：每当接收到来自罗盘模块的磁场数据时，自动驾驶仪需要验证该数据的完整性。当检测到不正确的数据时，自动驾驶仪应使车辆着陆。

相关故障：1,2

C.2.13安全要求13

目标：每当从非易失性存储器读取有关罗盘校准的数据时，自动驾驶仪需要验证数据的完整性。相关故障：1

C.2.14安全要求14

（安全C2链路）

目的：为了保护自动驾驶仪和地面军事系统之间的通信，需要实施安全协议。本议定书确保：

1.    交换数据的完整性。每当接收到来自RF模块的数据时，自动驾驶仪和地面军事系统都可以验证数据包在内容、时间（顺序）、原始来源（身份验证）方面没有被修改。

2.    交换数据的保密性。只有授权设备（自动驾驶仪、地面军事系统）才能解释交换数据中的信息。

C.2。网络安全要求

3.    交换数据的可用性。自动驾驶仪和地面军事系统都有自己控制通信质量的机制。他们需要验证每条消息是否到达目的地。如果通信链路不可用，则会触发故障安全过程，自动驾驶仪将着陆车辆。

相关故障：1,2,3,4,5,7

C.2.15安全要求15

目标：每当收到地面军事系统的命令时，自动驾驶仪需要确认该命令不会对操作安全产生任何影响（例如，在飞行过程中更改飞行参数、飞行计划等）。如果这是一个危险命令，自动驾驶仪需要重新验证操作员的身份，并在执行前提示操作员验证该命令。相关故障：1,2

C.2.16安全要求16

目标：地面军事系统应仅允许授权方访问。地面军事系统需要验证其身份（身份验证）和访问控制机制（访问控制）。每个参与方的角色需要详细定义。相关故障：1,2,5,8

C.2.17安全要求17

目标：地面军事系统需要确认存储在地面军事系统计算机中的地图和飞行计划没有被恶意修改。需要向操作员报告这些数据的完整性违规情况。相关故障：4

C.2.18安全要求18

目标：需要控制自动驾驶仪与外部环境之间通过连接端口的数据流。不同类型的数据需要通过不同的端口发送或接收。这一要求可以通过软件和硬件设计来实现。相关故障：1、2、3、5、7

C.2.19安全要求19

目标：当摄像头不可用时，3G/4G模块需要向地面军事系统发送警报信息。

相关故障：7

C.2.20安全要求20

目标：当视频数据不可用时，地面军事系统需要向操作员显示警报信息。

相关故障：7

C.2.21安全要求21

对象：万向节仅允许授权人员访问和修改其固件。应实施访问控制机制。相关故障：6、7

C.2.22安全要求22

目标：框架的参数需要在完整性方面得到保护。在操作开始时，万向节需要验证这些参数是否由授权人员创建且未被修改。相关故障：7

C.2.23安全要求23

（用于视频传输的安全协议）

目标将视频数据传输至地面军事系统时，需要实施安全通信协议。本议定书需要确保：

1.    交换数据的完整性。无论何时从互联网接收视频数据，地面军事系统都可以验证数据是否已根据内容、时间（顺序）、原始来源（身份验证）进行了修改。

C.3。风险水平

2.    交换数据的保密性。只有经授权的地面军事系统才能解释数据中的信息。

3.    exchange数据的可用性。地面军事系统需要测量链路质量并向运营商报告。

相关故障：6、7、8

C.2.24安全要求24

对象需要控制Internet和地面军事系统之间的数据流。只有制造商定义的数据类型才能从互联网到达地面军事系统，或由地面军事系统发送到互联网。

相关故障：6、7、8

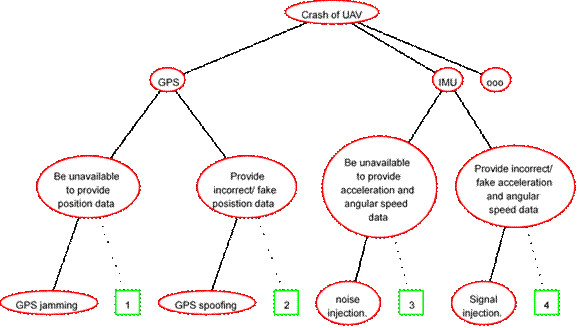
C.3风险水平

（见下一页）

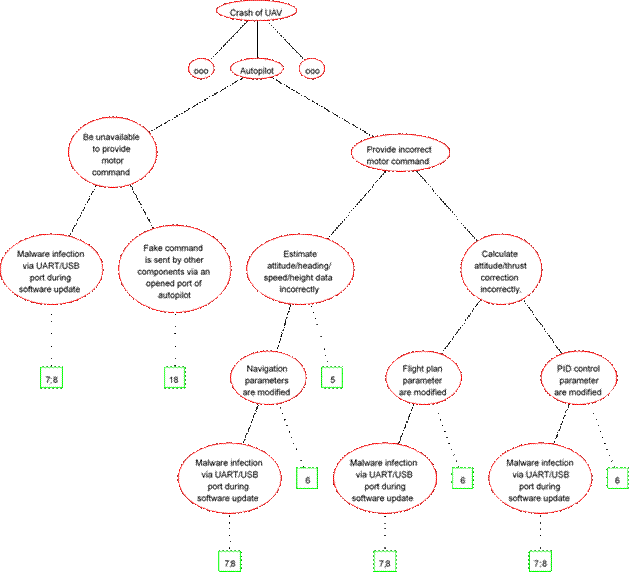
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 脚本 | 准备 | 机会 | 处决 | 全部的 | DOA | 严重程度 | 数量 | 目标组件 | 要求 |
| 1\u可用性\u 1 | 2 | 1 | 4 | 7基本的 | | 高高 | | 全球定位系统 | 1 |
| 1\u可用性\u 2 | 2 | 1 | 8 | 11基本的 | | 高高 | | 全球定位系统 | 2 |
| 1\_可用性\_3 | 6 | 1 | 12 | 19高 | | 高中 | | 伊姆 | 3 |
| 1\u可用性\u 4 | 6 | 1 | 12 | 19高 | | 高中 | | 伊姆 | 4 |
| 1\u可用性\u 5 | 6 | 8 | 10 | 24高 | | 高中 | | 自动驾驶仪 | 7,8 |
| 1\u可用性\u 6 | 6 | 6 | 10 | 22高 | | 高中 | | 自动驾驶仪 | 18 |
| 1\u可用性\u 7 | 6 | 8 | 10 | 24高 | | 高中 | | 自动驾驶仪 | 7,8,6,5 |
| 1\u可用性\u 8 | 6 | 8 | 10 | 24高 | | 高中 | | 自动驾驶仪 | 7,8,6 |
| 1\u可用性\u 9 | 6 | 8 | 10 | 24高 | | 高中 | | 自动驾驶仪 | 7,8,6 |
| 1\u可用性\u 10 | 2 | 1 | 12 | 15中等 | | 高中 | | 气压计 | 9 |
| 1\u可用性\u 11 | 2 | 1 | 12 | 15中等 | | 高中 | | 气压计 | 10 |
| 1\u可用性\u 12 | 6 | 1 | 12 | 19高 | | 高中 | | 罗盘 | 11 |
| 1\u可用性\u 13 | 6 | 1 | 12 | 19高 | | 高中 | | 罗盘 | 12 |
| 1\_可用性\_14 | 6 | 2 | 6 | 14中等 | | 高中 | | 非易失性存储器 | 13 |
| 1\u可用性\u 15 | 5 | 1 | 6 | 12基本的 | | 高高 | | 射频 | 14,15 |
| 1\u可用性\u 16 | 5 | 1 | 6 | 12基本的 | | 高高 | | 射频 | 14,15 |
| 1\_可用性\_17 | 6 | 3 | 2 | 11基本的 | | 高高 | | 地面军事系统 | 14,15,16,24 |
| 1\_完整性\_1 | 2 | 1 | 8 | 11基本的 | | 甚高 | | 全球定位系统 | 2 |
| 1\_完整性\_2 | 6 | 8 | 10 | 24高 | | 甚高至中等 | | 自动驾驶仪 | 5,6,7,8 |
| 1\_完整性\_3 | 6 | 8 | 10 | 24高 | | 甚高至中等 | | 自动驾驶仪 | 6,7,8 |
| 1\_完整性\_4 | 6 | 1 | 12 | 19高 | | 甚高至中等 | | 伊姆 | 4 |
| 1\_完整性\_5 | 5 | 1 | 6 | 12基本的 | | 甚高 | | 射频 | 15,14 |
| 1\_完整性\_6 | 5 | 1 | 6 | 12基本的 | | 甚高 | | 射频 | 14,15 |
| 1\_完整性\_7 | 6 | 1 | 12 | 19高 | | 甚高至中等 | | 罗盘 | 12 |
| 1\_完整性\_8 | 6 | 1 | 12 | 19高 | | 甚高至中等 | | 气压计 | 10 |
| 2\_完整性\_1 | 2 | 1 | 6 | 9基本的 | | 中号 | | 射频 | 14 |
| 2\_完整性\_2 | 2 | 1 | 6 | 9基本的 | | 中号 | | 射频 | 14 |
| 2\_完整性\_3 | 6 | 6 | 10 | 22高 | | 中低 | | 地面军事系统 | 17 |
| 2\_完整性\_4 | 6 | 6 | 10 | 22高 | | 中低 | | 地面军事系统 | 24 |
| 2\_完整性\_5 | 6 | 6 | 10 | 22高 | | 中低 | | 自动驾驶仪 | 7,8 |
| 2\u保密性\u 1 | 5 | 1 | 6 | 12基本的 | | 中号 | | 射频 | 14 |
| 2\_保密性2 | 6 | 6 | 10 | 22高 | | 中低 | | 自动驾驶仪 | 7,8,18 |
| 2\u保密性\u 3 | 6 | 6 | 10 | 22高 | | 中低 | | 自动驾驶仪 | 7,8,18 |
| 2\u保密性\u 4 | 6 | 3 | 2 | 11基本的 | | 中号 | | 地面军事系统 | 16,24 |
| 3\u可用性\u 1 | 6 | 6 | 10 | 22高 | | 低低 | | 地面军事系统 | 24 |
| 3\u可用性\u 2 | 6 | 6 | 10 | 22高 | | 低低 | | 地面军事系统 | 16,24 |
| 3\u可用性\u 3 | 6 | 3 | 2 | 11基本的 | | 低低 | | 地面军事系统 | 16,24 |
| 3\u可用性\u 4 | 6 | 6 | 10 | 22高 | | 低低 | | 自动驾驶仪 | 7,8 |
| 3\u可用性\u 5 | 4 | 1 | 6 | 11基本的 | | 低低 | | 3G/4G模块 | 23 |
| 3\u可用性\u 6 | 6 | 8 | 12 | 26非常高 | | 低低 | | 3G/4G模块 | 23 |
| 3\u可用性\u 7 | 6 | 6 | 10 | 22高 | | 低低 | | 万向节 | 21,22 |
| 3\u保密性\u 1 | 6 | 1 | 12 | 19高 | | 高中 | | 3G/4G模块 | 23 |
| 3\u保密性\u 2 | 6 | 1 | 10 | 17中等 | | 高中 | | 3G/4G模块 | 23 |
| 3\_保密性\_3 | 6 | 1 | 10 | 17中等 | | 高中 | | 地面军事系统 | 24 |
| 3\u保密性\u 4 | 6 | 3 | 2 | 11基本的 | | 高高 | | 地面军事系统 | 16 |
| 3\_完整性\_1 | 6 | 6 | 10 | 22高 | | 高中 | | 地面军事系统 | 24 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3\u完整性\u 2 | 6 | 1 | 12 | 19高 | 高的 | 中等的 | 3G/4G模块 | 23 |
| 3\_完整性\_3 | 6 | 1 | 12 | 19高 | 高的 | 中等的 | 3G/4G模块 | 23 |
| 3\_完整性\_4 | 6 | 1 | 12 | 19高 | 高的 | 中等的 | 3G/4G模块 | 23 |

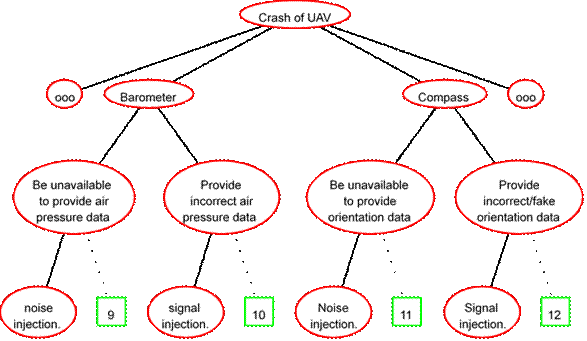
C.4攻击树



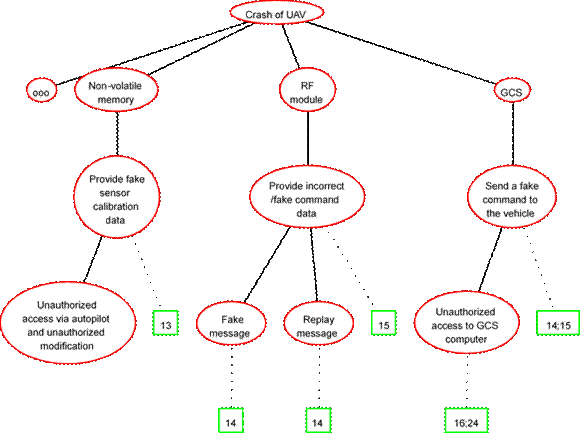
图C.1：1-可用性故障的攻击树-第1部分



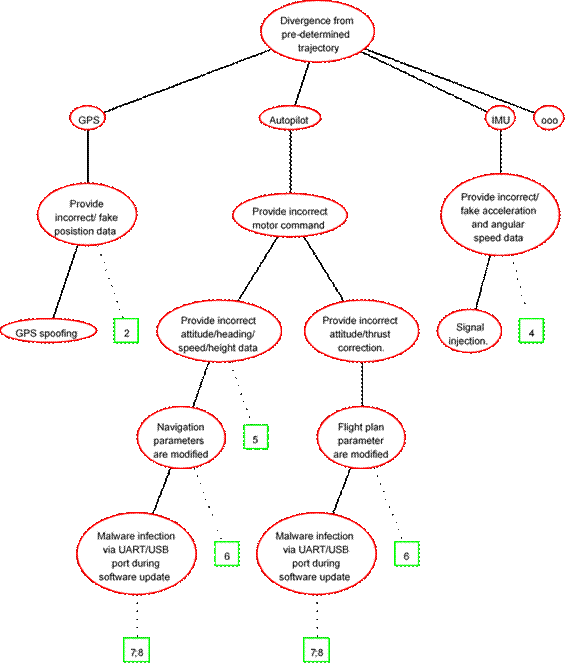
图C.2：1-可用性故障的攻击树-第2部分



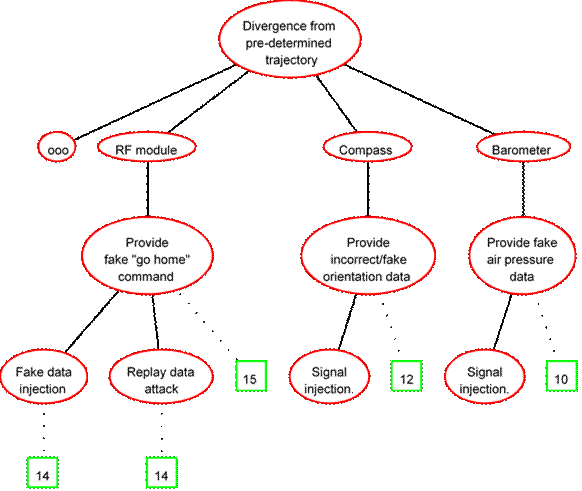
图C.3：1-可用性故障的攻击树-第3部分



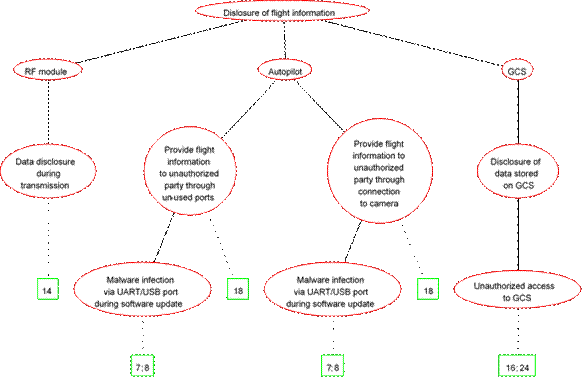
图C.4：1-可用性故障的攻击树-第4部分



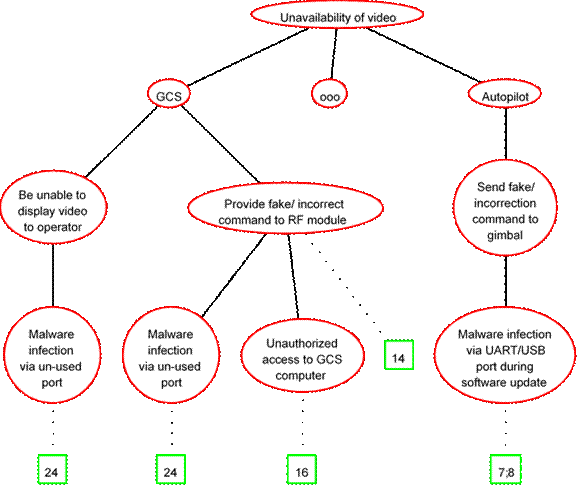
图C.5：1-完整性故障的攻击树-第1部分



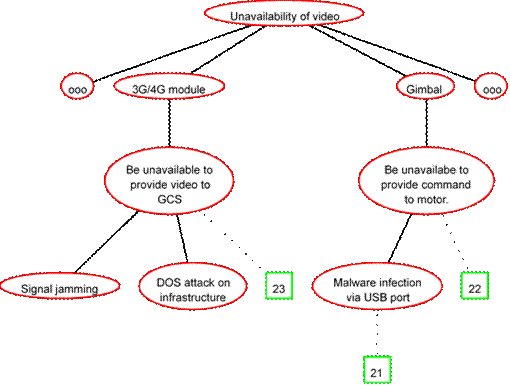
图C.6：1-完整性故障的攻击树-第2部分



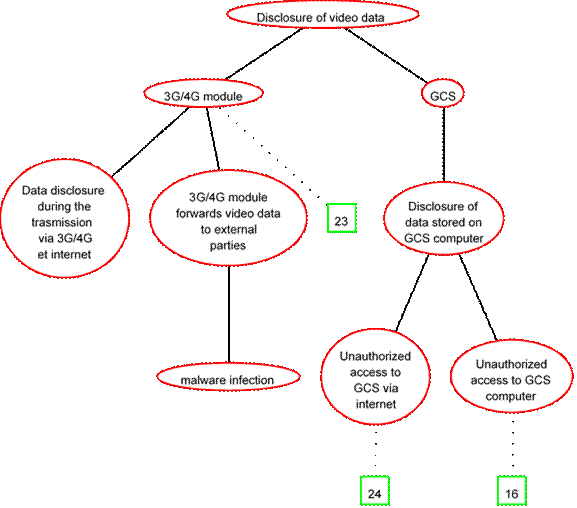
图C.7：2-1故障的攻击树



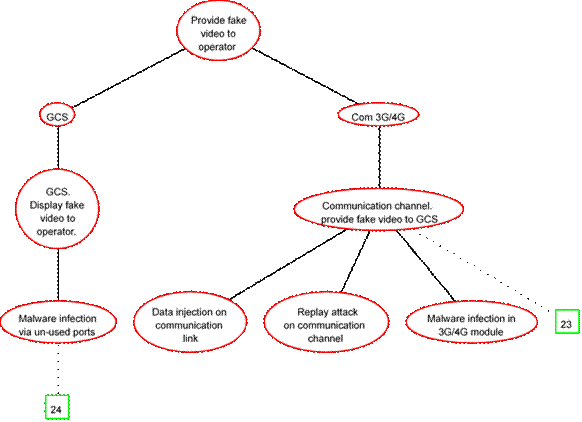
图C.8：2-机密性故障的攻击树-第1部分



图C.9：2-机密性故障的攻击树-第2部分



图C.10：3-1故障的攻击树



图C.11:3-integrity故障的攻击树

附录D

GPS欺骗及其对策



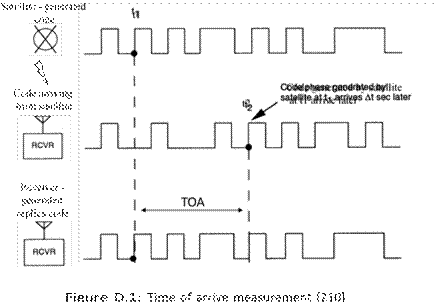
151

附录D.GPS欺骗和对策



D.1全球定位系统基础

全球定位系统（GPS）是一种全球导航卫星系统（GNSS），自1973年以来由美国陆军开发和维护[209]。GPS卫星提供了参考点，地球上的GPS接收器可以据此估计其位置。位置估计基于对卫星发射信号的观测。每个GPS卫星在两个载波频率L1=1575.42 MHz和L2=1227.6 MHz上同时广播信号。信号采用两种伪随机噪声（PRN）编码进行调制：C/A（粗/捕获）和P（精确）。C/A代码用于民用应用，每个卫星都是唯一的，而P代码是加密的，用于军事应用。



由于这些卫星以稳定的速度在精确的轨道上飞行，它们的位置可以用数学方法估计。理想情况下，为了确定接收器在地球上的位置，我们需要知道从这一点到至少三颗卫星的距离。GPS接收机和GPS卫星之间的距离是通过观测卫星信号的到达时间（TOA）获得的。如上所述，GPS卫星连续生成并发送用PRN码调制的信号。同时，在地球上，GPS接收机还产生用PRN码调制的信号。当从卫星接收信号时，接收器将接收到的代码与自身生成的代码进行比较，以确定TOA（见图D.1）。然后，通过将TOA乘以无线电传播速度来计算卫星接收机距离。然而，实际上，所提出的计算并没有给出从卫星到接收器的实际距离，而只是给出伪距离。原因是接收机时钟通常与卫星的时钟不严格同步。这会导致TOA估计和距离估计的偏差。接收机位置和伪距之间的关系如方程式D.1所示。在这个方程中，我们有四个未知变量（三个坐标和一个时钟偏差）。因此

D.1。全球定位系统基础153



为了确定接收机位置，需要知道四颗卫星的伪距，而不是三颗卫星的伪距。



*ρ* = P2 (xs)− xr）2+（ys− yr）2+（（zs− zr）2）+c∗ δt（D.1）

哪里：

*ρ* 是从卫星到接收器的伪距

（xs，ys，zs）是卫星的位置（xr，yr，zr）是接收机的位置是无线电传播速度是接收机时钟偏差*Cδt*

D.1.1欺骗攻击策略

由于民用GPS信号不受保护，GPS欺骗攻击的原理是用假GPS信号欺骗GPS接收。生成伪GPS信号的策略可以遵循以下方法之一：GPS信号发生器、基于中间接收器的欺骗和基于复杂接收器的欺骗[211]。

•GPS信号发生器是攻击者使用GPS模拟器生成虚假GPS信号的最直接方法。这种技术产生的信号通常与真实的GPS信号不同步。因此，伪信号可以通过不同的反欺骗技术进行检测，如振幅监测、不同测量之间的一致性检查[212]

•基于接收器的欺骗是一种更先进的方法，其中欺骗由GPS接收器和信号发射器组成。spoofer首先与真实的GPS信号同步，并提取导航信息。然后，欺骗者将提取的信息生成假信号发送给目标接收器。这种攻击很难检测，比第一类攻击更复杂。这种方法的主要挑战是以正确的信号延迟和强度将欺骗信号投射到目标接收器[212]。

•复杂的基于接收器的欺骗复杂的基于接收器的欺骗是最复杂和有效的技术。它的目标是在接收端产生与真实信号相似的伪信号，包括载波相位、信号功率、噪声。为此，spoofer必须能够精确跟踪接收器的位置和移动。与以前的攻击相比，这种攻击更为复杂，实现起来更具挑战性，但检测起来也更为困难

[212].

附录D.GPS欺骗和对策



D.2对抗技术的现状

文献中有许多工作提出了应对GPS欺骗攻击的不同对策。本节回顾了以GPS欺骗检测为重点的欺骗对策。主要有三种方法：（1）信号处理，（2）空间处理，（3）数据处理。

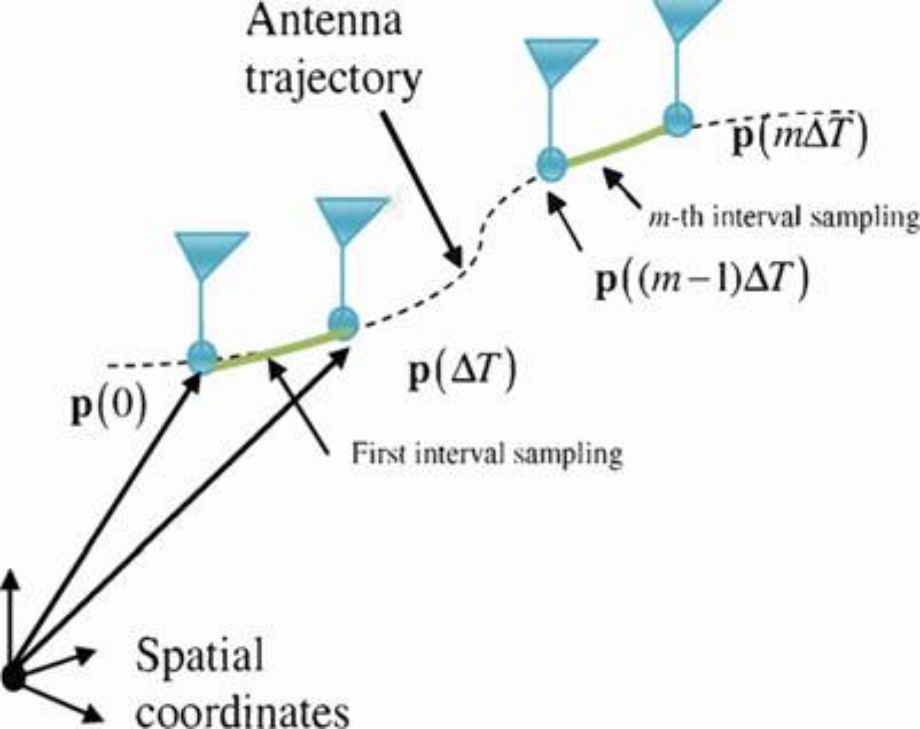
1.    信号处理：GPS欺骗的原理是用假信号欺骗GPS接收器。因此，检测联合国攻击的一种方法是信号监测。信号特性（如载波幅度、载波相位、信号强度、信号功率）突然出现不合理的跳跃可能会导致攻击[213]。Wen等人提出监测信噪比（SNR）指标[214]。所提出的技术将接收信号的信噪比水平与预定义的阈值进行比较，以鉴别假信号。Shepard[215]提出了另一种基于信号功率监测的技术。由于欺骗者和目标接收器之间的距离，很难用适当的功率电平调整假信号，该功率电平足以欺骗接收器，但低于真实信号的通常强度电平。Jovanovic等人[216]提出了一种算法来监控许多信号特征的统计特性并检查不一致性，而不是监控单一特征。

2.    空间处理：正常情况下，GPS接收机将接收不同卫星发送的信号。因此，信号将从不同方向到达接收器。在攻击的情况下，攻击者可以生成不同卫星信号的多个伪版本，并使用单个天线进行传输。这导致了伪信号的空间相关性。这一论点是基于空间特征的几种GPS欺骗检测解决方案的原理。McDowell[217]和Montgomery等人[218]部署了一个多天线接收器，通过监测不同天线单元之间的相位差来检测欺骗信号。Nielsen等人[219]使用带有单天线的移动接收机代替多天线接收机，形成合成天线阵列结构，如图D.2所示。

3.    数据处理：GPS欺骗的主要目的是使GPS接收器提供错误的位置数据。因此，我们自然会想到，我们可以查找接收器输出数据的异常情况，以检测GPS欺骗攻击。大多数GPS接收机采用接收机自主完整性监测（RAIM）算法来检测和拒绝异常测量值。RAIM算法寻找五个或更多伪范围的不一致集合，以检测异常测量。Psiaki et al.[213]认为，这种技术可以提供一种基本的防御手段，以防在接收器接收到的真实信号中只发送一个或两个虚假信号的不成熟的欺骗。对于更复杂的攻击，如Humphreys[49]实现的攻击，这种技术不实用。为了应对复杂的攻击，一些研究人员通过查找GPS数据和其他传感器（其他传感器）之间的不一致性来寻找解决方案。乔等人[220]利用IMU和单目摄像机为无人机提供了GPS欺骗解决方案。数据融合在电力系统中的应用

D.2。对策的现状155





图D.2：合成天线阵列结构[219]

IMU数据和摄像头数据允许确定无人机的速度。然后，将该值与从GPS数据获得的值进行比较。当无人机靠近地面飞行时，该解决方案可以很好地工作。然而，在高海拔地区，相机捕捉到的图像细节的退化可能会降低该解决方案的有效性。Panice等人[221]提出了一种使用支持向量机（SVM——一种机器学习）的解决方案。此解决方案只需要来自GPS和IMU的数据。比较从GPS数据和IMU数据获得的位置信息，以寻找不一致性。为了从IMU测量中估计位置，需要将加速度随时间积分。在此操作中，无论误差多么小，都会随着时间的推移而累积。这导致了IMU数据位置估计中的漂移效应。Panice等人提出的解决方案对长时间攻击（超过30秒）不具有鲁棒性。Feng等人[222]提出了另一种基于IMU/GPS数据分析的解决方案。该解决方案将重点放在从IMU数据和GPS数据获得的加速度值上，而不是无人机位置。这样可以避免误差累积效应，并使结果更加稳健。然而，该解决方案需要手动校准一些参数和阈值，这取决于无人机的性质。

小结：在本节中，我们简要回顾了GPS欺骗检测解决方案。我们将提出的解决方案分为三种方法：（1）信号处理，（2）空间处理，（3）数据处理。前两种方法需要开发特定的GPS接收机（硬件和软件）。同时，与第三种方法相关的大多数解决方案都可以在市场上现有的产品上实施。其中一些只需要修改自动驾驶仪软件。

附录E

原始SORA方法中的运行安全目标



157



**无人驾驶系统规则制定联合机构**

**关于索拉的JARUS指南**

**附件E**

**运行安全目标（OSO）的完整性和保证水平**

**文档标识符：JAR-DEL-WG6-D.04**

|  |  |  |  |
| --- | --- | --- | --- |
| **版本号** | **:** |  | **1.0** |
| **出版日期** | **:** |  | **25.01.2019** |
| **地位** | **:** |  | **最终/公开发布** |
| **打算** | **:** |  | **出版** |
| **类别** | **:** |  | **指导方针** |
| **工作组** | **:** |  | **6** |

**©未经JARUS许可，不得复制**

*版权所有。除非另有规定，否则可使用本文件中的信息，但未经JARUS许可，不得复制粘贴。*

**目录**

**附件E：**

**运行安全目标（OSO）的完整性和保证水平**

1.如何使用SORA附件E。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。3.

2.UAS的技术问题。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。4.

OSO#01-确保操作员有能力和/或证明。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。4.

OSO 02-由合格和/或经验证的实体制造的UAS。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。5.

OSO#03-由合格和/或经证明的实体维护的UAS。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。6.

OSO 04-根据权威机构认可的设计标准开发的无人机。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。7.

OSO 05-UAS的设计考虑了系统的安全性和可靠性。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。8.

OSO#06-C3链路特性（例如性能、频谱使用）适用于操作。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。9

OSO#07-检查UAS（产品检查），以确保与ConOps的一致性。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。11

3.与操作程序相关的OSO。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。12

OSO#08-定义、验证和遵守操作程序（以解决UAS的技术问题）。。。。。。。。。12

OSO#11-制定程序处理支持UAS运行的外部系统的恶化。。。。。。。。。。。。。。。。。。。。。。12

OSO#14-定义、验证和遵守操作程序（以解决人为错误）。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。12

OSO 21-定义、验证和遵守操作程序（以解决不利操作条件）。。。。。。。。。12

4.与远程船员培训相关的OSO。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。14

OSO#09-远程机组人员经过培训，能够控制异常和紧急情况（即UAS的技术问题）。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。14

OSO#15-受过培训的远程机组人员，能够控制异常和紧急情况（即人为错误）14

OSO#22-远程机组人员接受培训，以识别关键环境条件并避免这些条件。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。14

5.与安全设计相关的OSOs。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。15

OSO第10条-技术问题的安全恢复。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。15

OSO#12-无人机系统设计用于管理支持无人机运行的外部系统的退化。。。。。。。。。。。。。。。。。。。。。。。。15

6.支持UAS运行的外部系统恶化。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。16

OSO#13-支持UAS运营的外部服务足以满足运营要求。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。16

7.人为错误。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。17

OSO 16-多机组协调。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。17

OSO 17-远程船员适合操作。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。19

OSO#18-自动保护飞行包线免受人为错误影响。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。20

OSO 19-从人为错误中安全恢复。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。21

OSO#20-已经进行了人因评估，发现人机界面（HMI）适合任务。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。23

8.不利的操作条件。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。24

OSO#23-定义、测量和遵守安全操作的环境条件。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。24

OSO#24-针对不利环境条件设计和鉴定的无人机（例如，足够的传感器、DO-160鉴定）。25

9技术OSO的保证水平标准。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。26

# *1.   如何使用SORA附件E*

下表提供了使用Sura附录E时应考虑的基本原则。

|  |  |  |
| --- | --- | --- |
|  | **原理描述** | **补充资料** |
| #1 | 附录E提供了完整性（即安全增益）和保证（即。  操作安全的证明方法  申请人提出的目标（OSO）。 | 申请人应负责确定给定操作的操作安全目标。 |
| #2 | 附件E未涵盖以下内容：  主管当局的参与（LoI）。Lol基于主管当局对申请人执行给定操作能力的评估。 | 一些JARUS集团（如WG-7）可能会提供参与程度的标准，供主管当局使用。 |
| #3 | 达到一定程度的  完整性/保证，当该级别的完整性/保证存在多个标准时，需要满足所有适用标准。 |  |
| #4 | SORA主体表8中定义的“可选”情况不需要在附录E中定义完整性和保证水平。 | 运行安全目标的所有稳健性水平均可接受，SORA主体的表6“推荐运行安全目标（OSO）”中定义了“可选”稳健性水平。 |
| #5 | 当评估运行安全目标的完整性或保证水平的标准依赖于尚不可用的“标准”时，OSO需要以主管当局可接受的方式制定。 |  |
| #6 | 附件E故意使用非规定性条款（例如，适当的、合理可行的）为申请人和主管当局提供灵活性。这并不限制申请人提出缓解措施，也不限制主管当局根据具体情况评估所需措施。 |  |
| #7 | 本附件全文也适用于单人组织。 |  |

# *2.   与UAS的技术问题*

## OSO#01-确保操作员有能力和/或经过验证

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **诚信水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#01确保操作员有能力和/或经过验证** | 标准 | 申请人了解正在使用的UAS，并且至少具有以下相关操作程序：检查表、维护、，  培训、责任和相关职责。 | 和低的一样。此外，申请人有一个适合预期操作的组织。申请人还拥有识别、评估和缓解与飞行运行相关风险的方法。这些应符合规定操作的性质和范围。 | 和中号一样。 |
| *评论* | *不适用* | *1在本次评估中，适当的应解释为与组织规模和业务复杂性相称/相称。* | *不适用* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#01确保操作员有能力和/或经过验证** | 标准 | 完整性等级中描述的要素在ConOps中进行了说明。 | 在第一次操作之前，有能力的第三方对组织进行审核 | 申请人持有组织运行证书或具有公认的飞行试验组织。  此外，合格的第三方会反复验证操作员的能力。 |
| *评论* | *不适用* | *不适用* | *不适用* |

## OSO#02-由合格和/或经验证的实体制造的无人机

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **诚信水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#02由合格和/或经验证的实体制造的无人机** | 标准 | 制造程序至少包括：  •材料规范  •所用材料的适用性和耐久性，  •允许  制造的重复性和合格性在可接受的公差范围内。 | 和低的一样。此外，制造程序还包括：  •配置控制，  •验证来料产品、零件、材料和设备，  •标识和可追溯性，  •过程中和最终检查与测试，  •工具的控制和校准，  •搬运和储存，  •不符合项控制。 | 和中号一样。此外，制造程序至少包括：  •制造过程，  •人员能力和能力  资格  •供应商控制。 |
| *评论* | *不适用* | *不适用* | *不适用* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#02由合格和/或经验证的实体制造的无人机** | 标准 | 已申报的制造程序是按照主管当局认为适当的标准和/或按照主管当局可接受的合规手段制定的。 | 和低的一样。此外，有证据表明UAS是按照其设计制造的。 | 和中号一样。此外：  •制造程序，  •UAS符合其设计和规范  由合格的第三方通过过程或产品审核进行反复验证。 |
| *评论* | *国家航空管理局（NAAs）可以定义他们认为适当的标准和/或遵守方法。SORA附录E将在稍后时间根据NAAs提供的反馈更新，并提供适当标准清单。* | *不适用* | *不适用* |

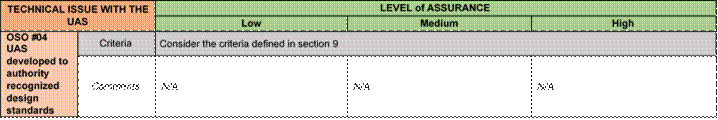
## OSO#03-由合格和/或经验证的实体维护的UAS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **诚信水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#03由合格和/或经验证的实体维护的无人机（如行业标准）** | 标准 | •定义了UAS维护说明，适用时涵盖UAS设计师说明和要求。  •维护人员有能力并已获得执行UAS维护的授权。  •维护人员在执行维护时使用UAS维护说明。 | 和低的一样。此外：  •根据维护计划组织每个UAS的定期维护。  •完成后，维护日志系统用于记录在UAS上进行的所有维护，包括发布。维修放行只能由已获得该特定UAS型号/系列维修放行授权的工作人员完成。 | 和中号一样。此外，维护人员按照维护程序手册进行工作  提供与维护设施、记录、维护说明、发布、工具、材料、组件、缺陷延期相关的信息和程序… |
| *评论* | *不适用* | *不适用* | *不适用* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#03由合格和/或经验证的实体维护的无人机（如行业标准）** | 标准#1（程序） | •记录维护说明。  •在UAS上进行的维护记录在维护日志系统1/2中。  •建立并更新授权进行维护的维护人员名单。 | 和低的一样。此外：  •维护计划是根据主管当局认为适当的标准和/或该当局可接受的合规手段3制定的。  •建立并更新具有维修放行授权的维修人员名单。 | 和中号一样。此外，维护计划和维护程序手册由合格的第三方验证。 |
| *评论* | *1目的是记录在飞机上执行的所有维护，以及执行的原因（缺陷或故障纠正、修改、，*  *定期维护等）2审批机关或授权代表可要求检查/审计维护日志。* | *3 国家航空管理局（NAAs）可以定义他们认为适当的标准和/或遵守方法。SORA附录E将在稍后时间根据NAAs提供的反馈更新，并提供适当标准清单。* | *不适用* |
| 标准#2（培训） | 维护人员完成的所有相关资格、经验和/或培训记录均已建立并保持最新。 | 和低的一样。此外：  •培训大纲和培训标准，包括最初的  定义了理论/实践要素、持续时间等，并与维护人员持有的授权相称。  •对于持有维修放行许可证的员工，初始培训针对特定的UAS型号/系列。  •所有维护人员都接受了初步培训。 | 和中号一样。此外：  •制定了持有维修放行许可证的员工的定期培训计划；和  •本计划由合格的第三方验证。 |
| *评论* | *不适用* | *不适用* | *不适用* |

## OSO#04-根据权威机构认可的设计标准开发的无人机

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| **OSO#04 UAS根据权威机构认可的设计标准开发** | 标准 | UAS的设计符合主管当局认为适当的标准和/或该当局可接受的合规手段。标准和/或合规手段应适用于低水平的完整性和预期操作。 | UAS的设计符合主管当局认为适当的标准和/或该当局可接受的合规手段。标准和/或合规手段应适用于中等水平的  完整性和预期操作。 | UAS的设计符合主管当局认为适当的标准和/或该当局可接受的合规手段。标准和/或合规手段应适用于高水平的完整性和预期操作。 |
| *评论* | *国家航空管理局（NAAs）可以定义他们认为适当的标准和/或遵守方法。SORA附录E将在稍后时间根据NAAs提供的反馈更新，并提供适当标准清单。* | | |



## OSO#05-UAS的设计考虑了系统的安全性和可靠性

（a） 本OSO补充了：

•主体中规定的安全壳安全要求

•OSO#10和OSO#12，仅解决在人口稠密地区或人群聚集地作业时的死亡风险。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **诚信水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#05无人机的设计考虑了系统的安全性和可靠性** | 标准 | 设备、系统和装置的设计应确保在UAS可能发生故障或故障时，将危险降至最低。 | 和低的一样。此外，对于可能导致危险的任何故障、故障或其组合的检测、警报和管理策略也是可用的。 | 和中号一样。此外：  •主要故障条件的频率不超过Remote3；  •危险故障条件的频率不超过3；  •灾难性故障条件的频率不超过极不可能3；  •软件（SW）和机载电子硬件（AEH），其开发错误可能导致或促成危险或灾难性故障条件，按照主管当局认为适当的行业标准或方法开发，和/或按照主管当局可接受的合规手段开发。 |
| *评论* | *1 在本评估中，术语“危险”应解释为与以下方面相关的故障条件：*  *重大的、危险的或灾难性的。*  *2 在本评估中，“可能”一词应定性解释为“预计在UAS的整个系统/运行寿命内发生一次或多次”。* | *不适用* | 3 *安全目标可以从*  *JARUS AMC RPAS.1309第2版表3取决于UAS类别或主管当局可接受的同等基于风险的方法。*  4 *SW/AEH的开发保证水平（DAL）可从JARUS AMC RPAS.1309第2版表3中得出，具体取决于UAS等级或主管当局可接受的同等基于风险的方法。* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#05无人机的设计考虑了系统**  **安全性和可靠性** | 标准 | 功能危害评估1和设计与安装评估表明危害最小化。 | 和低的一样。此外：  •根据主管当局认为适当的标准和/或根据主管当局可接受的合规手段进行安全分析。  •单一故障检测策略包括飞行前检查。 | 和中号一样。此外，安全分析和开发保证活动由合格的第三方进行验证。 |
| *评论* | *1应根据JARUS AMC RPAS.1309中提供的定义确定故障条件的严重性（无安全影响、轻微、重大、危险和灾难性）*  *问题2。* | *不适用* | *不适用* |

## OSO#06-C3链路特性（例如性能、频谱使用）适用于该操作

（a） 就SORA和本特定OSO而言，“C3链接”一词包括：

•指挥和控制（C2）链路，以及

•飞行安全所需的任何通信链路。

（b） 为了正确评估本OSO的完整性，申请人应确定：

1） C3链接预期操作所需的性能要求。

2） 所有C3链路及其实际性能和射频（RF）频谱使用情况。

笔记：UAS设计师通常在UAS手册中记录C2链路的性能和射频频谱规范。

笔记：与C2链路性能（RLP）相关的主要参数和其他通信链路的性能参数（例如，与ATC通信的RCP）包括但不限于：

o事务过期时间o可用性o连续性o完整性

有关定义，请参阅国际民航组织参考资料。

3） 预期操作的射频频谱使用要求（包括必要时的授权需求）。

笔记：通常，国家会公布适用于其领土的射频频段分配。这种分配主要来自国际通信联盟（ITU）的无线电条例。但是，申请人应检查当地要求，并在需要时请求授权，因为可能存在国家差异和具体分配（例如，国际电联分配的国家分部）。一些航空波段（如AM（R）S、AMS（R）S 5030-5091MHz）被分配用于国际民航组织范围内归类为cat的无人机运行中的无人机运行。C（“认证”），但可授权其用于特定类别下的操作。预计在特定类别下也可授权使用其他许可频段（例如分配给移动网络的频段）。某些未经许可的波段（例如ISM（工业、科学、医疗）或SRD（短程设备））在特定类别下也可以接受，例如用于完整性要求较低的操作。4） 可能影响C3链路性能的环境条件。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | | **诚信水平** | |  |
| **低的** | **中等的** | **高的** |
| **OSO#06**  **C3链路特性（例如：。**  **性能、频谱使用）适用于该操作** | 标准 | •申请人确定C3链路的性能、射频频谱使用1和环境条件足以安全进行预期操作。  •UAS远程飞行员能够持续监控C3性能，并确保性能继续满足运行要求2。 | 与Low3相同。 | 和低的一样。此外，C2链路需要使用许可的4个频段。 |
| *评论* | *1 对于较低的完整性水平，在某些条件下，可以接受未经许可的频带，例如：*  • *申请人证明UAS设备符合其他射频频谱使用要求（例如，对于欧盟：指令2014/53/EU，对于美国：CFR标题47第15部分联邦通信委员会（FCC）规则），从而证明符合这些要求*  *（例如FCC标记），以及*  • *使用机制防止干扰（例如FHSS、程序频率解冲突）。*  *2远程飞行员能够持续、及时地访问可能影响飞行安全的相关C3信息。对于仅要求该OSO具有较低完整性的操作，可通过监测C2链路信号强度并在信号过低时从UAS HMI接收警报来实现。* | *3 根据运营情况，可能需要使用许可频段。在某些情况下，可以接受使用非航空频段（例如蜂窝网络的许可频段）。* | *4 这确保了最低水平的性能，且不限于航空许可频段*  *（例如，蜂窝网络的许可频段）。然而，一些操作可能需要使用分配给航空移动服务的频带来使用C2链路（例如5030–5091 MHz）。*  *在任何情况下，使用许可频段都需要授权。* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#06**  **C3链路特性（例如：。**  **性能、频谱使用）适用于该操作** | 标准 | 考虑第9节中定义的保证标准（低保证水平） | C3链路性能的证明符合主管当局认为适当的标准和/或该当局可接受的合规手段。 | 和中号一样。此外，证据由合格的第三方验证。 |
| *评论* | *不适用* | *国家航空管理局（NAAs）可以定义他们认为适当的标准和/或遵守方法。SORA附录E将在稍后时间根据NAAs提供的反馈更新，并提供适当标准清单。* | *不适用* |

## OSO#07-检查UAS（产品检查），以确保与ConOps的一致性

（a） 本OSO的目的是确保用于操作的UAS符合用于支持操作批准/授权的UAS数据。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| **OSO#07 UAS检查（产品检查）以确保一致性**  **到**  **ConOps** | 标准 | 远程机组确保UAS处于安全运行状态，并符合批准的运行概念。1 | | |
| *评论* | *1 该标准的低、中、高鲁棒性水平之间的区别是通过保证水平实现的（见下表）。* | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **技术问题**  **无人机** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#07 UAS检查（产品检查），以确保与**  **ConOps** | 标准#1（程序） | 产品检查记录在案，并说明制造商的建议（如有）。 | 和低的一样。此外，使用检查表记录产品检查。 | 和中号一样。此外，产品检验由合格的第三方进行验证。 |
| *评论* | *不适用* | *不适用* | *不适用* |
| 标准#2（培训） | 远程工作人员接受过产品检验的培训，并且该培训是自我声明的（有证据可用）。 | •提供培训大纲，包括产品检验程序。  •操作员提供基于能力的理论和实践培训。 | 合格的第三方：  •验证培训大纲。  •验证远程乘员能力。 |
| *评论* | *不适用* | *不适用* | *不适用* |

# *3.   与操作程序有关的OSO*

### OSO#08-定义、验证和遵守操作程序（解决UAS的技术问题）

### OSO#11-制定了程序，以处理支持无人机运行的外部系统的恶化

### OSO#14-定义、验证和遵守操作程序（以解决人为错误）

### OSO#21-定义、验证并遵守操作程序（以解决不利操作条件）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **操作程序** | | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| **OSO#08，**  **OSO 11、OSO 14和OSO**  **#21** | 标准#1  （程序定义） | •定义了适用于拟定操作的操作程序1，并至少涵盖以下要素：  o飞行计划，  o飞行前和飞行后检查，o评估飞行前和飞行期间环境条件的程序（即实时评估），o应对意外不利运行条件的程序（例如，在未经批准的结冰条件下运行期间遇到冰时）  o正常程序、o应急程序（应对异常情况）、o应急程序（应对紧急情况）和o事件报告程序。  •操作手册中编制了正常、应急和应急程序。  •支持UAS操作的外部系统的限制2在操作手册中定义。 | | |
| *评论* | *1操作程序包括UAS本身和任何支持UAS操作的外部系统的退化。*    *2在本评估范围内，支持UAS运行的外部系统被定义为不属于UAS的系统，但用于：*  • *发射/起飞无人机，进行飞行前检查，*  • *使UA保持在其业务量内（例如，全球导航卫星系统、卫星系统、空中交通管理、UTM）。*  *在运行失控后激活/使用的外部系统不包括在本定义中。*    *3为正确解决运行所需外部系统的退化问题，建议：*  • *识别这些“外部系统”，*  • *识别可能导致运行失控的“外部系统”劣化模式（例如，全球导航卫星系统完全丧失、全球导航卫星系统漂移、延迟问题等），*  • *描述检测外部系统/设施劣化模式的方法，*  • *描述检测到劣化时使用的程序（例如，激活紧急恢复能力，切换到手动控制…）。* | | |
| 标准#2（程序复杂性） | 操作程序非常复杂，可能会增加远程机组的工作量和/或与其他实体（例如：。  自动取款机。 | 当UAS通常自动控制时，应急/应急程序需要遥控器2手动控制。 | 操作程序简单。 |
| *评论* | *不适用* | 2 *这仍在讨论中，因为并非所有无人机都有飞行员可以直接控制地面的模式；此外，一些人声称，要想不让事情变得更糟，这需要很高的技巧。* | *不适用* |
| 标准#3  （审议  潜在人为错误） | 操作程序至少应提供：  •明确分配和分配任务  •确保员工充分执行分配任务的内部检查表。 | 操作程序将人为错误考虑在内。 | 和中号一样。此外,  远程Crew3接受乘员资源管理（CRM）4培训。 |
| *评论* | *不适用* | *不适用* | *3 在SORA中，“远程机组人员”一词是指参与任务的任何人员。*  *4 CRM培训的重点是有效使用所有远程机组，以确保安全高效的运行，减少错误，避免压力，提高效率。* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **操作程序** | |  | **保证水平** | |
| **低的** | **中等的** | **高的** |
| **OSO#08，**  **OSO 11、OSO 14和OSO**  **#21** | 标准 | •操作程序不需要根据主管当局认为适当的标准或合规手段进行验证。  •宣布操作程序的充分性，但经测试的应急程序除外。 | •根据主管当局认为适当的标准和/或根据主管当局可接受的合规手段对操作程序进行验证1。    •通过以下方式证明应急和应急程序的充分性：  o专用飞行试验，或o模拟，前提是该模拟被证明对预期目的有效，并产生积极结果。 | 和中号一样。此外：    •为验证程序和检查表而进行的飞行试验涵盖了整个飞行包线或被证明是保守的。  •程序、检查表、飞行试验和模拟由合格的第三方验证。 |
| *评论* | *不适用* | 1 *国家航空管理局（NAAs）可以定义他们认为适当的标准和/或遵守方法。SORA附录E将在稍后时间根据NAAs提供的反馈更新，并提供适当标准清单。* | |

# *4.   与远程船员培训相关的OSO*

### OSO#09-远程机组人员经过培训，掌握最新信息，能够控制异常和紧急情况（即UAS的技术问题）

### OSO#15-受过培训的远程机组人员，能够控制异常和紧急情况（即人为错误）

### OSO#22-远程机组人员接受培训，以识别关键环境条件并避免这些条件

（a） 申请人需要提出基于能力的理论和实践培训：

•适用于待批准的操作，以及

•包括熟练度要求和培训复发。

（b） 整个远程机组人员（即参与操作的任何人员）应接受针对其职责的基于能力的理论和实践培训（如飞行前检查、地面设备操作、气象条件评估…）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **远程船员能力** | | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| **OSO#09，OSO**  **#15和OSO**  **#22** | 标准 | 基于能力的理论和实践培训确保了解：a）UAS法规  b） 无人机空域工作原理  c） 航空技术与航空安全  d） 人因限制  e） 气象学  f） 导航/图表  g） UA知识  h） 操作程序  并足以进行操作。1/2 | | |
| *评论* | *1JARUS WG1将于2019年提供上述不同主题所涵盖区域的详细信息。2本标准的低、中、高鲁棒性水平之间的区别通过保证水平实现（见下表）。* | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **远程船员能力** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#09，OSO**  **#15和OSO**  **#22** | 标准 | 培训是自我声明的（有证据可用）。 | •提供培训大纲。  •操作员提供基于能力的理论和实践培训。 | 合格的第三方：  •验证培训大纲。  •验证远程乘员能力。 |
| *评论* | *不适用* | *不适用* | *不适用* |

# *5.   与安全设计相关的OSOs*

### OSO#10-技术问题的安全恢复

### OSO#12-无人机系统旨在管理支持无人机运行的外部系统的退化

（a） OSO#10和OSO#12的目标是通过解决在人口稠密地区或人群聚集地上运行时的死亡风险，补充技术安全壳安全要求。

（b） 在本评估范围内，支持UAS运行的外部系统被定义为不属于UAS的系统，但用于：

•发射/起飞无人机， 进行飞行前检查，

•将UA保持在其业务量内（例如，全球导航卫星系统、卫星系统、空中交通管理、UTM）。

在运行失控后激活/使用的外部系统不包括在本定义中。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | **诚信水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#10和OSO#12** | 标准 | 当在人口稠密的地区或人群聚集的地方进行操作时，可以合理预期，无人机或支持操作的任何外部系统的任何可能故障都不会导致死亡。 | 在人口稠密地区或人群聚集地作业时：  可以合理预期，UAS或支持运行的任何外部系统的任何单一故障3不会导致死亡。  软件（SW）和机载电子硬件（AEH），其开发错误可能直接导致影响运行的故障，从而合理预期将发生致命事故，并根据主管当局认为适当的标准和/或该当局可接受的合规手段4制定。 | 和中号一样 |
| *评论* | *1 在本评估中，“可能”一词应定性解释为“预计在UAS的整个系统/运行寿命内发生一次或多次”。*    *2 如果可以证明这些机械部件的设计符合航空工业最佳实践，则某些结构或机械故障可能被排除在标准之外。* | *3 如果可以证明这些机械部件的设计符合主管当局认为适当的标准和/或符合主管当局可接受的合规手段，则某些结构或机械故障可从nosingle故障标准中排除*    *4 国家航空管理局（NAAs）可以定义他们认为适当的标准和/或遵守方法。SORA附录E将在稍后时间根据NAAs提供的反馈更新，并提供适当标准清单。* |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#10和OSO#12** | 标准 | 可进行设计和安装评估。特别是，本次评估表明：  •设计和安装特征（独立、分离和冗余）满足低完整性标准；  •与ConOps相关的特殊风险（如冰雹、冰、雪、电磁干扰等）不违反独立性声明（如有）。 | 和低的一样。此外，通过分析和/或试验数据以及支持性证据证明所声称的完整性水平。 | 和中号一样。此外，有能力的第三方验证所声称的完整性水平。 |
| *评论* | *不适用* | *不适用* | *不适用* |

# *6.   支持无人机运行的外部系统恶化*

## OSO#13-支持UAS运营的外部服务足以满足运营要求

就SORA和本特定OSO而言，“支持UAS运行的外部服务”一词包括保障飞行安全所需的任何服务提供商，例如：。

•通信服务提供商（CSP），

•UTM服务提供商…

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **变质**  **外部系统**  **支持无人机**  **不受UAS控制的操作** | | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| **OSO#13支持UAS的外部服务**  **操作对操作是足够的** | 标准 | 申请人确保为确保飞行安全所需的任何外部服务的性能水平足以满足预期运行。  如果外部提供的服务需要运营商和服务提供商之间的沟通，申请人应确保进行有效沟通，以支持服务条款。  定义了申请人和外部服务提供商之间的角色和责任。 | | |
| *评论* | *不适用* | *不适用* | *与服务提供商签订服务合同的要求可根据国际民航组织标准和*  *推荐做法——SARP（目前正在开发中）。* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **变质**  **外部系统**  **支持无人机**  **不受UAS控制的操作** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#13外部服务**  **支持无人机**  **操作对操作是足够的** | 标准 | 申请人声明已达到为确保飞行安全所需的任何外部服务的要求性能水平（无必要提供证据）。 | 申请人有证据证明，在整个飞行任务期间，为确保飞行安全所需的任何外部服务都能达到要求的性能水平。  这可以采取服务水平协议（SLA）或服务提供商与申请人之间就服务相关方面（包括质量、可用性、责任）达成的任何官方承诺的形式。  申请人有能力监控影响飞行关键系统的外部服务，并在实时性能可能导致运行失控时采取适当措施。 | 与介质相同。此外：  •外部提供服务绩效的证据通过演示获得。  •合格的第三方验证声称的完整性水平。 |
| *评论* | *不适用* | *不适用* | *不适用* |

# *7.   人为错误*

## OSO#16-多机组协调

（a） 本OSO仅适用于直接参与飞行操作的人员。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **人为错误** | | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| **OSO#16多机组协调** | 标准#1（程序） | 确保机组成员之间的协调和可靠有效的沟通渠道可用的程序，且至少覆盖：  •向船员分配任务，  •建立逐步沟通。1 | | |
| *评论* | *1 该标准的低、中、高鲁棒性水平之间的区别是通过保证水平实现的（见下表）。* | | |
| 标准#2（培训） | 远程乘员培训包括多乘员协调 | 与Low相同。此外，远程乘员2接受乘员资源管理（CRM）3培训。 | 和中号一样。 |
| *评论* | *不适用* | *2 在SORA中，“远程机组人员”一词是指参与任务的任何人员。*    *3 CRM培训的重点是有效使用所有远程机组，以确保安全高效的运行，减少错误，避免压力，提高效率。* | *不适用* |
| 标准#3  （通讯设备） | 不适用 | 通信设备符合主管当局认为适当的标准和/或符合主管当局可接受的合规手段4。 | 通信设备为冗余设备5，并符合主管当局认为适当的标准和/或符合主管当局可接受的合规手段6。 |
| *评论* | *不适用* | *4国家航空管理局（NAAs）可以规定他们认为适当的标准和/或遵守的标准。SARA附件E将在稍后的时间点更新，并根据NAAs提供的反馈提供适当的标准清单。* | *5 这意味着提供一个额外的装置，以应对第一个装置的故障情况。*  *6 国家航空管理局（NAAs）可以规定他们认为适当的标准和/或遵守的标准。SARA附件E将在稍后的时间点更新，并根据NAAs提供的反馈提供适当的标准清单。* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **人为错误** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#16多机组协调** | 标准#1（程序） | •程序不需要对照标准进行验证  或主管当局认为适当的合规手段。  •宣布程序和检查表的充分性。 | •根据主管当局认为适当的标准和/或根据主管当局可接受的合规手段1对程序进行验证。    •通过以下方式证明程序的充分性：  o专用飞行试验，或o模拟，前提是该模拟被证明对预期目的有效，并产生积极结果。 | 与介质相同。此外：    •为验证程序而进行的飞行试验涵盖了整个飞行包线或被证明是保守的。  •程序、飞行试验和模拟由合格的第三方验证。 |
| *评论* | *不适用* | *1国家航空管理局（NAAs）可以规定他们认为适当的标准和/或遵守的标准。SARA附件E将在稍后的时间点更新，并根据NAAs提供的反馈提供适当的标准清单。* | *不适用* |
| 标准#2（培训） | 培训是自我声明的（有证据） | •提供培训大纲。  •操作员提供基于能力的理论和实践培训。 | 合格的第三方：  •验证培训大纲。  •验证远程乘员能力。 |
| *评论* | *不适用* | *不适用* | *不适用* |



## #17远程机组适合操作

（a） 在本评估中，“适合操作”一词应解释为身体和精神上适合安全履行职责和履行职责。

（b） 疲劳和压力是导致人为错误的因素。因此，为确保保持警惕，使其达到令人满意的安全水平，可考虑以下事项：

•远程机组值班时间；

•定期休息；

•休息时间；

•移交/接管程序。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **人为错误** | |  | **诚信水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#17**  **远程机组适合操作** | 标准 | 申请人有一项政策，规定远程机组人员如何在进行任何操作之前声明自己适合操作。 | 与Low相同。此外：  •远程机组的值班、飞行值班和休息时间由申请人确定，并足以进行操作。  •操作员定义适合远程机组操作UAS的要求。 | 与介质相同。此外： 远程船员身体状况良好，  疲劳风险管理系统（FRMS）用于管理值班/飞行值班时间的任何升级。 |
| *评论* | *不适用* | *不适用* | *不适用* |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **人为错误** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#17**  **远程机组适合操作** | 标准 | •定义远程乘员如何声明自己适合操作（操作前）的政策已记录在案。  •远程乘员适合操作声明（操作前）基于申请人定义的政策。 | 与Low相同。此外：  •记录远程机组值班、飞行值班和休息时间政策。  •记录远程机组工作循环，并至少覆盖：  o远程机组成员的值日开始时，  o当远程机组人员不值勤时，  o占空比内的休息时间。  •有证据表明远程机组适合操作UAS。 | 与介质相同。此外：  •建立主管当局认为适当的医疗标准和/或主管当局可接受的合规手段1，并由主管第三方验证远程船员的健康状况。  •合格的第三方验证值班/飞行值班时间。  •如果使用FRMS，则由合格的第三方进行验证和监控。 |
| *评论* | *不适用* | *不适用* | *1国家航空管理局（NAAs）可以规定他们认为适当的标准和/或遵守的标准。SARA附件E将在稍后的时间点更新，并根据NAAs提供的反馈提供适当的标准清单。* |

## OSO#18-自动保护飞行包线免受人为错误

（a） 无人驾驶飞机（UA）设计有一个飞行包线，该包线描述了其在最低和最高运行速度以及运行结构强度方面的安全性能极限。

（b） 飞行包线的自动保护旨在防止远程飞行员在其飞行包线外操作UA。如果申请人证明远程飞行员不在回路中，则本OSO不适用。

（c） 实施此类自动保护功能的无人机将确保无人机在可接受的飞行包线裕度内运行，即使在远程飞行员控制输入不正确的情况下（人为错误）。

（d） 无自动保护功能的无人机容易受到不正确的远程飞行员控制输入（人为错误）的影响，如果超过飞机的设计性能限制，则可能导致无人机丢失。

（e） 飞行包线保护的故障或开发错误在OSOs第5、10和12条中进行了说明。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **人为错误** | |  | **诚信水平** | |
| **低的** | **中等的** | **高的** |
| **OSO#18**  **自动保护飞行包线不受人为错误影响** | 标准 | UAS飞行控制系统包括对飞行包线的自动保护，以防止远程飞行员在正常操作条件下进行任何单一输入，从而导致UA超出其飞行包线或阻止其及时恢复。 | UAS飞行控制系统包括对飞行包线的自动保护，以确保UA保持在飞行包线内，或确保在远程飞行员出错后及时恢复到设计的运行飞行包线。1 | |
| *评论* | *不适用* | *1通过保证水平（见下表），可以区分该标准的中等稳健性水平和高稳健性水平。* | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **人为错误** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#18**  **自动保护**  **飞行包线不受人为错误的影响** | 标准 | 飞行包线的自动保护是在内部或开箱即用的情况下开发的（例如，使用组件现货元件），没有遵循特定标准。 | 飞行包线的自动保护已发展到主管当局认为适当的标准和/或按照主管当局可接受的合规手段。 | 与介质相同。此外，证据由合格的第三方验证。 |
| *评论* | *不适用* | *国家航空管理局（NAAs）可以规定他们认为适当的标准和/或遵守的标准。SARA附件E将在稍后的时间点更新，并根据NAAs提供的反馈提供适当的标准清单。* | *不适用* |

## #19从人为错误中安全恢复

（a） 本OSO解决了如果不及时预防、检测和恢复可能影响操作安全的人为错误风险。

i） 错误可能来自操作中涉及的任何人ii）一个示例可能是人为错误，导致有效载荷加载不正确，有可能在操作过程中从UA上跌落。iii）另一个示例可能是人为错误，没有延伸天线杆，降低了C2链路覆盖范围。

笔记：本OSO不包括飞行包线保护，因为OSO#18专门涵盖了飞行包线保护。

（b） 本OSO包括：

i） 程序和清单，ii）培训，以及

iii）无人机设计，即检测和/或从人为错误中恢复的系统（例如安全别针、使用确认功能、燃料或能源消耗监测功能…）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **人为错误** | | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| **OSO#19安全恢复**  **来自人类**  **错误** | 标准#1  （程序和清单） | 定义并使用程序和检查表，以降低任务相关人员潜在人为错误的风险。  程序至少提供：  •明确分配和分配任务，  •确保员工充分执行分配任务的内部检查表。 | | |
| *评论* | *不适用* | *不适用* | *不适用* |
| 标准#2（培训） | •对远程Crew1进行程序和检查表培训。  •远程乘员1接受乘员资源管理（CRM）2培训。3 | | |
| *评论* | *1 在SORA中，“远程机组人员”一词是指参与任务的任何人员。*  *2 CRM培训的重点是有效使用所有远程机组，以确保安全高效的运行，减少错误，避免压力，提高效率。*  *3该标准的低、中、高鲁棒性水平之间的区别是通过保证水平实现的（见下表）。* | | |
| 标准#3（无人机设计） | 根据行业最佳实践，开发了检测和/或恢复人为错误的系统。 | 根据主管当局认为适当的标准和/或根据主管当局可接受的合规手段，开发检测和/或从人为错误中恢复的系统。 | 和中号一样。 |
| *评论* | *不适用* | *国家航空管理局（NAAs）可以规定他们认为适当的标准和/或遵守的标准。SARA附件E将在稍后的时间点更新，并根据NAAs提供的反馈提供适当的标准清单。* | *不适用* |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **人为错误** | | **保证水平** | | | | | | | |
| **低的** | | **中等的** | | | **高的** | | |
| **OSO#19**  **安全恢复**  **来自人类**  **错误** | 标准#1  （程序和清单） | •程序和检查表不需要根据主管当局认为适当的标准或合规手段进行验证。  •宣布程序和检查表的充分性。 | | •根据主管当局认为适当的标准和/或根据主管当局可接受的合规手段1验证程序和检查表。    •通过以下方式证明程序和检查表的充分性：o专用飞行试验，或o模拟，前提是模拟被证明对预期目的有效，并产生积极结果。 | | | 与介质相同。此外：    •为验证程序和检查表而进行的飞行试验涵盖了整个飞行包线或被证明是保守的。  •程序、检查表、飞行试验和模拟由合格的第三方验证。 | | |
| *评论* | *不适用* | | *1国家航空管理局（NAAs）可以规定他们认为适当的标准和/或遵守的标准。SARA附件E将在稍后的时间点更新，并根据NAAs提供的反馈提供适当的标准清单。* | | | *不适用* | | |
| 标准#2（培训） |  | 考虑一般远程船员培训OSO（即OSO 09，OSO 15）的保证水平定义的标准。 | | | | | |  |
| OSO#22）对应于操作的帆 | | |  | | |
| **人为错误** | |  | | | **保证水平** | |  |  | |
| **低的** | |  | **中等的** | |  | **高的** | |
|  | *评论* | *不适用* | | *不适用* |  | | *不适用* |  | |
| 标准#3（无人机设计） | 考虑第9节中定义的标准 | | |  | |  |  | |
| *评论* | *不适用* | | *不适用* |  | | *不适用* |  | |
|  |  |  |  |  |  |  |  |  |  |

## #20已进行人为因素评估，发现人机界面（HMI）适合任务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **人为错误** | | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| **OSO#20**  **已进行人为因素评估，HMI适合任务** | 标准 | UAS信息和控制界面清晰简洁，不会混淆、造成不合理的疲劳或导致可能对操作安全产生不利影响的远程乘员错误。 | | |
| *评论* | 如果使用电子手段支持潜在的视觉观察者保持对无人机位置的感知，其HMI：  •足以让视觉观察员在运行期间确定UA的位置；  •不会降低视觉观察员的能力：o目视扫描无人驾驶飞机运行的空域，以发现任何潜在的碰撞危险；o始终保持与远程飞行员的有效通信。 | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **人为错误** | |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **OSO#20**  **人**  **已进行因素评估，HMI适合任务** | 标准 | 申请人对UAS进行人为因素评估，以确定HMI是否适合任务。HMI评估基于检查或分析。 | 与Low相同，但HMI评估基于演示或模拟。1 | 与介质相同。此外，有能力的第三方见证HMI评估。 |
| *评论* | *不适用* | *1 使用模拟时，需要证明模拟中使用的目标环境的有效性。* | *不适用* |

# *8.   不利的操作条件*

## OSO#23-定义、测量和遵守安全操作的环境条件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **不利的操作条件** | | **诚信水平** | | |
| **低的** | **中等的** | **高的** |
| **OSO#23定义、测量和遵守安全操作的环境条件** | 标准#1（定义） | 飞行手册或同等文件中定义并反映了安全运行的环境条件。1 | | |
| *评论* | *1该标准的低、中、高鲁棒性水平之间的区别是通过保证水平实现的（见下表）。* | | |
| 标准#2（程序） | 任务前和任务期间的环境条件评估程序（即实时评估）可用，包括使用简单记录系统评估气象条件（METAR、TAFOR等） | | |
| *评论* | *2该标准的低、中、高鲁棒性水平之间的区别是通过保证水平实现的（见下表）。* | | |
| 标准#3（培训） | 培训内容包括气象条件评估 | | |
| *评论* | *3该标准的低、中、高鲁棒性水平之间的区别是通过保证水平实现的（见下表）。* | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **不利的操作条件** | |  | **保证水平** | |  |
| **低的** |  | **中等的** | **高的** |
| **OSO#23定义、测量和遵守安全操作的环境条件** | 标准#1（定义） | 考虑第9节中定义的标准 |  | |  |
| *评论* | *不适用* |  | |  |
| 标准#2（程序） | •程序不需要对照标准进行验证  或主管当局认为适当的合规手段。  •宣布程序和检查表的充分性。 | •根据主管当局认为适当的标准和/或根据主管当局可接受的合规手段对程序进行验证。    •通过以下方式证明程序的充分性：  o专用飞行试验，或o模拟，前提是该模拟被证明对预期目的有效，并产生积极结果。 | | 和中号一样。此外：    •为验证程序而进行的飞行试验涵盖了整个飞行包线或被证明是保守的。  •程序、飞行试验和模拟由合格的第三方验证。 |
| *评论* | *不适用* | *不适用* | | *不适用* |
| 标准#3（培训） | 培训是自我声明的（有证据可用）。 | •提供培训大纲。  •操作员提供基于能力的理论和实践培训。 | | 合格的第三方：  •验证培训大纲。  •验证远程乘员能力。 |
| *评论* | *不适用* | *不适用* | | *不适用* |
|  |  |  |  |  |  |

## #针对不利环境条件设计和鉴定的24个UAS（例如，足够的传感器、DO-160鉴定）

（a） 为了评估本OSO的完整性，申请人确定：

•设备环境鉴定测试/声明是否可以获得学分，例如回答以下问题：

*我申请人是否有设计和性能（DDP）声明，说明设备测试的环境资质等级？*

*二,。环境鉴定试验是否遵循主管当局认为适当的标准（如DO-160）？*

*三,。环境鉴定试验是否适当且足以涵盖与ConOps相关的所有环境条件？*

*四,。如果未按照公认标准进行试验，则试验是否由合格的组织/实体进行，或是否具有执行DO-160类似试验的经验？*

•能否根据运行经验或相关测试结果确定设备在预期/预期UAS环境条件下的适用性？

•可能影响设备适用于预期/预期UAS环境条件的任何限制。

（b） 对于UAS设备只有部分环境认证和/或部分相似性证明和/或完全没有认证的零件的情况，应考虑最低完整性水平。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **不利的操作条件** | |  |  | **诚信水平** |  |
|  | **不适用** | **中等的** | **高的** |
| **OSO#24无人机设计并符合不利环境条件的要求** | 标准 | 不适用 |  | UAS旨在限制环境条件的影响。 | UAS的设计采用主管当局认为适当的环境标准和/或符合主管当局可接受的合规手段。 |
| *评论* | *不适用* |  | *不适用* | *国家航空管理局（NAAs）可以定义他们认为适当的标准和/或遵守方法。SORA附录E将在稍后时间根据NAAs提供的反馈更新，并提供适当标准清单。* |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **不利的操作条件** | |  |  | **保证水平** |  |
|  | **不适用** | **中等的** | **高的** |
| **OSO#24无人机设计并符合不利环境条件的要求** | 标准 | 不适用 |  | 考虑第9节中定义的标准 |  |
| *评论* | *不适用* |  | *不适用* |  |

# *9.   技术OSO的保证水平标准*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | **保证水平** |  |
| **低的** | **中等的** | **高的** |
| **技术OSO** | 标准 | 申请人声明已达到要求的诚信水平1。 | 申请人有证据证明已达到要求的诚信水平。这通常通过测试、分析、模拟2、检查、设计审查或运行经验来完成。 | 合格的第三方验证声称的完整性水平。 |
| *评论* | *1支持性证据可能可用，也可能不可用* | *2 使用模拟时，需要证明模拟中使用的目标环境的有效性。* | *不适用* |

参考文献

[1] W.Moskwa，“普华永道说，2020年世界无人机市场将接近1270亿美元”，彭博社，2016年（见第1、9、10页）。

[2] E.Yağdereli，C.Gemci和A.Z.Aktaş，“自动和无人驾驶车辆的网络安全研究”，《国防建模与仿真杂志》，第12卷，第4期，第369-381页，2015年（第1、15、75页上的引文）。

[3] C.L.Krishna和R.R.Murphy，“无人机网络安全漏洞审查”，2017年IEEE安全、安保和救援机器人国际研讨会（SSRR），IEEE，2017年，第194-199页（第1页，第75页，同上）。[4] E.Vattaparamban、I.Guvenc、A.I.Yurekli、K.Akkaya和S.Uluagac，“智能城市的无人机：网络安全、隐私和公共安全问题”，恩，2016年国际互联网-

*国际无线通信和移动计算会议（IWCMC）*，IEEE，2016年9月，第216-221页（见第1、4、16、75页）。

[5] 陈文华，段子端，董耀东，“基于EKF的导航控制系统中的虚假数据注入”-

trol，“2017年国际无人机系统会议（ICUAS），2017年，第1608-1617页（第1页的引文）。

[6] ，国际民用航空组织（ICAO），2011年（引文第4、7页）。*无人机系统（UAS）*

[7] A.Zolich、T.A.Johansen、K.Cisek和K.Klausen，“海上任务无人机系统架构。设计和硬件描述”，2015年研讨会

*关于无人机系统（RED-UAS）的研究、教育和开发*，IEEE，2015，第342-350页（第4、5、7、8页上的引文）。

[8] S.G.Gupta，D.Ghonge，P.M.Jawandhiya，等，“无人机系统（UAS）综述”，国际计算机工程与技术高级研究杂志（IJARCET）卷，第2卷，2013年（第4、5页上的引文）。

[9] P.Rudol，“通过使用成像传感器提高无人机系统的自主性”，博士。论文，林克平大学电子出版社，2011年（同上，第4页）。

[10] K.Nonami，F.Kendoul，S.Suzuki，W.Wang和D.Nakazawa，自主飞行机器人：无人机和微型飞行器。斯普林格科学与商业媒体，2010年（第5页上的引文）。

[11] 刘志军，D.泰利奥尔，杨立军，何耀勇，韩建军，“基于多模型自适应方法的倾转旋翼无人机过渡控制”，2017年国际无人机系统会议（ICUAS），2017年，第560-566页（第5页上的引文）。

[12] B.Lee，P.Park，C.Kim，S.Yang和S.Ahn，“无人机混合电力推进系统的功率管理”，《机械科学与技术杂志》，第26卷，第8期，2291-22992012页（第5页上的引文）。

185

[13] T.H.Bradley，B.A.Moffitt，D.N.Mavris和D.E.Parekh，“燃料电池驱动飞机的开发和实验表征”，《电源杂志》，第171卷，第2期，第793-801页，2007年（第5页上的引文）。

[14] A.Gong、J.L.Palmer、G.Brian、J.R.Harvey和D.Verstraete，“模拟小型无人驾驶飞机飞行任务中基于燃料电池的混合动力系统的性能”，《国际氢能杂志》，第41卷，第26期，第11418-11426页，2016年（第5页上的引文）。

[15] H González Jorge、M Bueno、J Martínez-Sánchez和P Arias，“用于森林防火的低空长续航太阳能无人驾驶飞机：在Serra do Xures（西班牙）自然公园的应用”，《摄影测量学、遥感和空间信息科学国际档案》，第42卷，第页。2017年第135页（第5页上的引文）。

[16] P.Oettershagen、A.Melzer、T.Mantel、K.Rudin、T.Stastny、B.Wawrzacz、T.Hinzmann、K.Alexis和R.Siegwart，“小型太阳能无人机的永久飞行：

飞行结果、性能分析和模型验证”，2016年IEEE航空航天会议，IEEE，2016年，第1-8页（第5页引文）。

[17] E.Baskaya，G.Manfredi，M.Bronz和D.Delahaye，“用于将无人机集成到空域的灵活开放式体系结构：狗仔队自动驾驶仪系统”，2016年IEEE/AIAA第35届数字航空电子系统会议（DASC），IEEE，2016年，第1-7页（第6页的引文）。

[18] M Bryson和S Sukkarieh，“使用惯性传感器和卫星定位系统的无人机定位”，载于《无人机手册》，斯普林格，2015年，第433-460页（第6页的引文）。

[19] L.Mejias、J.Lai和T.Brugemann，“任务传感器”，载于《无人机手册》，斯普林格，2015年，第385-399页（第6页上的引文）。

[20] M.S.Grewal、L.R.Weill和A.P.Andrews，全球定位系统、惯性导航和集成。约翰·威利父子公司，2007年（第6页上的引文）。

[21]D.Dusha和L.Mejias，“单目GPS/视觉里程计组合导航滤波器的误差分析和姿态可观测性”，《国际机器人学研究杂志》，第31卷，第6期，第714-737页，2012年（第6页上的引文）。

[22]J.R.G.Braga、H.F.de Campos Velho和E.H.Shiguemori，“用于无人机自主导航的激光雷达和非扩展粒子滤波器”，载于《工程应用新兴技术中的计算智能》，斯普林格，2020年，第227-238页（第6页上的引文）。

[23]N.Hallermann和G.Morgenthal，“从航空摄影到桥梁的三维检查”，载于IABSE会议记录，2016年，第8-11页（见第7页）。

[24]I.Colomina和P.Molina，“用于摄影测量和遥感的无人机系统：综述”，ISPRS摄影测量和遥感杂志，第92卷，第79-97页，2014年（见第7页）。

[25]S.Kim和J.Irizarry，“建筑和基础设施环境中无人机运行中的人因绩效”，《工程管理杂志》，第35卷，第6期，第页。2019年4月19日至26日（第7页引述）。

[26]陈绍伟，G.V.纳达里，李易斯，曲春春，刘晓峰，罗梅罗，和库马尔，“斯隆：森林资源清查的语义激光雷达里程计和地图”，IEEE机器人与自动化通讯，第5卷，第2期，第612-6192020页（第7页上的引文）。

[27]郭彦，基于激光雷达的测绘方法、设备和系统，美国专利105787422002年3月（第7页上的引文）。

[28]R.Kestur、S.Omkar和S.Subhash，“用于农药喷洒的无人驾驶系统技术”，载于《21世纪创新害虫管理方法》，斯普林格，2020年，第47-60页（第7页的引文）。

[29]Y.A.Pederi和H.S.Cheporniuk，“无人机和精确农业中监测和作物保护的新技术方法”，2015年IEEE

*国际会议无人机发展的实际问题（APUAVD）*，2015年，第298-301页（第7页上的引文）。

[30]H.Okcu，“无人机系统数据链路和通信系统的操作要求”，《计算机网络进步杂志》，第4卷，第1期，第28-32页，2016年（第8页的引文）。

[31]A Klimkowska、I Lee和K Choi，“无人机用于海洋监测的可能性”，该报告

*国际摄影测量学、遥感和空间信息科学档案馆*，第41卷，p。2016年5月885日（第8页引述）。

[32]，单一欧洲天空Atm研究联合企业（SESAR），2016年11月（见第8、10页的引文）。*欧洲无人机展望研究：释放欧洲价值*

[33]F.Giones和A.Brem，“从玩具到工具：无人机行业技术和创业发展的共同演变”，《商业视野》，第60卷，第6期，第875-884页，2017年（同上，第9、10页）。

[34]G.Thibault和G.Aoude，“公司正在将无人机转变为一种竞争优势”，《哈佛商业评论》，2016年（第9页，同上）。

[35]F.Veroustraete，“无人机在农业中的崛起”，欧共体农业，第2卷，第2期，第325-327页，2015年（第9页，同上）。

[36]M.Kulbacki，J.Segen，W.Knieć，R.Klempous，K.Kluwak，J.Nikodem，J.Kulbacka和A.Serester，“从种植到农业自动化的无人机调查”-

vest，“2018年IEEE第22届智能工程系统国际会议（INES），IEEE，2018年，第000353–000358页（第9页上的引文）。

[37]K.Ghaffarzadeh，“2017-2027年农业机器人和无人机：技术、市场、参与者”，IDTechEx，技术代表，2017年（第9页上的引文）。

[38]，无人机行业洞察，2018年12月（第9页上的引文）。*能源工业中的无人机*

[39]，无人机行业洞察，2019年3月（第10页引述）。*2019-2024年无人机市场规模和预测*

[40]，市场研究未来，2018年7月（cit。*无人机市场研究报告-预测2028年*

第10页）。

[41]，互动分析（见第10页）。*2022年的商用无人机*

[42]M.Huttunen，“u空间概念”，转载自《航空航天法》，第44卷，第1期，第69-89页，2019年（第10、11、14页上的引文）。

[43]E.Baskaya，“利用机器学习对无人机进行故障检测和诊断”，博士。论文，ENAC-2019年国家民用航空学院（见第11页）。

[44]，欧盟航空安全局，2017年5月（第11页的引文）。*2017-05年拟议修正案公告：引入无人机运行监管框架*

[45]J Kamienski和J Semanek，“管制空域中无人机集成的空中交通管制视角”，Promedia Manufacturing，第3卷，第1046-1051页，2015年（第11页上的引文）。

[46]，欧盟航空安全局，2015年10月（第11页的引文）。*2015-10年拟议修正案公告：引入无人机操作监管框架*

[47]，SESAR联合承诺，2017年（第13、14页上的引文）。*U空间：蓝图*

[48]A.Jafarnia Jahromi，S.Daneshmand和G.Lachapelle，“全球导航卫星系统接收器的欺骗对策——当前和未来研究趋势回顾”，欧洲航天局，第4卷，第页。2013年6月6日（同上，第15页）。

〔49〕T. Humphreys，“关于民用无人机和其他系统对民用GPS欺骗的脆弱性的声明”，德克萨斯大学在奥斯丁（2012年7月18日），第1页-第16, 2012页（参见第15, 75, 154页）。

[50]S.-H.Seo，B.-H.Lee，S.-H.Im和G.-I.Jee，“利用伪造GPS信号对无人机进行欺骗的影响”，《定位、导航和计时杂志》，第4卷，第2期，第57-65页，2015年（第15、75页上的引文）。

[51]S.Yunmok、S.Hocheol、K.Dongkwan、P.Youngseok、N.Juhwan、C.Kibum、C.Jungwoo和K.Yongdae，“陀螺传感器上带有有意噪声的摇摆无人机”，第24届USENIX安全研讨会（USENIX Security 15），华盛顿特区：USENIX协会，2015年，第881-896页（第15、75页上的引文）。

[52]陆春云，郭炳国，冯立华，杨亚耀，王建尧，邢春云，“基于短时傅立叶分析控制MEMS陀螺仪输出信号的有意声干扰方法”，2019年第20届国际电子封装技术会议（ICEPT），IEEE，2019年，第1-4页（第15、75页上的引文）。

[53]T.Trippel，O.Weisse，W.Xu，P.Honeyman和K.Fu，“胡桃木：质疑具有声注入攻击的MEMS加速计的完整性”，2017年IEEE欧洲安全与隐私研讨会（EURO&P），IEEE，2017年，第3-18页（第15、75页的引文）。

[54]杜志强、费菲、伊根、徐德明和邓X，“带受损imu的微型飞行器的飞行恢复”，arXiv预印本arXiv:1812.000632018（第15页上的引文）。

[55]M.Crispoltoni，M.L.Fravolini，F.Balzano，S.D&apos;Urso和M.R.Napolitano，“鲁棒飞机IMU传感器故障检测的区间模糊模型”，传感器，第18卷，第8期，第页。2018年第2488页（第16页的引文）。

[56]A.A.Yaseen和M.Bayart，“有故障设备的网络控制系统中的网络攻击检测”，2017年第25届地中海控制和自动化会议（MED），IEEE，2017年，第980-985页（第16页的引文）。

[57]G.Fournier、P.Audren De Kerdrel、P.Cotret和V.Vieture Triem Tong，“无人机杰克：与无人机吻别！”，2017年SSTIC-法国雷恩信息与通信技术安全与安全研讨会，2017年6月，第1-8页（同上，第16、75页）。

[58]，在线（见第16页的引文）。*Mavlink开发者指南*

[59]J.A.Marty，“无人机指挥和控制用mavlink协议的脆弱性分析”，美国空军技术研究所，技术代表，2013年（第16页，同上）。[60]C.Stracquodaine、A.Dolgikh、M.Davis和V.Skormin，“使用实时自动驾驶仪软件分析的无人机系统安全”，2016年国际无人机系统会议（ICUAS），IEEE，2016年，第830-839页（第16页上的引文）。

[61]M.Heiges、R.Bever和K.Carnahan，“如何安全地测试受网络攻击的无人机”，佐治亚理工研究所，技术代表，2015年（同上，第16、75页）。

[62]S.Nas，“安全和安保的定义”，《埃塔海事科学杂志》，第3卷，第2期，第53-54页，2015年（第20页上的引文）。

[63]A.Burns，J.McDermid和J.Dobson，“关于安全和安保的意义”，《计算机杂志》，第35卷，第1期，第3-15页，1992年（第20页上的引文）。

[64]，第1版，无人驾驶系统规则制定联合机构（JARUS），2017年6月（第20页的引文）。*术语表*

[65]Y.Li和F.W.Guldenmund，“安全管理体系：文献综述”，安全科学，第103卷，第94-123页，2018年（第20页上的引文）。

[66]，国际标准化组织，国际电工委员会，ISO/IEC日内瓦，2012年（第20页的引文）。*ISO/IEC 27032:2012–网络安全信息技术安全技术指南*

[67]David Kleidermacher、Mike Kleidermacher和Mike Kleidermacher，嵌入式系统安全。纽斯，2012年（第20页引述）。

[68]L.Piètre Cambacédès和M.Bouissou，“安全和安保工程之间的相互作用”，可靠性工程与系统安全，第110卷，第110-126页，2013年（第20、24-26、40页上的引文）。

[69]D Delves，“国际原子能机构。原子能机构安全术语表：核安全和辐射防护术语。2007年”，维也纳：国际原子能机构，第页。2007年第227页（同上，第20、22页）。

[70]L.Piètre Cambacédès和C.Chaudet，“SEMA参考框架：避免“安全”和“安全”术语的歧义”，《关键基础设施保护国际期刊》，第3卷，第2期，第55-66页，2010年（第20页上的引文）。

[71]S.Kriaa，L.Pietre Cambacedes，M.Bouissou和Y.Halgand，“工业控制系统安全与安保相结合方法的调查”，可靠性工程与系统安全，第139卷，第156-178页，2015年（第20页上的引文）。

[72]C.Raspotnig和A.Opdahl，“比较安全和安保要求的风险识别技术”，《系统与软件杂志》，第86卷，第4期，第1124-1151页，2013年（第20页的引文）。

[73]C.Schmittner、T.Gruber、P.Puschner和E.Schoitsch，“信息安全应用”

故障模式和影响分析（FMEA），“en，计算机安全、可靠性和安全，A.Bondavali和F.Di Giandomenico编辑，第8666卷，斯普林格国际出版社，2014年，第310-325页（第20、41页上的引文）。

[74]D.R.Steve Kremer Ludovic Mé和V.Roca，“网络安全——当前的挑战和Inria的研究方向”，Inria，技术代表，2019年（第20页，同上）。

[75]，SAE国际集团（第22、26页的引文）。*民用飞机和系统开发指南-ARP4754*

[76]，化学工艺安全中心（见第22页的引文）。*过程安全术语表*

[77]、国际标准化组织（ISO）和国际电工委员会（IEC）（第22页的引文）。*ISO 14971:2019医疗器械-风险管理在医疗器械中的应用*

[78]R Ask、Røisli、S Johnsen、M Line、A Ueland、B Hovland、L Groteide、B Birkeland、A Steinback、E Hagelsteen等，过程控制、安全和支持ict系统的信息安全基线要求。isbr，olf104（2006年）（第22页引述）。

[79]R.Kissel，“关键信息安全术语表”，en，国家标准与技术研究所，技术代表NIST IR 7298r2，2013年5月（第22页的引文）。

[80]、国际标准化组织（ISO）和国际电工委员会（IEC）。（同上，第22页）。*ISO/IEC 27000术语表标准*

[81]R.Shirey，“互联网安全术语表，第2版”，RFC 49492007年8月，技术代表，2007年（第22页上的引文）。

[82]M.E.Whitman和H.J.Mattord，《信息安全原则》。圣智学习，2011年（第23页上的引文）。

[83]M.Kabir Querrec，“智能电网控制系统的网络安全：IEC 61850通信网络中的入侵检测”，博士。格勒诺布尔阿尔卑斯大学论文，2017年（第23、25、28页上的引文）。

[84]M.Stamatelatos、W.Vesely、J.Dugan、J.Fragola、J.Minarick和J.Railsback，断层

*航空航天应用树木手册*. 美国宇航局华盛顿特区，2002年（第23页，同上）。

[85]，国际标准化组织（ISO）（第23页的引文）。*Iso/指南73:2009风险管理-词汇*

[86]F.Khan、S.Rathnayaka和S.Ahmed，“过程安全和风险管理的方法和模型：过去、现在和未来”，过程安全和环境保护，第98卷，第116-147页，2015年（第23、32页上的引文）。

[87]P.Kobes，“Zoom sur la norme international e IEC 62443 pour la cybersécuritédes systemémes numériques industriels”，载于塞帕杜斯，2016年（第23、39页上的引文）。

[88]J.Mcdonald，N.Oualha，A.Puccetti，A.Hecker和F.Planchon，“EBIOS在配电变电站ICT使用风险评估中的应用”，2013年IEEE格勒诺布尔会议，IEEE，2013年，第1-6页（第25页引述）。

[89]V.Agrawal，“ISO 27005标准中的信息分类框架”，年

*2017年ieee第四届网络安全和云计算国际会议（cscloud）*，IEEE，2017，第264-269页（第25页上的引文）。

[90]S.Ariyani和M.Sudarma，“ISO/IEC 27005在管理信息系统风险安全分析中的实施”，2016年第6卷第1-6页（第25、27页上的引文）。

[91]R.A.Clothier和R.A.Walker，“无人机系统的安全风险管理”，《无人机手册》，第2229-22752015页（第25页的引文）。

[92]J.Jalouneix、P.Cousinou、J.Couturier和D.Winter，“比较中心和居里公寓的方法”，融洽技巧，第117卷，2009年（第25、26页的引文）。

[93]C.A.Ericson等人，《系统安全的危害分析技术》。约翰·威利父子公司，2015年（同上，第25、32、34、36-38页）。

[94]，EUROCAE，2014年6月（同上，第25页）。*DO-326a/ED-202a：适航安全过程规范*

[95]D.Vasseur，Riskes Industries:复杂性、不确定性和决策性：跨学科的方法。Tec&doc Lavoisier，2006年（第26页上的引文）。

[96]S.Tom，D.Christiansen和D.Berrett，“控制系统补丁管理的推荐实践”，爱达荷州国家实验室（INL），技术代表，2008年（第26页上的引文）。

[97]，法国巴黎皮埃尔塞马尔街30号CLUSIF，75009号（见第26页）。*居里服务费手册*

[98]，无人系统规则制定联合机构（JARUS），2019年1月（同上，第26、66、92、95页）。*SORA附录E——运行安全目标（oso）的完整性和保证水平*

[99]K.D.Mitnick和W.L.Simon，《欺骗的艺术：控制人类的安全因素》。约翰·威利父子公司，2003年（第26页上的引文）。

[100]R.Bell，“IEC 61508简介”，载于ACM国际会议程序系列，2006年第162卷，第3-12页（见第27页的引文）。

[101]，国际电工委员会（IEC），2015年（第27页的引文）。*功能安全对整体安全至关重要-功能安全和iec 61508系列简介*

[102]S.ARP4761，“对机载系统和设备进行安全评估过程的指南和方法”，美国：推进机动性的工程学会陆-海-空和空间，1996年（第27页上的引文）。

[103]，第1版，无人系统规则制定联合机构（JARUS），2017年6月（第27、62、64、66、67、69页上的引文）。*JARUS特定运营风险评估指南（SORA）*

[104]，第2版，无人系统规则制定联合机构（JARUS），2019年10月（见第27、62、66、86、87页）。*Jarus特定运营风险评估指南（SORA）*

[105]B.Leander，A.Čaušević和H.Hansson，“IEC 62443标准在中国的适用性

工业4.0/IIoT，“第14届可用性、可靠性和安全性国际会议记录，2019年，第1-8页（第28页的引文）。

[106]，2014年6月，法国马拉科夫市艾蒂安多莱街102号，邮编92240（同上，第28页）。*适航安全工艺规范ed-202/do-326*

[107]J.P.朱亚斯、J.L.鲁尔、D.布克、O.科尔比、M.加涅、M.哈赞、G.莫林、C.皮诺、L.普林、P.萨塞维尔、C.乔利维和M.图布尔，梅哈里概览，法国信息俱乐部（CLUSIF），2010年4月（第28页上的同前）。

[108]，法国信息博物馆俱乐部（CLUSIF），摩加多街11号，巴黎，2011年，75009年（见第28页）。*梅哈里危机分析基础发展指南*

[109]E.Kelling、M.Friedewald、T.Leimbach、M.Menzel、P.Säger、H.Seudié和B.Weyl，“电子安全相关用例的规范和评估”，电子安全车辆入侵保护应用项目，技术代表，2009年12月（第28页上的引文）。

[110]S.Idrees、Y.Roudier、M.Friedewald、T.Leimbach、F.Andreas、G.Sigrid、H.Olaf、R.Roland、R.Matthias、B.Henrik、A.Ludovic、P.Renaud、P.Gabriel、R.Alastair、W.David和W.Benjamin，“基于黑暗面场景的车载网络安全要求”，EVITA，技术代表，2009年（第28页同上）。

[111]，产品质量研究所，2015年5月（第29页上的引文）。*培训指南：危险与可操作性分析（HAZOP）*

[112]J.Dunjó，V.Fthenakis，J.A.Vílchez和J.Arnaldos，“危险与可操作性（hazop）分析，文献综述”，危险材料杂志，第173卷，第1-3期，第19-32页，2010年（第29页上的引文）。

[113]D.P.Nolan，《流程工业的安全和安保审查：HAZOP、PHA、假设和SVA审查的应用》。威廉·安德鲁，2011年（同上，第29页）。

[114]M.Sallak，C.Simon和J.-F.Aubry，“确定安全完整性水平的模糊概率方法”，IEEE模糊系统交易，第16卷，第1期，第239-248页，2008年（同上，第29-32页）。

[115]A.E.Summers，“分配目标安全完整性水平的技术”，ISA交易，第37卷，第2期，第95-104页，1998年（同上，第30、31页）。

[116]A.A.Baig，R.Ruzli和A.B.Buang，“使用故障树分析的可靠性分析：综述”，《国际化学工程与应用杂志》，第4卷，第3期，第页。2013年第169页（第32页上的引文）。

[117]J.B.Dugan，S.J.Bavuso和M.A.Boyd，“容错计算机系统的动态故障树模型”，IEEE可靠性事务，第41卷，第3期，第363-377页，1992年（第33页上的引文）。

[118]H.Boudali，A.Nijmeijer和M.I.Stoelinga，“Dftsim：扩展动态故障树的模拟工具”，2009年春季模拟多冲突会议记录，Citeseer，2009年，第1-8页（见第33页）。

[119]G.Merle，J.-M.Roussel和J.-J.Lesage，“基于结构功能的动态故障树定量分析”，质量与可靠性工程国际，第30卷，第1期，第143-156页，2014年（第33页上的引文）。

[120]G.Merle，J.-M.Roussel，J.-J.Lesage，V.Perchet和N.Vayatis，“基于结构功能耦合和蒙特卡罗模拟的动态故障树定量分析”，质量与可靠性工程国际，第32卷，第1期，第7-18页，2016年（第33页上的引文）。

[121]H.Tanaka，L.Fan，F.Lai和K Toguchi，“基于模糊概率的故障树分析”，IEEE可靠性交易，第32卷，第5期，第453-457页，1983年（第33页上的引文）。

[122]U.Hauptmanns，“利用频率和概率范围对工艺装置安全进行半定量故障树分析”，《工艺工业损失预防杂志》，第17卷，第5期，第339-345页，2004年（第33页上的引文）。

[123]R.Ferdous，F.Khan，B.Veitch和P.R.Amyotte，“计算机辅助模糊故障树分析方法”，过程安全与环境保护，第87卷，第4期，第217-226页，2009年（第33页上的引文）。

[124]M.Yazdi，F.Nikfar和M.Nasrabadi，“利用模糊故障树分析进行故障概率分析”，《国际系统保证工程与管理杂志》，第8卷，第2期，第1177-1193页，2017年（第33页上的引文）。

[125]J Andrews，“故障树分析教程”，载于《第16届国际系统安全会议论文集》，拉夫伯勒，1998年（同上，第33页）。

[126]J.D.Andrews和S.J.Dunnett，“使用二元决策图的事件树分析”，IEEE可靠性交易，第49卷，第2期，第230-238页，2000年（第34页上的引文）。

[127]，美国核管理委员会，1975年（第34页的引文）。*反应堆安全研究：美国商业核电厂事故风险评估*

[128]A.de Ruijter和F.Guldenmund，“领结法：综述”，安全科学，第88卷，第211-218页，2016年（同上，第35、36页）。

[129]S.Sklet，“安全屏障：定义、分类和性能”，《流程工业损失预防杂志》，第19卷，第5期，第494-506页，2006年（第35页上的引文）。

[130]A.Badredine，T.B.Romdhane，M.A.B.HajKacem和N.B.Amor，“在领结图中实施预防性和保护性屏障的新多目标方法”，《流程工业损失预防杂志》，第32卷，第238-253页，2014年（第36页上的引文）。

[131]R.Ferdous，F.Khan，R.Sadiq，P.Amyotte和B.Veitch，“领结分析中不确定信息的处理和更新”，《流程工业损失预防杂志》，第25卷，第1期，第8-19页，2012年（第36页上的引文）。

[132]O.Salvi和B.Debray，“ARAMIS的全球观点，SEVESO II指令框架下的行业风险评估方法”，《危险品杂志》，第130卷，第3期，第187-199页，2006年（第36页上的引文）。

[133]C.Jacinto和C.Silva，“使用蝴蝶结表示法的职业风险半定量评估”，《安全科学》，第48卷，第8期，第973-979页，2010年（第36页上的引文）。[134]N.Paltrinieri，F.Khan，P.Amyotte和V.Cozzani，“风险管理的动态方法：适用于hoeganaes金属粉尘事故”，过程安全与环境保护，第92卷，第6期，第669-6792014页（第36页上的引文）。

[135]R.Ferdous，F.Khan，R.Sadiq，P.Amyotte和B.Veitch，“使用蝴蝶结图分析不确定性下的系统安全和风险：创新方法”，过程安全与环境保护，第91卷，第1-2期，第1-18页，2013年（第36页上的引文）。

[136]N.J.Duijm，“作为安全管理工具的安全屏障图”，可靠性工程与系统安全，第94卷，第2期，第332–341页，2009年（第36页上的引文）。

[137]，国际标准化组织，2000年（第36页上的引文）。*ISO 17776:2000石油和天然气工业-海上生产装置-危险识别和风险评估工具和技术指南*

[138]J.L.Rouvroye和E.G.van den Bliek，“比较安全分析技术”，可靠性工程与系统安全，第75卷，第3期，第289-2942002页（第36、38页上的引文）。

[139]M.Bouissou和J.-L.Bon，“结合故障树和马尔可夫模型优点的新形式主义：布尔逻辑驱动的马尔可夫过程”，可靠性工程与系统安全，第82卷，第2期，第149-163页，2003年（第36页上的引文）。

[140]H.-C.Liu，L.Liu和N.Liu，“失效模式和影响分析中的风险评估方法：文献综述”，专家系统与应用，第40卷，第2期，第828-838页，2013年（第37页上的引文）。

[141]P.David，V.Idasiak和F.Kratz，“实现设计和可靠性分析之间的更好互动：源自UML/SysML模型的FMEA”，ESREL 2008和第17届SRA-EUROPE年会论文集，第3卷，2008年9月（第37页上的引文）。

[142]S.Kmenta和K.Ishii，“采用元行为建模进行产品和控制并行设计的高级FMEA”，1998年ASME设计工程技术会议论文集，1998年（第38页，同上）。

[143]M Nicholson和J McDermid，“为复杂系统扩展PSSA”，载于2003年第21届国际系统安全会议（ISSC）论文集（同上，第39页）。

[144]N.Kube和B Singer，“安全保证水平：安全的SIL方法”，年

*第二届SCADA安全科学研讨会（S4）会议纪要*，2008年（同上，第39页）。

[145]J.D.Gilsinn和R.Schierholz，“安全保证水平：描述安全需求的向量方法”，NIST，2010年（第39页上的引文）。

[146]R.Winther，O.-A.Johnsen和B.A.Gran，“使用HAZOP对安全关键系统进行安全评估”，载于计算机安全、可靠性和安全国际会议，Springer，2001年，第14-24页（第40页上的引文）。

[147]Wei，Y.Matsubara和H.Takada，“基于Hazop的嵌入式系统安全分析：开放的案例研究”，2015年第七届电子、计算机和人工智能国际会议（ECAI），IEEE，2015年，SSS-1（第40页上的引文）。

[148]T.Srivatanakul，J.A.Clark和F.Polack，“有效的安全需求分析：Hazop和用例”，信息安全国际会议，斯普林格，2004年，第416-427页（第40页上的引文）。

[149]B.Daruwala、S.Mandujano、N.K.Mangipudi和H.-c。Wong，“使用HazOP对硬件和软件产品进行威胁分析”，《国际计算和信息科学会议记录》，2009年，第446-453页（同上，第40页）。

[150]B.Schneier，“安全威胁建模”，Dobb博士的期刊，1999年（第40页，同上）。

[151]V.Nagaraju，L.Fiondella和T.Wandji，“网络风险管理的故障和攻击树建模与分析调查”，2017年IEEE国土安全技术国际研讨会（HST），IEEE，2017年，第1-6页（第40页上的引文）。

[152]O.Henniger、L.Apvrille、A.Fuchs、Y.Roudier、A.Ruddle和B.Weyl，“汽车车载网络的安全要求”，2009年第九届智能运输系统电信国际会议，（ITST），IEEE，2009年，第641-646页（第40、75页的引文）。

[153]Xu J.Xu，K.K.Venkatasubramanian和V.Sfyrla，“可互操作医疗设备的系统攻击树生成方法”，2016年IEEE系统年会（SysCon），2016年，第1-7页（第40页上的引文）。

[154]E.J.Byres、M.Franz和D.Miller，“利用攻击树评估SCADA系统中的漏洞”，载于《国际基础设施生存能力研讨会论文集》，Citeseer，2004年，第3-10页（同上，第40页）。

[155]K.Edge、R.Raines、M.Grimaila、R.Baldwin、R.Bennington和C.Reuter，“利用攻击和保护树分析网上银行系统的安全性”，2007年第40届夏威夷国际系统科学年会（HICSS&apos;07），IEEE，2007年，144b–144b（第40页上的引文）。

[156]M.Ekstedt和T.Sommestad，“网络安全分析的企业架构模型”，2009年IEEE/PES电力系统会议和博览会，IEEE，2009年，第1-6页（第40页的引文）。

[157]B.Kordy，S.Mauw，M.Melissen和P.Schweitzer，“攻击-防御树和两人二进制零和扩展形式博弈是等价的”，载于《安全决策和博弈论国际会议》，斯普林格，2010年，第245-256页（第40页同上）。

[158]A.Jürgenson和J.Willemson，“使用估计参数值处理多参数攻击树”，国际安全研讨会，Springer，2007年，第308-319页（第40页的引文）。

[159]R.R.Yager，“OWA树及其在使用攻击树进行安全建模中的作用”，信息科学，第176卷，第20期，第2933-29592006页（第40页上的引文）。

[160]S.Garg和G.S.Aujla，“使用博弈论和模糊逻辑概念对vanet进行风险和安全评估的基于攻击树的综合框架”，《网络智能新兴技术杂志》，第6卷，第2期，第247-252页，2014年（第40页上的引文）。

[161]J.O.Aagedal、F.Den Braber、T.Dimitrakos、B.A.Gran、D.Raptis和K.Stern，“基于模型的风险评估以提高企业安全性”，诉讼中。第六届国际企业分布式对象计算，IEEE，2002年，第51-62页（第41页上的引文）。

[162]A.Gorbenko、V.Kharchenko、O.Tarasyuk和A.Furmanov，“F（I）MEA web服务分析和可靠性保证技术”，在《复杂容错系统的严格开发》中，Springer，2006年，第153-167页（第41页的引文）。

[163]C.Schmittner，Z.Ma和P.Smith，“智能和协作车辆安全和安保分析的FMVEA”，载于计算机安全、可靠性和安保国际会议，斯普林格，2014年，第282-288页（第41页上的引文）。

[164]J.B.Bowles和W.Hanczaryk，“威胁影响分析：将FMEA应用于计算机系统威胁建模”，2008年年度可靠性和可维护性研讨会，IEEE，2008年，第463-468页（第41页的引文）。

[165]M.Rebekah，“评估工程环境中的网络风险：拟议的框架和方法”，SANS研究所，技术代表，2016年（同上，第41页）。

[166]A.E.Tucci，“海上运输系统中的网络风险”，载于《网络物理安全》，斯普林格，2017年，第113-131页（第41页的引文）。

[167]P.Harry，“网络安全蝴蝶结（0x01）：如何打网络蝴蝶结”，PI Square，技术代表，2016年（第41页上的引文）。

[168]K.Bernsmed、C.Frøystad、P.H.Meland、D.A.Nesheim和Ø。J.Rødseth，“用蝴蝶结图可视化网络安全风险”，在安全图形模型国际研讨会上，斯普林格，2017年，第38-56页（第41页上的引文）。

[169]H.Abdo，“风险分析中的不确定性处理：安全与安保的结合”，论文，格勒诺布尔阿尔卑斯大学，2017年12月（同上，第41、43页）。

[170]N.Ye，Y.Zhang和C.M.Borror，“网络攻击检测的马尔可夫链模型的鲁棒性”，IEEE可靠性交易，第53卷，第1期，第116-123页，2004年（第42页上的引文）。

[171]C.Xiaolin，T.Xiaobin，Z.Yong和X.Hongsheng，“基于马尔可夫博弈论的网络信息系统风险评估模型”，2008年计算机科学与软件工程国际会议，IEEE，2008年第3卷，第1057-1061页（第42页上的引文）。

[172]V.Lakhno，D.Kasatkin和A.Blozva，“基于博弈论和马尔可夫过程的信息系统智能城市网络安全建模”，2019年

*IEEE国际科学实用会议信息通信、科学与技术问题（PIC S&T）*，IEEE，2019年，第497-501页（第42页的引文）。

[173]L.Piètre Cambacédès和M.Bouissou，“超越攻击树：布尔逻辑驱动马尔可夫过程（BDMP）的动态安全建模”，2010年欧洲可靠计算会议，IEEE，2010年，第199–208页（第42页上的引文）。

[174]L.Piètre Cambacédès和M.Bouissou，“使用BDMP进行攻击和防御建模，”

在计算机网络安全的数学方法、模型和体系结构国际会议上，斯普林格，2010年，第86-101页（第42页的引文）。

[175]J.P.McDermott，“攻击网络渗透测试”，2000年新安全范例研讨会论文集，2001年，第15-21页（第42页的引文）。

[176]周S，秦Z，张F，张X，陈W.和刘杰，“基于有色petri网的攻击建模”，在粗糙集，模糊集，数据挖掘和粒度软计算国际研讨会上，Springer，2003，第715-718页（第42页上的引文）。

[177]傅耀勇，朱建军，高树森，“基于Petri网的CPS信息安全风险评估系统”，2017年IEEE第二届网络空间数据科学国际会议（DSC），IEEE，2017年，第541-548页（第42页上的引文）。

[178]周建军，G.雷尼尔和张磊，“化学过程安全背景下基于Petri网的攻击时间分析”，计算机与化学工程，第130卷，p。2019年106546月（见第42页的引文）。

[179]E.Lisova，I.Šljivo和A.Čaušević，“安全和安保共同分析：系统文献综述”，《IEEE系统杂志》，第13卷，第3期，第2189-2200页，2018年（第43页上的引文）。

[180]F.Reichenbach，J.Endresen，M.M.Chowdhury和J.Rossebø，“联合安全和安全风险分析的实用方法”，2012年IEEE第23届软件可靠性工程国际研讨会，IEEE，2012年，第239-244页（第43页上的引文）。

[181]S.Plósz，C.Schmittner和P.Varga，“工业协作自动化系统的安全与安全分析相结合”，载于计算机安全、可靠性和安全国际会议，斯普林格，2017年，第187-198页（第43页上的引文）。

[182]I.N.Fovino，M.Masera和A.De Cian，“在故障树中集成网络攻击”，可靠性工程与系统安全，第94卷，第9期，第1394-1402页，2009年（第43页上的引文）。

[183]M.Puys，M.-L.Potte和A.Khaled，“针对工业系统的应用攻击场景的生成”，发表于《安全基础与实践国际研讨会》，斯普林格，2017年，第127-143页（第43页上的引文）。

[184]，附件A：收集和呈现特定无人机操作的系统和操作信息指南，无人系统规则制定联合机构，2017年（第47、98、101页上的引文）。*关于索拉的Juras指南*

[185]，2015年9月，法国马拉科夫市艾蒂安多莱街102号，邮编92240（同上，第53页）。*适航安全方法和注意事项*

[186]O.Gadyatskaya、R.Jhawar、P.Kordy、K.Lounis、S.Mauw和R.Trujillo Rasua，“用于实际安全评估的攻击树：攻击场景的排序，具有

ADTool 2.0，“在系统的定量评估中，G.Agha和B.Van Houdt编辑，Cham:Springer国际出版，2016年，第159-162页（第55页的引文）。

[187]F.Nikodem、A.Bierig和J.S.Dittrich，“与普通民用航空风险评估相比，无人机监管的新的具体运营风险评估方法”，DLRK 2018，2018年（第62页的引文）。

[188]，欧盟航空安全局（EASA），2019年10月（见第62页的引文）。*委员会实施条例（eu）2019/947的可接受合规手段（AMC）和指导材料（GM）*

[189]，欧盟航空安全局（EASA），2015年12月（第62、67页上的引文）。*无人机操作监管框架介绍*

[190]，欧盟航空安全局（EASA），2015年10月（第67页上的引文）。*A-NPA 2015-10：引入无人机操作监管框架*

[191]C.Pauner，I.Kamara和J.Viguri，“无人机。隐私和数据保护领域的当前挑战和标准化解决方案”，2015年《国际电联万花筒：信息社会的信任》（K-2015），2015年，第1-7页（同上，第67、69、71页）。

[192]S.Winkler，S.Zeadally和K.Evans，“隐私和民用无人机的使用：进一步监管的必要性”，IEEE安全与隐私，第16卷，第5期，第72-802018页（第67页的引文）。

[193]志彦，傅志忠，孙X.孙和余J.Yu，“无人机的安全和隐私问题：调查”，移动网络和应用，第95-101页，2019年（第69页上的引文）。

[194]R.L.Finn、D.Wright和M.Friedewald，“七种类型的隐私”，载于《欧洲数据保护：成年》，斯普林格，2013年，第3-32页（第69页的引文）。

[195]Z.Li，C.Gao，Q.Yue和X.Fu，“通过调节高度和有效载荷实现无人机隐私”，2019年国际计算、网络和通信会议（ICNC），2019年，第562-566页（第69页的引文）。

[196]J.Villasenor，“从上面观察：无人驾驶飞机系统和隐私”，《哈佛法律公共政策杂志》，2013年（同上，第69页）。

[197]S.Park和K.Lee，“制定个人无人机侵犯隐私的标准，”

2017年平台技术与服务国际会议（PlatCon），2017年，第1-7页（第69页和第71页的引文）。

[198]M.Bonetto，P.Korshunov，G.Ramponi和T.Ebrahimi，“基于微型无人机的视频监控中的隐私”，2015年第11届IEEE自动人脸和手势识别（FG）国际会议和研讨会，第04卷，2015年，第1-6页（第69、71、72页上的引文）。

[199]R.F.Babiceanu、P.Bojda、R.Seker和M.A.Alghumgham，“机载UAS可视隐私保护系统”，2015年综合通信、导航和监视会议（ICNS），2015年，第1-8页（第69页上的引文）。

[200]P.Blank、S.Kirrane和S.Spiekermann，“无人机系统的隐私意识限制区域”，IEEE安全隐私，第16卷，第2期，第70-79页，2018年（第70、72页上的引文）。

[201]，英国安全工业协会（BSIA），2014年7月（第71页的引文）。*cctv监控系统的规划、设计、安装和运行。实务守则及相关指引*

[202]A.Y.Javaid，W.Sun，V.K.Devabhaktuni和M.Alam，“无人机系统的网络安全威胁分析和建模”，2012年IEEE国土安全技术会议（HST），IEEE，2012年，第585-590页（第75页上的引文）。[203]D.Davidson、H.Wu、R.Jellinek、V.Singh和T.Ristenpart，“利用传感器输入欺骗攻击控制无人机”，2016年第10期（第75页的引文）。*USENIX进攻性技术讲习班(胡特16)*

[204]C.Capitán、J.Capitán、A.R.Castano和A.Ollero，“基于无人机媒体制作应用的SORA方法的风险评估”，2019年国际无人机系统会议（ICUAS），IEEE，2019年，第451-459页（第84、90页的引文）。

〔205〕，布里斯托大学多靶子计划，第2017卷（第84页）。*可交付成果d2.1：多无人机介质生产要求*

[206]R.Chevalier、M.Villatel、D.Plaquin和G.Hiet，“基于协处理器的行为监控：用于检测针对系统管理模式的攻击，”

2017年第33届年度计算机安全应用会议记录，第399-411页（第106页上的引文）。

[207]X.阮，平台嵌入式安全技术披露。《斯普林格自然》，2014年（第106页上的引文）。

[208]S.Krishnamurthy，J.R.O&apos;donoghue和N.Bhatia，《在没有内部非易失性存储器的设备中提供固件版本防回滚保护的方法》，美国专利99106592018（第106页上的引文）。

[209]P.Raju，“gps基础”，卫星遥感和GIS在农业气象学中的应用，P。第121页，2004年（同上，第152页）。

[210]E.Kaplan和C.Hegarty，《理解GPS：原理和应用》。Artech house，2005年（第152页引述）。

[211]M.Ahmad、M.A.Farid、S.Ahmed、K.Saeed、M.Asharf和U.Akhtar，“GPS欺骗的影响和检测及反欺骗对策”，2019年第2期

*国际计算、数学和工程技术会议（iCoMET）*，IEEE，2019年，第1-8页（第153页引述）。

[212]A.Jafarnia Jahromi，A.Broumandan，J.Nielsen和G.Lachapelle，“全球定位系统对欺骗威胁的脆弱性和反欺骗技术的回顾”，国际导航与观测杂志，2012年第卷（第153页上的引文）。

[213]M.L.Psiaki和T.E.Humphreys，“全球导航卫星系统欺骗和检测”，IEEE会议记录，第104卷，第6期，第1258-1270页，2016年（第154页上的引文）。

参考书目

[214]温H.Wen，P.Y.-R.Huang，J.Dyer，A.Archinal和J.Fagan，“GPS信号欺骗的对策”，载于ION GNSS，2005年第5卷，第13-16页（第154页上的引文）。

[215]D.Shepard，“接收器对欺骗攻击的响应特征”，博士。毕业论文，得克萨斯大学奥斯汀分校，第2011页（第154页）。

[216]A.Jovanovic，C.Botteron和P.-A.Fariné，“针对全球导航卫星系统接收器的欺骗攻击的多测试检测和保护算法”，2014年IEEE/离子位置、位置和导航研讨会计划2014年，IEEE，2014年，第1258-1271页（第154页上的引文）。

[217]C.E.McDowell，使用数字空间置零的GPS欺骗和中继器缓解系统，美国专利7250903，2007（第154页上的引文）。

[218]P.Y.Montgomery，“接收器自主欺骗检测：多天线接收器防御便携式民用GPS欺骗的实验结果”，无线电导航实验室会议记录，2011年（第154页，同上）。

[219]J.Nielsen，A.Broumandan和G.Lachapelle，“单天线手持接收机的GNSS欺骗检测”，导航，第58卷，第4期，第335-344页，2011年（第154-155页上的引文）。

[220]Qiao，Yu.Zhang和X.Du，“小型无人机基于视觉的GPS欺骗检测方法”，2017年第13届计算智能与安全国际会议（CIS），IEEE，2017年，第312-316页（第154页上的引文）。

[221]G Panice、S.Luongo、G.Gigante、D.Pascarella、C.Di Benedetto、A.Vozella和A.Pescapè，“基于支持向量机的无人机GPS欺骗攻击检测方法”，2017年第23届国际自动化与计算会议（ICAC），IEEE，2017年，第1-11页（第155页的引文）。

[222]冯志强，关N.关M.吕，刘W.刘，邓Q.邓，刘X.刘和易W.Yi，“使用车载运动传感器的有效无人机劫持检测”，载于2017年欧洲设计、自动化和测试会议展览（日期），IEEE，2017年，第1414-1419页（第155页上的引文）。

[[1]](" \l "_ftnref1" \o ")没有设备或通常已经找到的东西

[[2]](" \l "_ftnref2" \o ")容易买到的东西，但通常还不是普通人所拥有的东西

[[3]](" \l "_ftnref3" \o ")买不到但需要组装/建造的东西

[[4]](" \l "_ftnref4" \o ")需要少量资源来组装的特殊设备

[[5]](" \l "_ftnref5" \o ")Sogilis公司的一家分公司正在参与CEDSO项目（CErfiried无人机安全操作系统），以开发一种经过认证的UAS，用于在与SAIL VI相对应的市区内进行操作