

**无人机系统的网络安全风险评估**

Trung Duc Tran

引用这个版本:

Trung Duc Tran.无人机系统的网络安全风险评估。自动化。格勒诺布尔阿尔卑斯大学校址[2020-。.]2021年。英语。NNT: 2021GRALT004.电话: 03200719v2

**电话: 03200719**

**Https://hal.archives-ouvertes.fr/tel-03200719v2**

在2021年6月1日提交

**HAL 是一个多学科的开放存取档案馆，用于存储和传播科学研究文件，无论这些文件是否发表。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。**

多学科开放档案馆 HAL 是为了存放和传播法国或外国教育机构和研究机构、公共或私人实验室发布或未发布的高水平科学研究文件。



论文



为了获得等级



法国格勒诺布尔阿尔卑斯大学(université DE GRENOBLE ALPES)博士



特色产品: 自动化产品



部长停职: 2016年5月25日



由



TRAN Trung Duc



论文由阿尔卑斯格勒诺布尔大学教授 Jean-Marc THIRIET 共同指导



Nicolas MARCHAND，CNRS，GIPSA-lab 和 Amin EL MRABTI，société Sogilis 的研究主管



准备好了



格勒诺布尔实验室图片自动假释信号(Gipsa-lab)



在电子、电技术、自动化(Automatique)、信号处理(EEATS)博士学位



无人机系统的网络安全风险评估



2021年2月2日，在由以下人士组成的陪审团面前，这些观点得到了公开支持:



玛丽-劳拉 · 波特



格勒诺布尔阿尔卑斯大学教授，陪审团主席 Mireille BAYART



里尔大学教授，报告员



弗雷德里克 · 克拉茨



卢瓦尔中心国立应用科学学院教授，报告员



Didier THEILLIOL



洛林大学教授，检查员 Guillaume HIET

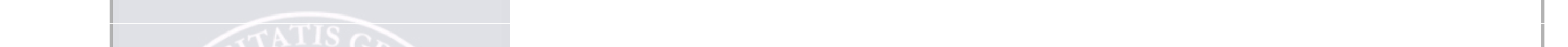


高等教育中心会议主任，检查员 Eric GAILLARD



负责技术和操作，Star Engineering，examiner

Amin EL MRABTI



Sogilis 公司负责研发，尼古拉 · 马尔昌德(Nicolas MARCHAND)

法国国家科学研究中心主任，论文主任

Jean-Marc THIRIET



格勒诺布尔阿尔卑斯大学教授，研究主任

今天，由无人机组成的系统(无人机系统或 UAS)的操作数量的增长引起了公众对网络安全问题的关注。因此，必须考虑到这一方面，因此，我们建议制定方法，以便在无人机发展过程中解决这些问题。这个问题是我们研究的核心。这篇论文在这方面提出了两个重要的贡献。第一个是一种以加强现有无人机(或概念)的网络安全系统为中心的方法。这种方法为使用者提供了一个分析无人机的”工作流程”，确定可能的攻击方案和采取的反措施。我们称这种方法为“面向网络安全的系统风险管理”。第二种方法是以操作为中心，它从系统概念的初始阶段就考虑了网络安全问题。这种方法被认为是“特定操作风险评估”(SORA)方法的延伸版本。这一选择的原因是，SORA 是评估无人机”特定”操作风险的一种参考方法。SORA 的方法仅仅关注于安全，而忽视了网络安全，我们的扩展模块就是为了弥补这一缺陷。我们的扩展方法被称为“安全和网络安全特定操作风险评估”(英文名为 SORA-C2S)。在这种方法的基础上，我们建立了一个 Web 工具，帮助用户以半自动的方式评估风险，包括功能安全和网络安全的两个方面。这篇论文被写入了 Sogilis 公司和 gipsa 实验室的合作框架中。

关键词: 网络安全，风险评估，无人机系统，SORA，特定类别。

GIPSA-lab，11 Rue des mathematiques

法国圣马丁德赫尔38400号

摘要: 如今，无人机系统(UAS)操作数量的增加引起了公众对网络安全问题的关注。因此，在无人机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。这篇论文有两个重要贡献。首先，我们提出了一个以系统为中心的方法论，以加强现有(或设计)无人机的网络安全。这种方法为用户提供了一个工作流来分析 UAS，识别可能的攻击场景，并确定合适的对策。我们称之为“系统网络安全风险管理”。其次，我们提出了一个以操作为中心的方法论，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 是一种广为人知的方法，用于评估“特定”类别下的无人机操作风险。然而，目前阶段的 SORA 方法只关注安全，忽略了网络安全。我们的扩展模块完成了这个缺失的部分。我们将我们的扩展方法称为安全和网络安全特定操作风险评估(SORA-C2S)。基于这种方法，我们建立了一个基于网络的工具，帮助用户进行半自动的风险评估。本论文是 SOGILIS 公司和 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-lab，11 Rue des mathematiques

法国圣马丁德赫尔38400号

目录

|  |  |  |
| --- | --- | --- |
| 引言 | | 1 |
| 1无人驾驶飞机系统及相关网络安全问题 | | 3 |
| 1.1 | 定义..。 | 4 |
| 1.2 | 系统描述..。 | 4 |
| 1.3 | 无人机市场和应用。 | 9 |
| 1.4 | 无人机进入空域。 | 10 |
| 1.5 | 网络安全问题。 | 14 |
| 1.6 | 结论。 | 17 |
| 2安全与保安/网络安全的比较 | | 19 |
| 2.1 | 引言... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 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 | 安全和安保的综合方法。 | 43 |
| 2.8 | 结论。 | 43 |
| 3系统网络安全风险管理 | | 45 |
| 3.1 | 引言... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 46 |
| 3.2 | 提议的方法..。 | 46 |
| 3.3 | 案例分析。 | 53 |
| 3.4 | 结论。 | 60 |
|  | i |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 二 |  |  | 目录 | |
| 4 | 操作风险评估: 从安全到网络安全 | |  | 61 |
|  | 4.1 | 引言... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | . . . . | 62 |
|  | 4.2 | 对 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 | 危害扩展: 隐私危害的 SORA。 | . . . . | 69 |
|  | 4.5 | 威胁扩展: 新的网络安全威胁 SORA。 | . . . . | 74 |
|  | 4.6 | 一个基于网络的扩展 sora 风险评估工具。 | . . . . | 79 |
|  | 4.7 | 结论。 | . . . . | 81 |
| 5 | 扩展的 SORA 方法说明 | |  | 83 |
|  | 5.1 | 引言... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | . . . . | 84 |
|  | 5.2 | 我们的方法与 MULTIDRONE 84项目中使用的方法的比较 | | |
|  | 5.3 | 其他案例研究的应用。 | | 90 |
|  | 5.4 | 使用扩展的 SORA 方法进行系统开发 | . . . . | 97 |
|  | 5.5 | 结论。 | ... 107 | |
| 全球结论和展望 | | |  | 109 |
| A | 网络安全运作目标 | |  | 113 |
| B | 网络工具手册 | |  | 121 |
|  | B. 1 | 一般资料页。 | . . 121 | |
|  | B. 2 | 地面风险等级(GRC)的确定。 | . . 122 | |
|  | B. 3 | 航空风险等级(ARC)确定... ... ... ... ... ... ... ... ... ... ... ..。 | . . 124 | |
|  | B. 4 | 隐私风险等级(PRC)的确定... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | . . 127 | |
|  | 乙. 5 | 网络安全易受影响等级(OCSL)的确定。 | . . 128 | |
|  | B. 6 | 结果..。 | . . 130 | |

C 风险管理结果131

|  |  |  |  |
| --- | --- | --- | --- |
| 目录 | | | (三) |
|  | 丙. 1 | 故障..。 | . . . . . 131 |
|  | C. 2 | 网络安全要求。 | ... 132 |
|  | 丙三 | 风险等级。 | ... 137 |
|  | C. 4 | 攻击树。 | ... 140 |
| D | GPS 欺骗与对策 | | 151 |
|  | D. 1 | 全球定位系统基础。 | ... 152 |
|  | D. 2 | 最先进的反制手段。 | . . . . . 154 |
| E | 原有 SORA 方法中的操作安全目标 | | 157 |
| 参考书目 | | | 200 |

图表列表

|  |  |  |
| --- | --- | --- |
| 1.1 | 无人机系统架构。 | 4 |
| 1.2 | 从左到右: 固定翼，旋转翼，飞艇和扑翼 |  |
|  | 机身。 | 5 |
| 1.3 | 三种类型的无人机操作。 | 11 |
| 1.4 | U 太空插图[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 | 故障树分析的例子[125] ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 33 |
| 2.6 | 事件树图的例子[126] ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 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 | 攻击树木建造工作流程... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 49 |
| 3.4 | 无人机的架构。 | 54 |
| 3.5 | 完整的攻击树与故障2有关-完整性..。 | 56 |
| 3.6 | 攻击场景分布到不同的目标部件。 | 58 |
| 3.7 | 风险场景在不同目标部件和风险水平上的分布 | 59 |
| 4.1 | 以蝴蝶结图表示的 SORA 方法论的风险模型。 | 63 |
| 4.2 | 根据 SORA [103] ，地面和空中致命伤害的可能性。 | 64 |
| 4.3 | 简化风险评估程序... ... ... ... ... ... ... ... ... ... ... ..。 | 65 |
|  | v |  |

|  |  |  |
| --- | --- | --- |
| Vi | 图表列表 | |
| 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 | 申请书概述。 | 79 |
| 4.10 | 有些人需要信息..。 | 80 |
| 4.11 | 2D-SAIL 的结果页面... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 81 |
| 5.1 | 送货行动..。 | 92 |
| 5.2 | 建议的方法，以整合扩展的 SORA 分析到发展 |  |
|  | 行动过程。 | 97 |
| 5.3 | UAS 行动..。 | 99 |
| 5.4 | 操作音量102 | |
| 5.5 | 系统架构... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... 104 | |
| 5.6 | 地面站105 | |
| 5.7 | 在开发过程中提出的两种方法... ... ... ... ... ... ... 110 | |
| B. 1 | 一般资料页... 121 | |
| B. 2 | 计算内在 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 | |
| 乙. 5 | 计算初始 ARC 的信息... ... ... ... ... ... ... ... ... ... ... ... 125 | |
| B. 6 | 减少 ARC 的缓解方案... ... ... ... ... ... ... ... ... ... ... ... ... 126 | |
| B. 7 | 计算初始中华人民共和国的信息... ... ... ... ... ... ... ... ... ... 127 | |
| B. 8 | 摄像头特征127 | |
| B. 9 | 计算 OCSL 的信息... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... 129 | |
| B. 10 | 根据 GRC 和 ARC 值计算的 SAIL... ... ... ... ... ... ... ... ... ... 130 | |

|  |  |  |
| --- | --- | --- |
| 图表列表 | | Vii |
| 丙. 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-第二部分。 | ... ... ... ... ... ... 141 |
| 丙三 | 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-第二部分。 | ... 145 |
| C. 7 | 二级机密故障的攻击树。 | . . . . . 146 |
| C. 8 | 2保密故障的攻击树——第一部分。 | ... 147 |
| C. 9 | 2保密故障的攻击树——第2部分。 | ... ... ... ... ... 148 |
| C. 10 | 3-保密故障的攻击树... ..。 | . . . . . . 149 |
| C. 11 | 3号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 |

表格列表

|  |  |  |
| --- | --- | --- |
| 1.1 | 流行的开源和商业自动驾驶仪的比较[17]。 | 6 |
| 2.1 | 不同社区的风险定义。 | 22 |
| 2.2 | Iso14971中的风险评估矩阵-医疗设备的风险管理。 | 23 |
| 2.3 | IEC61508中的 SIL 值[114] . . . . . . . . . . . . . . . . . 。 | 30 |
| 2.4 | SIL 分配基于 Consequence [115]。 | 30 |
| 2.5 | 风险评估技术比较。 | 38 |
| 2.6 | IAS99/IEC62443中的 SALs [145] ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 39 |
| 3.1 | 由于安全属性丢失而导致的故障。 | 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 | 执行意味着..。 | 52 |
| 3.6 | 攻击难度等级。 | 52 |
| 3.7 | 与故障2- 完整性有关的攻击场景的风险评估。 | 57 |
| 4.1 | SAIL 确定 SORA 方法[104]。 | 66 |
| 4.2 | 图像细节分类[201] ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 71 |
| 4.3 | 中华人民共和国内在的决心。 | 72 |
| 4.4 | 中华人民共和国损害修正系数障碍... ... ... ... ... ... ... ... ..。 | 73 |
| 4.5 | SAIL 值对应于 PRC 值。 | 73 |
| 4.6 | 3D-SAIL 测试结果。 | 74 |
| 4.7 | 网络安全威胁类别。 | 75 |
| 4.8 | 这次行动的特点和 CS 有关。 | 78 |
|  | 九 |  |

|  |  |  |
| --- | --- | --- |
| x | 表格列表 | |
| 4.9 | OCSO 的决定..。 | 79 |
| 5.1 | 无人机系统和操作规范(来自 MULTIDRONE 项目)。 | 85 |
| 5.2 | 源自 SORA 方法论的 Intrinsic GRC 表。 | 85 |
| 5.3 | 最终 GRC 决定的缓解。 | 86 |
| 5.4 | 照相机规格(来自 MULTIDRONE 项目)。 | 86 |
| 5.5 | 中华人民共和国内在的决心。 | 87 |
| 5.6 | SAIL 决定[104] ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 87 |
| 5.7 | 3D-SAIL 测试结果。 | 88 |
| 5.8 | OCSL 判定的结果..。 | 89 |
| 5.9 | 结果对比。 | 90 |
| 5.10 | OCSL 判定的结果..。 | 93 |
| 5.11 | 送货行动的分析结果... ... ... ... ... ... ... ... ... ... ..。 | 93 |
| 5.12 | 修改后的送货操作的分析结果。 | 94 |
| 5.13 | OCSL 判定的结果..。 | 95 |
| 5.14 | 有隐私保护过滤器。 | 96 |
| 5.15 | ”补充点”评估。 | 96 |
| 5.16 | 三种监测方法的比较 |  |
|  | 精神分裂..。 | 97 |
| 5.17 | OCSO 的定义中等健壮水平... ... ... ... ... ... ... ... ... 101 | |

缩写名单

ARC

AT

ATC

BVLOS

英国电信

C2

CONOPS

CS

欧洲航空航天局

ESC

外星人

金融时报

格拉斯哥昏迷指数

GRC

GPS

HMI

IACS

国际民航组织

ICS

移民局

IE

很多

IT

JARUS

迈哈里

OCSL

OCSO

OSO

加班

空气风险等级

攻击树

航空管制员

Beyond Visual Line of Sight 视线之外

领结

控制和指挥

运作概念

网络安全

欧洲联盟航空安全局

电子速度控制器

事件树

故障树

地面控制站

地面风险等级

全球定位系统

人机界面

工业自动化与控制系统

国际民用航空组织

工业控制系统

惯性导航系统

初始事件

物联网

资讯科技

无人系统规则制定联合权威机构

风险协调分析方法

操作网络安全易受影响水平

网络安全行动目标

行动安全目标

操作技术

Xi

|  |  |
| --- | --- |
| 十二 | 第0章缩略语列表 |
| PMU | 电源管理组 |
| 中国 | 隐私风险类别 |
| 航海 | 具体的保证和诚信水平 |
| SAL | 安全保证级别 |
| 监控系统 | 数据采集与监控系统 |
| SIL | 安全完整性等级 |
| SORA 网站 | 具体操作风险评估 |
| UA | 无人驾驶飞机 |
| 无人机 | 无人驾驶飞机系统 |
| 无人机 | 无人航空载具 |
| 欧洲联盟 | 不想要的事件 |
| VLOS | Visual Line Of Sight 视线 |

引言

无人驾驶飞机系统(UAS)最初用于军事目的，但现在这种系统越来越多地用于民用目的。在过去的几年里，民用无人机市场在市场规模和应用领域呈指数级增长。市场规模从2016年的20亿美元增加到2018年的141亿美元。我们目前可以在不同的经济部门找到许多 UAS 应用: 摄影，建筑，采矿，农业，现场监测，物流。无人机运营商正在继续探索和开发新的无人机应用。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空飞行。一方面，这种系统的普及可以给我们的生活带来新的方便和体验。另一方面，它也会给我们带来麻烦。这些系统的故障或误用，无论是有意还是无意，都可能导致严重的后果。例如，无人机操作可能有意或无意地侵犯飞行中人们的隐私; 无人驾驶飞机可能坠落并击中地面上的人和基础设施; 或者它可能与有人驾驶的飞机相撞。这种怀疑阻碍了公众的接受，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。

网络安全是妨碍公众接受无人机应用的主要问题之一。无人机系统是一个网宇实体系统，其中数字部件(传感器、软件、通信等)协同控制和监视实体部件(如执行器、机身)。像许多其他网络物理系统(工业控制系统、汽车等)一样，无人机的数字部分总是存在可能被攻击者利用的漏洞或缺陷。在文献中，有一些关于网络安全漏洞的报道: GPS 干扰和欺骗[2] ，视频拦截[3] ，通过通信的劫持攻击[4] ，传感器欺骗

通过利用数字部分的漏洞，对手可能会干扰无人机的运行或接管系统的控制，以达到恶意目的: 伤害地面上的人员，侵犯隐私，破坏基础设施等。因此，应该考虑无人机的网络安全，以防止可能的负面影响，并获得公众的接受。无人机的网络安全是本文的主题。

由于网络安全在无人机领域发展中的重要性，在这一领域有许多研究。通过观察无人机网络安全的文献，我们发现了两个传统的研究趋势。一是寻找新的漏洞或新的攻击策略。换句话说，就是回答这个问题: “我们如何攻击系统?”.另一个问题是寻找网络安全对策来应对可能发生的攻击。换句话说，它是为了回答这个问题: “我们如何防止可能的攻击?”.网络攻击和防御技术日新月异。然而，对于一个特定任务中的特定无人机来说，考虑到所有这些可能的网络安全攻击和实施所有相应的对策可能是昂贵和不必要的。因为这取决于

1

引言

无人机的性质和任务，攻击的成本可能优于从攻击者的角度获得的利润。从操作者的角度来看，反制措施的成本可能优于损失。因此，在考虑 UASs 的网络安全问题时，我们应该考虑损失收益和成本效益之间的平衡。为此，我们感兴趣的不是两个传统问题，而是另一个问题:”应该考虑哪些网络攻击和反措施，以及优先顺序是什么?”.

为了回答这些问题，我们需要进行风险评估。风险评估方法提供了一个系统和有效的方法来检测，分析，评估可能的安全攻击，并选择适当的对策。长期以来，不同的风险评估方法已经在不同的工业领域得到开发和应用。风险评估方法首次被用于预防潜在的事故(安全)。由于计算机在工业中被广泛使用，风险评估方法在保护系统免受网络攻击(网络安全)方面发挥着重要作用。例如，我们有 MEHARI 的 IT 系统，EVITA 的汽车系统，IEC61508的工业自动化和控制系统，ED202A 和 ED203的航空电子系统。在 UAS 领域，关于 UASs 的网络安全风险评估的研究并不多。最流行的风险评估方法是特定操作风险评估(SORA)。然而，它目前只关注安全性。因此，本论文的重点是开发无人机应用的网络安全风险评估。

本论文的组织形式如下。第一章给读者一个无人驾驶飞机系统的概述，包括无人机的定义，一般结构，市场，法规和网络安全漏洞。第二章比较了安全与安全/网络安全的不同方面: 定义，风险概念，以及风险管理的现状。第三章介绍了第一个贡献——一种加强现有或预先定义的无人机系统的网络安全的方法。第四章首先解释了 SORA 方法论，然后提出了我们提出的解决方案，以扩展该方法论到网络安全。第五章通过不同的案例研究说明了扩展的 SORA 方法，并演示了如何在开发过程中使用评估结果。最后，结论部分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

无人驾驶飞机系统及相关网络安全问题

目录

|  |  |  |  |
| --- | --- | --- | --- |
| 1.1 | 定义..。 | | 4 |
| 1.2 | 系统描述..。 | | 4 |
|  | 1.2.1 | 无人机段..。 | 5 |
|  | 1.2.2 | 地面部分..。 | 7 |
|  | 1.2.3 | 沟通片段。 | 8 |
| 1.3 | 无人机市场和应用。 | | 9 |
| 1.4 | 无人机进入空域。 | | 10 |
|  | 1.4.1 | 规定..。 | 11 |
|  | 1.4.2 | U 太空的概念..。 | 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 | 沟通..。 | 16 |
|  | 1.5.4 | 自动驾驶仪和地面控制系统。 | 16 |
| 1.6 | 结论。 | | 17 |
|  |  |  |  |

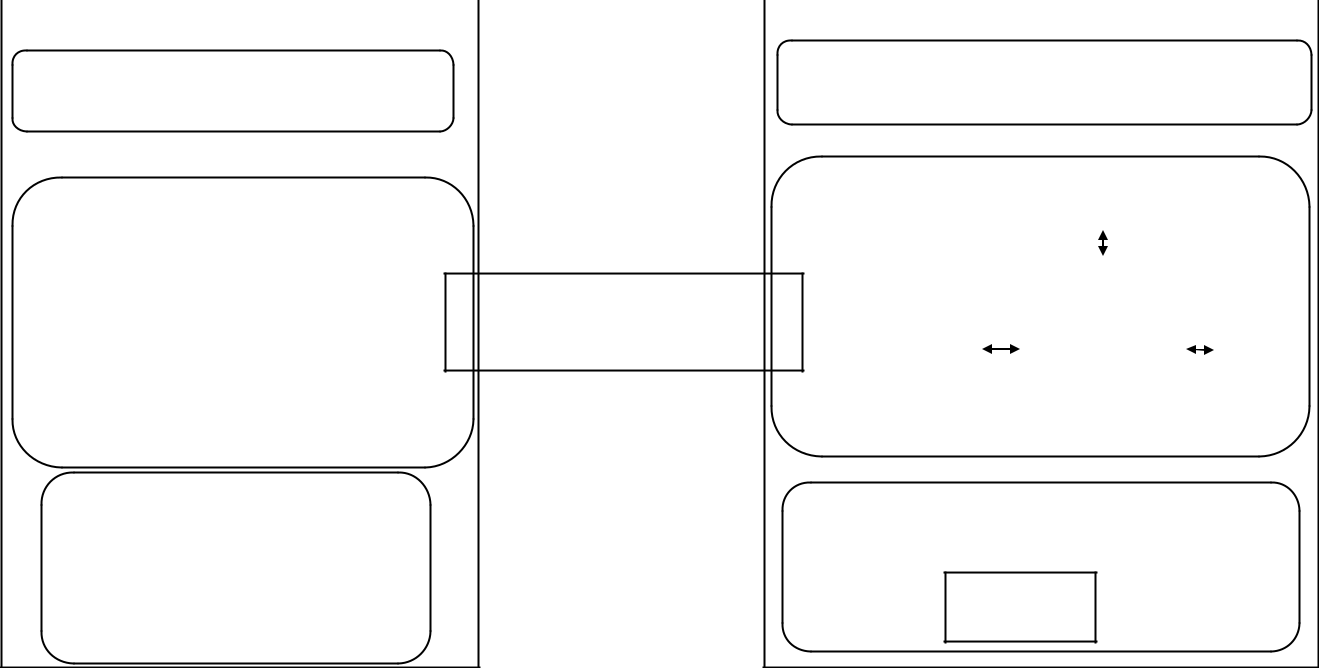
3

第一章无人驾驶飞机系统和相关的网络安全问题

1.1定义

根据国际民用航空组织(ICAO)[6] ，无人航空载具(UAV)或无人机是一种可以在没有飞行员的情况下飞行的飞机，可以从另一个地方进行遥控或完全控制。然而，无人机不能单独操作，而是需要与地面操作员保持互动。因此，另一个术语无人驾驶航空系统(UAS)被引入。该系统包括无人机和所有必要的设备、网络和人员，以控制无人驾驶飞机并完成特定任务[6] ，[7] ，[8]。这种系统首次应用于军事领域的危险任务。如今，技术的逐步发展降低了获取这项技术的成本。这导致无人机在许多民用领域的应用不断增加，如货物运输，农业，航拍[4]。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1.2 | |  | 系统描述 | | | | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 地面部分 | | | | | | | | |  |  |  |  | 无人机段 | | | | | | | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  | 飞机 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 电源 | | |  | |  |
|  |  |  | 接线员 | | | | | | | | | Airframe (机身) | | |  |  |  | 执行器 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 系统 | | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | 航班 | |  |  |  |  |  |  |  | 执行器 | | | |  |  |  |  |  |  |  |  |  |
|  |  |  | 控制室 | |  |  |  |  |  |  |  | 管理 | | | |  |  |  |  |  | 控制器 | | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 使用者 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 系统 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 车站 | |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 电脑 | | |  |  | |  |  | 传感器: | |  |  |  |  |  | 自动驾驶仪: | | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 通讯部分 |  | • | GPS, | |  |  |  |  |  | • | 态度 | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | • | IMU, | |  |  |  |  |  |  | 控制 | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | PMU | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | • | 气压计, | |  |  |  |  |  | • | 导航 | | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 电源 |  |  | 接线员 | |  |  |  |  |  | • | 皮托 | |  |  |  |  |  | • | 指引 | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |  | • | 应答器 | | |  |  |  |  | • | 碰撞和 | | | | | |  |  |  |  |  |  |
|  |  |  | 系统 |  |  | 电脑 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |  | • | 可选项 | |  |  |  |  |  |  | 避免 | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 附件 | |  |  | 执行器 | | |  |  |  |  |  |  | 有效载荷 | | | | | | |  |  | 执行器 | | | | |  |  |  |  |
|  |  |  | 电脑 | |  |  |  | | 有效载荷 | | |  | 电脑 | | | | | | |  |  |  |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 电源 | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | P |  |  |  |  | 传感器 | | | |  |  |  |  |
|  |  |  |  |  | 传感器 | | |  |  |  |  |  |  |  | 电源 | | | | |  |  |  |  |  |  |  |  |
|  |  |  | 系统 | |  |  |  | |  |  |  |  |  |  |  |  |  |  |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 系统 | | | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |



配件: 天线系统，发射器等。

图1.1: UAS 架构

根据任务期间无人驾驶飞机的自主程度，系统的复杂性可能会有所不同[9]。至于最低程度的自主性，我们可以参考简单的无人机业余爱好的目的，它包括一个简单的遥控飞机，一个遥控无线电控制和在地面上的飞行员。与此同时，为了获得更高程度的自主权，无人机系统可以由一个机队组成，这些机队配备了先进的传感器、处理器和通信设备，这使得无人机可以在没有飞行员互动的情况下飞越视距。文件的这一部分对无人机体系结构进行了概括性描述。基本 UAS 的组件可以分为三个部分:

|  |  |
| --- | --- |
| 1.2系统描述 | 5 |

无人航空载具(UAV)段，地面段和通信段[7] ，[8]。这些部分可以如图1.1所示描述，下面一节将详细说明。

1.2.1无人机部分

无人机部分由三个主要模块组成: 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。

Airframe 是飞行器的机械结构，不包括推进系统。无人机的机械结构存在多种形式，它们具有不同的气动特性、尺寸特性、质量特性，这些特性是根据目标作战的需要而选择的。无人机机身基本上可分为以下四类: 固定翼、旋转翼(如直升机、多直升机)、小型飞艇和扑翼[8]、[10](见图1.2)。除了基本的机身之外，还有具有基本机身特征的混合动力机身。例如，倾转旋翼机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、小型飞艇和扑翼机身

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、舵、扰流板和降落伞发射器。因此，飞行器可以改变它的姿态和高度。

电力系统是由用于储存、产生和分配能量的电气或机械部件组成。最初，动力系统的主体是内燃机[12] ，它适用于大型军用无人机。现在，对于较轻的商业无人机，电力系统变得更加流行与许多先进的技术，如燃料电池[13] ，[14] ，太阳能电池[15] ，[16]和电池。

第一章无人驾驶飞机系统和相关的网络安全问题

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 开源 | Airframe (机身) | 硬件 | 多无人机 | 飞行计划 | 地理围栏 | 碰撞 | 持续 |  |
| 逃避 | 释放 |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| 狗仔队 | 固定翼，旋转翼 | 多元化 | 是的 | 是的 | 是的 | 是的 | 19-12-18 |  |
| Pixhawk | 固定翼，旋转翼 | 具体点 | 是的 | 是的 | 是的 | 是的 | 21-04-20 |  |
| Ardupilot | 固定翼，旋转翼 | 多元化 | 是的 | 是的 | 是的 | 下 | 29-02-20 |  |
| 发展 |  |
|  |  |  |  |  |  |  |  |
| OpenPilot 开放式试点 | 固定翼，旋转翼 | 具体点 | 无 | 是的 | 不认识 | 没有 | 18-07-15 |  |
| AeroQuad 航空母舰 | 旋转翼 | 多元化 | 无 | 没有 | 不认识 | 没有 | 31-01-13 |  |
|  |  |  |  |  |  |  |  |  |
| 商业 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| Picollo | 固定翼，旋转翼 | 具体点 | 是的 | 是的 | 是的 | 是的 | 不认识 |  |
| 微型导航仪 | 固定翼，旋转翼，飞艇 | 具体点 | 是的 | 是的 | 是的 | 是的 | 不认识 |  |
| Veronte | 固定翼，旋转翼，飞艇 | 具体点 | 下 | 是的 | 是的 | 是的 | 不认识 |  |
| 发展 |  |
|  |  |  |  |  |  |  |  |

表1.1: 流行的开源和商业自动驾驶仪的比较[17]

1.2.1.2飞行管理系统

飞行管理系统是一套所有的航空电子元件，观察飞行器和控制执行器/发动机的行为，以执行安全和自动飞行。这个模块的关键部分是自动驾驶仪，基本传感器，电源管理单元，执行器控制器和机载通信模块。

涉及硬件和软件方面的自动驾驶仪。它是飞行管理系统(FMS)的中心，它与 FMS 的其他组件(传感器、执行器、通信、电源管理单元(PMU))进行通信。这一部分的基本作用是估计飞机的状态，并根据地面飞行员的指令或程序飞行计划对飞机进行导航。随着无人机数量的逐步增加，无论是开源形式还是商业形式的自动驾驶仪的硬件和软件都呈指数增长。当前流行的开源和商业自动驾驶仪的简要比较如表1.1所示。

传感器是机载传感器，允许飞机导航。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)

和惯性导航系统(IMU)。由于它们的互补性(例如 GPS 的准确度低，但数据率低; IMU 的数据率高，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组合[19]。这些传感器的输出被自动驾驶仪集成以估计飞机的行为。GPS/IMU 组合有许多已发展的算法，如解耦积分、松耦合积分、紧耦合积分和深耦合积分[20]。除了传统的 GPS/IMU 耦合外，本研究还研究了其他传感器组合，如 GPS/视觉-计算机耦合[21] ，IMU/视觉-计算机耦合[22]。为了提高飞机状态估计，无人机可以配备几种

|  |  |
| --- | --- |
| 1.2系统描述 | 7 |

各种辅助传感器，如气压计或磁力计。

执行器控制器是将自动驾驶仪指令转换成控制信号的电子元件，这些信号随后被发送到执行器。一个典型的执行器控制器是电子速度控制器(ESC) ，调节电机的速度。

PMU 由电子元件组成，负责测量和管理车辆的能量。

1.2.1.3有效载荷

有效载荷是无人机飞行中不必要的组件，但是对于完成特定的操作目标是必要的。为安全和保安起见，有效载荷应配备独立于飞机主动力系统的动力系统，不应直接与自动驾驶仪或其他关键系统连接[7]。因此，有效载荷系统可以有自己的传感器，驱动器，外围设备和处理器。根据应用的不同，无人航空载具可以配备各种类型的有效载荷部件。最流行的有效载荷部件是相机。该组件广泛应用于与视听制作、监控应用或大型基础设施(如桥梁、风车或电力线路)检查有关的许多 UAS 应用中[23]、[24]、[25]。激光雷达是另一种流行的传感器有效载荷，吸引了许多与无人机相关的研究。激光雷达可以高精度地测量距离，因此可以用来制作高分辨率地图[26] ，[27]。随着无人机应用数量的增加，现在越来越多的设备可以作为有效载荷安装在无人机上，例如用于精细农业的喷洒系统[28] ，[29] ，或用于良好运输的货物。

1.2.2地面段

地面部分(见图1.1)包括所有不是飞行器本身的部件但是飞行所需的元素。这个部分的主要元素是: 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(民航组织)[6]的定义，经营者是从事或提议从事飞机业务的个人、组织或企业。根据无人机操作或应用的复杂性，运营商的规模可能会有所不同。例如，对于最简单的无人机操作，操作员可能只是一个手动驾驶遥控飞机的飞行员。同时，在更复杂的无人机操作中，操作员可以是一个由许多人组成的结构化组织

第一章无人驾驶飞机系统和相关的网络安全问题

例如飞行员(或机组人员)、维修人员、经理。每个运营商成员的角色应该由当地民用航空当局来定义。

1.2.2.2控制站

控制站由地面硬件和软件组成，作为人机界面(HMI)用于控制/观察飞行器和有效载荷。根据 UAS 应用的目的，UAS 可以有多个控制站[7]。例如，为了观察一个工业站点，一个 UAS 可以部署两个控制站。第一个被放置在远离工业场所的地方，飞行员用它来完全控制飞行器和有效载荷。第二个是移动站(比如平板电脑，智能手机)。这个移动站由工业厂区内的人员使用，只能访问有效载荷数据，比如摄像头数据。

1.2.2.3附件

配件是不直接参与无人机操作但需要执行的设备，如天线/照相机跟踪系统、无人机弹射发射器、电池充电器或运输箱。

1.2.3通信段

通信部分(见图1.1)对于任何类型的 UAS 应用程序都是至关重要的。这个部分包括不同的通信系统，为 UAS 提供远程控制和远程数据采集的能力[30]。在操作过程中，通信系统可以传输各种数据。对于大多数无人机系统来说，最基本的是控制和指挥(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，包括控制有效载荷的数据和有效载荷产生的数据，如视频数据。这种数据对于飞行来说并不重要，但对于实现操作目标(如监控应用的视频数据)却很重要

除了这两种数据，通信系统还可以传输交通数据。这种数据在飞机、地面控制站和航空管制员(ATC)之间进行交换，以保证空域的安全和高效。随着未来无人机数量的增加，这种数据和相关技术是无人机成功融入国家空域系统的关键因素[30][32]。

根据预期操作的连通性需要(例如范围、带宽) ，通信系统的复杂性可能会有很大差异。对于一个简单的操作，通信系统只能提供飞机和地面控制站(GCS)之间的连接。对于更复杂的操作，通信系统可以

|  |  |
| --- | --- |
| 1.3无人机市场和应用 | 9 |

将一架无人驾驶飞机与其他无人机连接以建立一个无人机群，或将 GCS 与 ATC 连接以共享有关交通的信息。

1.3无人机市场和应用

UASs 的历史开始于20世纪初，当时它们首次被用作军事演习的目标[33]。从那时起，无人机市场逐步形成。上个世纪，市场只关注于军事应用，如侦察/战斗任务，而无人机的民用应用还没有得到认可。从2000年开始，民用无人机市场开始成长。起初，在民用领域，无人驾驶飞机被用作个人娱乐用途的玩具。然后，技术的发展(例如小型化部件、提高计算能力、改进传感器和电池容量)使无人机变得更小，在许多经济部门的专业和商业用途上更具吸引力，例如:

摄影和媒体行业: 在无人机技术出现之前，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照相机的无人机来实现。随着价格的下降，这种无人机在这个领域变得越来越受欢迎。事实上，与无人机相关的产品和服务在2016年为民用无人机行业创造了大部分收入(占总收入的60-70% [34] ，[1])。

农业部门: 这个部门的利润也随着无人机技术的出现而降低了运营成本。农民们可以用无人机代替飞机或卫星喷洒农药，收集和分析他们田地的数据(如田地养分吸收强度[35] ，植物在变得明显前几天的压力[36] ，...)。根据《2017-2027年农业机器人和无人机: 技术、市场、参与者》[37] ，用于农业的无人机应用将是一个主要市场，2027年将达到4.7亿美元以上。

能源行业: 无人机对能源行业的公司也很有吸引力。该部门专注于使用无人机进行维护和检查，以减少与基础设施和执行危险任务的工作人员相关的各种风险。根据2019年进行的一项调查[38] ，超过三分之二的能源公司(超过247家公司参加了调查)目前正在使用无人机进行活动。然而，大多数无人机操作仍然处于概念验证或无人机应用研发领域。对于 UAS 应用来说，这个领域最需要的特性是飞行的耐久性、灵活性和可靠性。

物流和运输部门: 无人机有望成为未来物流和运输系统的一部分。无人驾驶飞机系统可以用来在密集的(次)城市地区提供具有最大竞争优势的小包装。这种应用吸引了美国大公司的大量考虑

第一章无人机系统和相关的网络安全问题

亚马逊、 UPS、联邦快递等电子商务领域。根据 SESAR 合资公司(负责欧洲空中交通管理现代化的公营部门与私营机构合作)的预测，2035年用于该项目的无人机机队规模可能达到70000架[32]。然而，目前为了更好的交付，UASs 还没有得到广泛的部署和接受，这个部门的大多数飞行仍然是为了概念验证的目的。这种应用程序最重要的促成因素之一是没有完全定义的规定[32]。

在过去的十年中，我们认识到民用无人机市场的爆炸。从2012年到2019年，在这个领域投资了超过30亿美元，市场规模从2016年的20亿美元增长

到2018年将达到141亿美元[39]。与此同时，军用无人机市场总是被波音(Boeing)、洛克希德 · 马丁(Lockheed Martin)、空中客车(Airbus)等在该行业拥有强大地位的公司所主宰，而民用无人机市场几乎被新进入者或初创企业所主宰[33]。这种趋势的最好例子是中国大疆公司和法国鹦鹉公司，它们是市场上最成功的无人机制造商。市场的爆炸性增长不仅给制造商带来了机会，也给这个领域的其他参与者带来了发展他们业务的机会。他们是提供行业服务(监测、观察、检查... ... 无人机)、培训项目和软件解决方案的公司，用于分析无人机收集的海量数据[33]。

展望民用 UASs 的未来，许多组织和市场研究公司提出了市场预测。SEAR 合资公司预测，到2050年，欧洲上空将有大约40万架商用无人机(不包括700万架休闲无人机)。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。无人机行业洞察预测，到2024年，民用无人机市场将达到431亿美元。Interact Analysis 公司预测2022年市场价值为150亿美元[41]。虽然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无人机并入空域

空域的组织和维护基本上基于复杂的法规和标准体系，以确保所有航班以安全和有效的方式运行。这些法规和标准涵盖了航空工业从飞机设计到运营的许多方面。例如，有人驾驶的飞机必须经过认证，注册，按照程序进行维护; 机组人员必须有执照，操作员必须经过认证

此外，飞机需要与航空管制员交换以避免碰撞。然而，目前的管制系统已经被设计成适用于有人驾驶的飞机，而不是无人驾驶的飞机。

|  |  |
| --- | --- |
| 1.4. 无人机并入空域 | 11 |

事实上，将无人机安全有效地集成到空域中面临着许多挑战[43]。其中一个挑战是目前有人驾驶飞机的规定不适合无人驾驶飞机系统[42]。与载人飞机市场不同的是，无人机市场主要是大量低成本、周期短(约30个月[44])的 UASs。因此，基于有人驾驶飞机所使用的昂贵流程来设计、验证和操作无人机是没有意义的。另一个挑战是如何在无人驾驶飞机和载人飞机上保证空域的安全运行。为避免空中碰撞，有人驾驶的飞机一般配备多种设备，以便与航空管制员及其他飞机通讯，接收清关及紧急警告，例如无线电通讯、转发器等。所有无人机操作员遵守这些要求似乎是一种负担[42]。此外，由于无人驾驶飞机体积小，操作灵活性高，它可以在任何地方起飞/降落，不会按照有人驾驶飞机[45]、[42]等固定和命名的路点飞行。这使得载人和无人飞机的空中交通管制成为一项复杂的任务。



**开放分类**

**(低风险)**

**特定类别**

**(中等风险)**

**认证类别**

**(高风险)**

图1.3: 无人机操作的三个类别

1.4.1规例

为了将无人机整合到空域中，欧盟委员会于2008年开始考虑这种飞行器，颁布了 EC2008/216条例。这项规定是第一个专门针对无人机操作的法律文件。然而，这份文件详细规定了只有超过150公斤飞机的无人机操作规则。飞机重量低于150公斤的作战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分割，并可能阻止一些无人机操作(例如，跨境飞行)。因此，它需要考虑所有无人机操作的欧盟层面的法规来修改 EC2008/216法规。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，EASA 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:

第一章无人驾驶飞机系统和相关的网络安全问题

新规定考虑了所有类型的无人机。这意味着150公斤的限制应该被取消。

这个监管框架是以业务为中心的。这意味着监管是基于操作风险而组织起来的。它应该建立从低风险到高风险的三类操作:

1. 开放类别: 包括低风险运作，例如大部分休闲航班及一些专业活动。这个类别下的操作不需要民航当局的明确授权。对于这些操作，严格的操作限制(例如不接近人群、交通、基础设施、没有危险物品、没有物品掉落、每个飞行员只有一个无人机)确保了安全。

2. 具体类别: 重新组合中等风险的作业，例如视线以外的作业(即飞行中飞行员与无人机之间没有视线接触)。对于此类操作，需要进行风险评估。

3. 认证类别: 包括具有相当于载人飞机操作风险的操作。这些业务的要求与载人航空的要求相当，例如无人机认证、持有许可证的遥控飞行员和经主管当局批准的操作员。

这些规定应该处理不同的安全风险: 与载人飞机的空中相撞，对人的伤害，以及财产损失。

这些要求应该与操作风险相称。

应该考虑安全性和隐私性。安全并不局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，根据上述建议，欧盟委员会发布了《欧盟委员会放行条例(2019/945)》和《欧盟委员会执行条例(2019/947)》。欧盟委员会授权条例(EU)2019/945界定了认证要求，包括 CE 标记和第三国经营者。欧盟委员会实施条例(EU)2019/947界定了运营和注册的要求。在2019/947年度规例中，三个经营类别的界限定义如下:

开放类别: 在下列情况下，无人机操作始终被视为属于此类别:

最大起飞重量小于25公斤。

- 这架飞机没有运载危险品。

- 飞机不会掉落任何材料。

- 遥控飞行员的年龄等于或超过16岁。

- 飞行员始终将飞机保持在其视线范围内(视线操作)。

|  |  |
| --- | --- |
| 1.4. 无人机并入空域 | 13 |

ー飞机不飞越人群。

- 地面以上的最高高度是120米。

特定类别: 当不满足开放类别条件时，无人机操作总是被认为属于这一类别

认证类别: 在下列情况下，无人机操作始终被视为属于这一类别:

ー飞机飞越尺寸超过3米的人群; 或

- 运送人口; 或

ー运载危险品。

预计大多数无人机操作将在特定类别下进行。对于这个类别，运营商必须执行和提交风险评估根据 SORA 的方法。但在某些情况下，操作者可以跳过完整的风险评估:

该操作符合2019/947法规中预定义的标准情景(STS-01和 STS-02)。

角色塑造操作符合欧盟委员会实施条例(EU)2019/947的指导文件中描述的预定义风险评估中描述的操作特征。

1.4.2 u 空间概念

除了监管建议之外，欧洲航天局为无人机一体化所做的另一项努力是提出“ u 空间”概念。这一概念的名称不是指分配给无人机作业的新空域数量，而是指支持无人机作业的一套新技术服务。这些服务正在或将要开发，以便在包括城市、郊区、农村在内的所有操作环境中实现高度自主的复杂无人机操作[47]。随着无人机连通性和自动化水平的提高，U-space 概念提出了四个服务块:

基础服务(U1)包括电子注册、电子身份识别和地理围栏服务。这些服务帮助当局识别无人机，并支持安全和安全要求。

初始服务(U2)支持无人机操作的管理，可能包括飞行计划、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)为无人机提供了在密集区域飞行时自动探测和避免与他人冲突的能力。

14第1章无人驾驶飞机系统及相关的网络安全问题



图1.4: U-space 插图[47]

Full service (U4)提供与载人航空的综合接口，支持 u 空间的全面作业能力，并将依赖于无人机和 u 空间系统的高度自动化、连通性和数字化。

由于与 U-space 相关的标准和技术是由许多公共机构和私人公司同时开发的，这个概念的许多服务现在都可以使用。然而，这并不意味着 U-space 可以立即实施，因为这种开发是零碎的，并且在实际条件下缺乏真正的测试[42]。

1.5网络安全问题

1.5.1 GPS

正如在1.2.1.2中提到的，GPS 接收机是无人机的重要组成部分，特别是当无人机可以自动飞行时。这个组件提供了关于飞机的原始信息

|  |  |
| --- | --- |
| 1.5网络安全问题 | 15 |

根据卫星信号确定车辆的位置。这些信号来自距离地球1300英里的 GPS 卫星，它们必须穿过地球的大气层。当它们到达无人机上的接收器时，信号极其微弱。这使得 GPS 接收机很容易受到干扰攻击(GPS 干扰) ，攻击者可以通过更高功率的 GPS 信号接入原始 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] ，并且不需要任何专门知识。此外，民用 GPS 数据没有加密。这使得 GPS 接收器很容易受到欺骗攻击(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 GPS 欺骗攻击造成的，例如 S-100直升机无人机坠毁，军用无人机 RQ-170被捕[2]。在这项研究中，GPS 欺骗的可能性已经在许多工作中的攻击实验中得到了证明。例如，2012年7月，德州大学奥斯汀分校的无线电导航实验室在受控条件下对一架小型无人机进行了 GPS 欺骗攻击，导致了一次命令性俯冲[49]。Seo 等[50]进行了另一个实验，该实验通过使用 GPS 欺骗技术迫使无人机降落在不正确的位置。与 GPS 干扰攻击相比，执行成功的 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，攻击可以被检测到，并被认为是 GPS 部件的故障(GPS 信号丢失)。大多数商用无人机都有自动防故障装置来处理这种情况(比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控制无人机的飞行路线。针对 GPS 欺骗，文献中提出了不同的对策(详见附件 d)。

1.5.2 IMU

惯性测量单元(IMU)是无人机的另一个基本部件。这个部件为无人机提供了无需外部参考就能感知运动的能力(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(感知角速度)和一个加速度计组成。这些传感器基于传感质量的位移来测量无人机的运动。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无屏蔽的低成本 IMUs。这使得 IMU 容易受到声波干扰。尽管目前还没有关于通过 IMU 进行网络攻击的报道，但是已经做了一些工作来展示这种攻击的可能性。Yunmok 等[51]通过在传感器的近共振频率上的有意声干扰，对无人机的陀螺仪进行了分布式拒绝服务攻击。同时，Lu 等[52]论证了一种基于短时傅立叶变换家族中的关系，通过故意声干扰来完全控制陀螺仪输出信号的方法。Trippel 等[53]说明了对加速度计的相同攻击。除了与 IMU 相关的攻击技术之外，还研究了不同的防御方法。我们想到的常见方法是传感器冗余。然而，它需要额外的传感器。Tu 等[54]提出了一种 IMU 攻击检测和容错的方法

16章1. 无人机系统和相关的网络安全问题

没有附加传感器。如果 IMU 受到攻击，姿态数据仅基于位置数据和航向数据进行估计。Crispoltoni 等[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[56]提供了一个广义预测控制器以及故障检测机制。这种机制可以用作检测受损 IMU 数据的对策。

1.5.3通信

根据通信需求(范围、带宽、成本等) ，用于 UASs 的通信技术可能有所不同，如 WiFi、 RF、4G/LTE、卫星等。因为这些技术用于通用目的，不仅仅是 UAS 应用，许多工作被引入来保证这些技术的安全。对于小型/商用 UASs，由于资源有限或配置错误，通信的安全性不能达到合适的水平。为了说明通过通信系统对 UASs 进行网络攻击的可能性，文献中做了几项工作。Vattapparamban 等人。

通过利用 WiFi 的弱点，对不同的低成本 UASs 进行去认证攻击。对于相同的通信技术，Fournier 等[57]成功地接管了 DroneJack 项目中的一架无人机的控制。

许多商用 UASs 使用通信系统顶层的开源 MAVLink 协议来传输无人机和 GCS 信息。然而，Mavlink 协议的原始版本(版本1.0)没有提供任何保护交换消息的机制(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 通信受到威胁，MAVlink 就不能提供任何保护。自动驾驶仪资源的限制可能会阻碍 MAVlink 协议的健壮加密的实现。[58].Marty 的论文[59]讨论了加密的 MAVlink 协议。

1.5.4自动驾驶仪和 GCS

自动驾驶仪有时与外部设备连接，用于许多目的，如下载飞行数据、获取更新包或重新配置。这使得自动驾驶仪很容易受到病毒感染或未经授权的访问。在这类攻击中，攻击者可能恶意改变飞行参数，以改变系统的行为/控制规律[60]。对于大多数商用无人机来说，GCS 通常建立在通用计算机(笔记本电脑，台式机，智能手机)上，使用 GCS 软件。因此，像其他基于这些设备的应用程序一样，GCS 可能成为网络攻击的首要目标。例如，攻击者可以恶意修改存储在 GCSs 上的数据(如飞行参数、飞行计划、地图)来欺骗飞行员[60]。Heiges 等[61]试验了一种攻击方案，其中 GCS 软件受到损害，并显示错误信息以阻碍对自动驾驶仪的其他攻击。

|  |  |
| --- | --- |
| 1.6结论 | 17 |

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，这个系统的价格在过去的十年里迅速下降。它导致这个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。空域中无人驾驶飞机数量的快速增长要求采取行动保证空域、人民生命和地面财产的安全。为此，欧盟委员会和欧盟航空安全局(EASA)制定了无人机操作规程。除了新的规定外，欧洲航空安全局还引入了“ u- 空间”的概念，以有效地组织空域内的无人机操作，尤其是在城市地区。无人机是数字部件和机械部件的组合。除了安全性，网络安全也是无人驾驶飞机系统的一个问题。文献中报道了许多安全问题。

第二章

安全与安保的比较/网络安全

目录

|  |  |  |  |
| --- | --- | --- | --- |
| 2.1 | 引言... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | | 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 | 手术和人为因素。 | 25 |
| 2.4 | 风险管理的标准和方法。 | | 26 |
|  | 2.4.1 | 安全..。 | 26 |
|  | 2.4.2 | 保安..。 | 27 |
| 2.5 | 安全分析技术。 | | 29 |
|  | 2.5.1 | HAZOP... ... ... ... ... ... ... ... ... ... ... ... ... ... ... | 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 | 马尔可夫分析公司。 | 36 |
|  | 2.5.7 | Petri 网..。 | 37 |
|  | 2.5.8 | FMEA... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... | 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 | HAZOP 在安全部门..。 | 40 |
|  | 2.6.3 | 从断层树到攻击树。 | 40 |
|  | 2.6.4 | 基于 fmea 的技术。 | 41 |
|  | 2.6.5 | 领结分析是为了安全..。 | 41 |
|  | 2.6.6 | 马尔可夫过程的安全..。 | 42 |
|  | 2.6.7 | Petri-net 保护安全..。 | 42 |
| 2.7 | 安全和安保的综合方法。 | | 43 |
| 2.8 | 结论。 | | 43 |
|  |  |  |  |

19

第二章安全与保安/网络安全的比较

2.1引言

在上一章，我们介绍了无人驾驶飞机系统的一般概念，以及公众对其安全和保安/网络安全的关注。因为安全和安保都是指人和资产的保护，所以它们有时在语言的日常使用中可以互换使用[62]。这可能会导致一些混淆。因此，在本章中，我们首先提供这些术语的定义，强调它们之间的区别。然后我们讨论安全和安全之间的相似方面。本章还回顾了安全和安全/网络安全问题是如何在工业界和学术界得到解决的。

2.2定义

有许多不同的方法来定义两个术语: 安全和安全。这些可能因专家而异，因技术社区而异[63]。例如，在航空航天工业中，安全可以定义为”对人员或财产的损害风险降低到可接受水平的状态”[64] ，而对工业控制系统(ICS)可以定义为”这种状态不受可能产生负面后果的”某种东西”的影响,

如对人或动物的伤害，经济损失，或任何其他形式的损害或损失”[65]。对于信息系统，安全可以解释为“涉及

保护信息免受各种威胁，以确保业务连续性和尽量减少业务风险”[66] ，而对于嵌入式系统，这一术语可定义为”安全是实体保护其负有保护责任的资源的能力”[67]。这两个术语都没有绝对的定义: 安全和安全

这有时会导致使用这些术语的模糊性。此外，安全和安保都是指风险和某种保护，因此，在某些情况下，这些术语可以互换使用，如[69]。

然而，安全和安全仍然是两个不同的术语，应该有不同的含义。文献中的一些作品展示了这两个术语之间的区别。例如，根据对86份正式文件(不同部门的国际、国家标准/规章)中的定义的审查，Piètre-Cambacédès 等[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)区分。安全处理源于恶意行为的不良风险，同时安全处理源于意外/非故意事件的风险。这种区别似乎在文献[68] ，[71] ，[72] ，[73] ，[74]中被广泛接受。第二个区别称为环境系统(E-S)起源区分。安全性关注的是源自环境(被考虑的系统周围的所有其他事物)并可能影响系统的风险。同时，安全处理的风险产生的考虑系统和潜在的影响环境。这种区别在其他一些研究中也被接受，如[68]。然而，我们认为，第二个区别并不十分清楚。例如，关于飞机的安全，我们可以考虑恶意行为引起的情景，而不仅仅是影响

|  |  |
| --- | --- |
| 2.3安全和安保的不同方面 | 21 |

飞机，还有乘客的生活，公司的财务等等。与此同时，关于飞机的安全，我们可以担心由于恶劣的天气条件引起的不安全情况。

基于上述简短分析，我们采用以下定义:

安全性是一种保护系统免受来自恶意意图的风险的状态。网络安全是仅与数字世界相关的安全的一个子术语。

注意: 在我们的研究背景下，除了明确说明外，安全这个术语实际上在大多数情况下指的是网络安全。

安全是保护系统免受事故或意外事件风险的一种状态。

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为了避免在我们的上下文研究和文档的其余部分的误解。此外，在我们看来，理解安全和安保的本质比创造一个短语来描述这些术语更有趣。因此，在这一部分的下一部分，我们深刻地分析了安全和安保在不同方面的异同。

2.3安全和保安的不同方面

2.3.1风险概念

安全和保安有一个共同点，即“风险”。在这两个领域，风险作为一个基本概念被实践者和研究人员广泛使用，以推动保护所考虑的系统或操作的活动。如表2.1所示，这个术语的定义在不同的技术社区之间可能有所不同。尽管不同社区之间有一点差异，但风险术语总是可以表示为两种测量(或估计)的结合: “一个事件可能有多糟糕?”以及“多久会发生一次?”或者用一个简单的公式表示: 风险 = 可能性 x 后果的严重性。

2.3.2风险管理

一般来说，负责安全风险或安全风险的人必须回答一些问题，比如“所有事故都已经确认了吗?”例如，“实施的保护措施是否充分或必要”等等。为了回答这些问题，风险通常涉及到风险管理。风险管理提供了一个系统和有效的方法来检测，分析,

第二章安全与安全/网络安全的比较

|  |  |  |
| --- | --- | --- |
| 社区和来源 | 风险定义 |  |
| 安全 |  |  |
|  | 表示危险、危险或有害或有害的可能性的多属性量 |  |
| 核武器 | 与实际暴露或潜在暴露相关的后果 |  |
| (国际原子能机构词汇[69]) | 作为可能出现特定有害后果的可能性和规模 |  |
|  | 以及这些后果的性质。 |  |
| 航空 | 事件发生的频率(概率)及其相关水平的组合 |  |
| (ARP4754a [75]) | 严重性。 |  |
| Chemicals 化学品 | 衡量人员伤害、环境损害或经济损失的尺度 |  |
| (CCPS 词汇表[76]) | 事故的可能性和损失或伤害的程度 |  |
| 医疗仪器 | 损害发生的概率和损害的严重程度相结合 |  |
| (ISO 14971[77]) |  |
|  |  |
| 安保 |  |  |
| 石油和天然气 | 事件发生的可能性及其后果的组合 |  |
| (OLF-104[78]) |  |
|  |  |
|  | 对机构运作的影响程度(包括任务、职能、形象或 |  |
| 一般信息技术 | 名誉)、机构资产或个人，由于经营 |  |
| (NIST SP800-53[79]) | 考虑到威胁的潜在影响和可能发生这种情况的可能性, |  |
|  | 威胁发生。 |  |
| 资讯系统 | 风险通常表示为事件和结果的组合 |  |
| (iso27000[80]) | 相关的“可能性”发生 |  |
| 互联网 | 损失预期表示为特定威胁可能利用的概率 |  |
| (IETF rfc4949[81] | 具有特定有害结果的特定脆弱性 |  |

表2.1: 不同组织的风险定义

|  |  |
| --- | --- |
| 2.3安全和安保的不同方面 | 23 |

评估可能发生的事故，并选择适当的对策。此外，风险管理有助于平衡操作和实施对策的经济成本

大部分的风险管理包括风险评估。风险评估是“关键组成部分”，它提供足够的知识、意识和对风险的理解，以证明在风险管理过程中采取保安措施以减少风险[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不良影响的风险情景。对于这一步，不同的风险管理方法可以提出不同的策略。有些方法为了简化这一步骤，向用户提出了一系列基本方案(例如，为了信息系统的安全而采用的 MEHARI 方法(见2.4.2) ，以及为了无人机操作的安全而采用的 SORA 方法(2.4.1))。其他方法提供工具或模型，帮助用户推理可能的情况。这样的方法可以采用演绎法或归纳法[84]。归纳法侧重于回答“给定的后果如何发生?”或者“给定结果的原因是什么?”.这种情况下最好的例子是错误树方法和攻击树方法。同时，演绎方法从一个初始事件(组件故障或错误)开始，并试图回答“危险事件的后果是什么?”.这种方法的好例子是 HAZOP 方法和 FMEA 方法。以下部分描述了所有这些方法。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 频繁 | 很低 | 中等 | 很高 | 很高 | 很高 |
|  | 可能 | 很低 | 中等 | 中等 | 很高 | 很高 |
| 可能性 | 偶尔 | 很低 | 很低 | 中等 | 中等 | 很高 |
|  | 遥控器 | 很低 | 很低 | 很低 | 中等 | 中等 |
|  | 不太可能 | 很低 | 很低 | 很低 | 很低 | 中等 |
|  |  | 可以忽略不计 | 小 | 认真的 | 梅杰 | 情况危急 |
|  |  |  |  | 严重程度 |  |  |

表2.2: iso14971- 医疗器械风险管理中的风险评估矩阵

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。如前所述，风险是结果的可能性和严重性的组合，因此风险分析涉及到对这些因素的估计[85]。可能性和严重程度的估计可以是定性的或定量的。为了安全起见，根据 Khan 等[86]的观察，定量方法和混合方法比定性方法被越来越多地考虑。同时，为了安全，定性方法是最好的[87]。这些现象的原因可能是数据的可用性。在安全方面，有关部件故障或意外的资料通常可供查阅(例如通过测试，我们可以估计机械/电子元件的寿命周期) ，而有关安全意外的资料则可公开收集(新闻 -

24章2. 安全与保安/网络安全的比较

文件、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有关的风险的可能性因子。而对于安全性来说，关于安全事件的信息通常不是所有都可以访问的[68]。此外，攻击成功的可能性在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。这使得在安全学科中进行定量评估变得困难。在进行估算之后，可能性和严重性被合并为一个风险等级。通常，组合可以通过使用风险估计表来完成。(例如表2.2)

在风险评价中，决策者根据风险分析的结果，决定哪些风险可以忽略，哪些风险应该处理。最高的风险将首先以最高的优先级进行处理，较低的风险将被忽略或稍后进行处理。

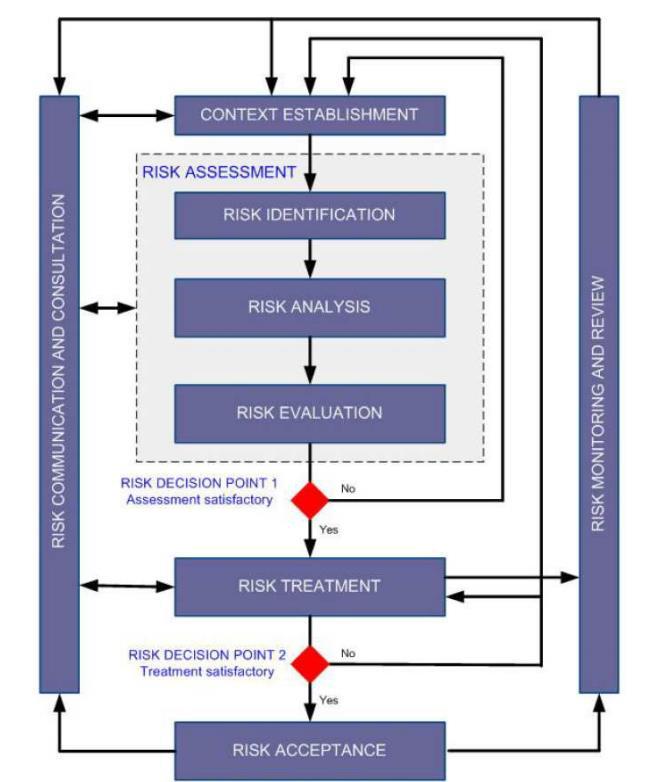


图2.1: ISO 27005风险管理框架

除了风险评估，风险管理还可以包括其他活动: 背景

|  |  |
| --- | --- |
| 2.3安全和安保的不同方面 | 25 |

机构设置、风险处理、风险沟通。上下文建立的目的是为风险评估准备所有必要的输入信息(如操作、系统、制定风险评估准则、风险接受准则等)(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] ,

风险治疗是指通过实施不同的治疗方案来降低风险评估后的风险。传统上，有四种治疗选择: 风险规避，风险降低(或减轻) ，风险接受和风险转移[68]。风险沟通是安全管理者与其他利益相关者(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展示了安全信息风险管理 ISO 27005标准提出的风险管理的完整框架。这个框架与同一组织的另一个一般风险管理指南-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要影响。它们不仅被认为是系统设计的补充，而且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，会导致冗余、多样化和子系统或部件的物理分离[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分割，其中组件根据其功能和安全风险实际上是分开的。这些措施或策略的实施对系统架构有着巨大的影响。因此，在设计过程中越早考虑安全和安保要求，它们的实施就越有效，财务效率也就越高。这个想法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。为了考虑到设计过程中每个步骤的安全问题，标准 ARP4754提出了第二个 v 循环过程，其中包括安全要求的识别、实施和验证(ARP4754标准在航空业中被广泛用作开发指南)。如图2.2所示，两个过程并行展开。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有关的第三个 v 周期流程，这是在 ED-202A/DO-326A [94]标准中提出的。网络安全过程与另外两个过程同时进行。

2.3.4手术与人为因素

安全和保安不仅应该在系统开发中考虑，而且应该在操作中考虑。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维护起着重要作用

26第二章安全与保安/网络保安的比较



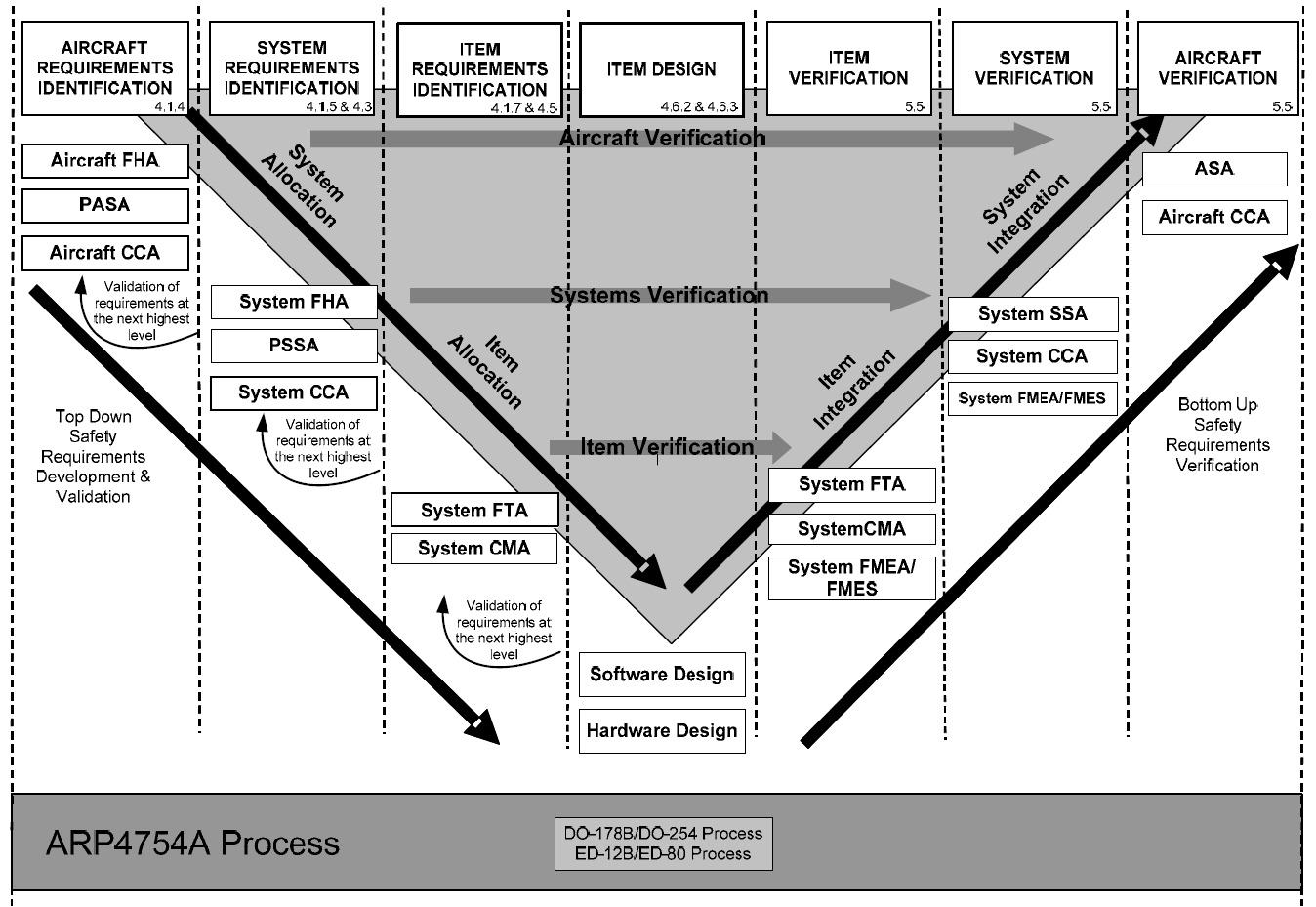


图2.2: 标准 ARP4754中的双 v 循环过程[75]

安全操作[95]和安全[96]。一方面，这些活动被认为是减少风险的预防措施。另一方面，这些活动有助于产生操作反馈，以开发新的技术措施或更新。除了这些活动外，员工培训、制定应急计划和定期测试演习也是确保系统在运行中的安全和保安的其他活动[97]、[98]、[92]。这些活动处理操作中的人为因素，这被认为是安全和安全事件的重要来源。在安全方面，三里岛事件是一个典型的核事故造成的故障，引起了人为因素的关注[68]。20世纪90年代初，在黑客 Mitnick 实现了社会工程攻击之后，人类因素在安全中的作用(网络安全)得到了承认。

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 | 27 |

这个标准是自从20世纪80年代计算机系统在工业中越来越多的使用以来发展起来的。一方面，采用计算机为基础的系统提出了许多安全优势，以及功能改进和经济效益。另一方面，这种采用使系统复杂性增加，并在设计这些系统以防止危险故障方面带来挑战[100]。IEC 61508指南在所有 e/e/PE 安全相关系统中尽量减少这些故障。该标准有助于建立要求，以确保系统的设计、实施、运行和维护能够提供所需的安全完整性等级(SIL)[101]。

ARP4754、 ARP4761构成了航空电子系统安全分析和开发的指南。其中，ARP4754标准在高度集成的航空电子系统中指导适航认证过程。硬件和软件的详细开发过程分别在 DO-254标准和 DO-178C 标准范围内进行。DO-254和 DO-178标准与 ARP4754标准之间的接口是 de-development Assurance Level (DAL)。数据分析处理由 ARP4754中提到的进程分配给软件/硬件系统，并由 DO-254和 DO-178C 中提到的进程详细实现。伴随着4754标准，ARP4761标准在风险评估技术方面提供了一个深入的指导，以进行 ARP4754标准中指出的过程。为了进行风险评估过程，使用了不同的技术，如故障树分析，马尔可夫分析，故障模式效应分析[102]。

特定操作风险评估(SORA)是一种针对无人机操作的风险评估方法。该方法被欧洲航空安全局(EASA)认可为满足欧盟要求的一种手段。一方面，这种方法为无人机操作员和航空当局提供了行政过程(如操作验证)中的通信工具[103]。另一方面，这种方法为无人驾驶飞机制造商、硬件/软件制造商提供了一种工具，以便在开发的早期阶段预测与安全有关的必要要求[103]。现在，SORA 方法集中在安全方面，但忽略了安全方面。这种方法的更详细的描述见[104]。

2.4.2保安

ISO 27005标准这个标准在2.3.2中有部分解释。我们提醒大家，这是一个组织实施信息安全风险管理的指南。这个标准没有提供具体的风险管理方法，而是构成了风险管理过程的框架[90]。该框架由六项活动组成: 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/评估。除了组织内的资讯保安外，ISO/IEC 27005亦被视为确保网络实体系统的网络安全的指引，在这些系统中，资讯科技部分和实体部分同时存在并相互作用。

28第二章安全与保安/网络安全的比较

IEC 62443是一个工业风险管理标准，用于确保工业自动化和控制系统(IACS)的安全。该标准提供了开发、集成和评估网络安全威胁组件的过程和最佳实践。Iec62443以 iso27005系列的概念为基础，并加以改进，以适应操作技术(OT)与资讯科技(IT)之间的差异[83]。然而，物联网设备与 IACS 的整合加速了 OT 与 IT 的融合，给 IACS 带来了新的网络安全威胁。因此，Leander 等[105]认为，在某些情况下，目前的 IEC62443标准不足以应对物联网设备给 IACS 带来的新的安全威胁，例如处理跨区域通信和软件更新。

ED202A/DO326是适航安全程序指南，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)共同制定。本文件的目的是在 APR4754标准所界定的当前飞机开发和认证过程中增加新的程序，以处理故意未经授权的电子威胁。适航保安程序包括三个主要部分: (1)认证活动; (2)风险评估相关活动(相当于 ISO/IEC 27005标准中的上下文建立和风险评估活动) ; 及(3)保安发展活动(相当于 ISO/IEC 27005标准中的处理活动)[106]。ED202A 标准之后是 ED203，更详细地解释了这些活动。

协调风险分析方法(MEHARI)是一种开源的信息风险管理方法。它是由 CLUSIF (法国信息安全俱乐部)开发和维护的，CLUSIF 是自1990年代中期以来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、程序和具体实例，而且还提供了关于脆弱性、安全事件和安全解决方案的知识数据库; 评估安全服务质量的调查表。因为 MEHARI 最初的应用领域是“组织中的信息安全”，所以现有的数据库和支持工具适用于这个领域。然而，CLUSIF 也为建立一个新的知识库提供了指导，以使 MEHARI 适应其他特定系统，如工业自动化和控制系统(IACS)、监控和数据采集与监控系统(SCADA)等[108]。

电子安全汽车入侵保护应用程序(EVITA)[109][110]是一个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。该项目的目标是设计，验证，原型一个模块化，成本效益高的安全解决方案，以保护敏感数据的汽车车载网络组成的电子控制单元(ECUs) ，电子传感器和电子执行器。为此，该项目提出了一种安全需求分析的方法。尽管符合 ISO/IEC 标准

|  |  |
| --- | --- |
| 2.5. 安全分析技术 | 29 |

27005标准没有提及，也不是一个目标，该方法可以涵盖 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 HAZOP

危害与操作(HAZOP)是一种系统的和结构化的技术，在世界范围内用于识别系统的危害及其操作问题。换句话说，这种方法旨在识别与给定系统相关的风险情景。该方法基于一个重要的论点，即风险情景是由系统偏离预期设计引起的[111]。因此，为了确定场景，HAZOP 集中于寻找偏差(状态，行为，...) ，并推断出这些偏差的后果。偏差识别过程依赖于使用指导词(较少、较多、较晚、较早、较快、较慢等)结合工艺参数(如温度、流量、压力)[112]。基于这些词语，负责人集思广益，将不同的偏差放在一起，比如“发动机运行速度比设计意图快”。由于只关注设备和工艺参数的故障，这种方法没有考虑与人为因素相关的场景。HAZOP 分析最早出现于20世纪60年代，目的是确定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 已经扩展到其他类型的设施。CHAZOP (计算机危害与可操作性分析)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、局部控制面板)[113]。这个版本提出了新的指导词和参数，如没有信号，超出范围信号，没有电源，没有通信，i/o 卡故障，软件编程，不正确/不充分和网络攻击[113]。EHAZOP (电气危害与可操作性分析)是 HAZOP 技术的另一个外推版本，但它致力于电力系统(发电、变电、输电和配电...)。这个版本还提出了新的指导词，如电源浪涌，24伏直流供电故障，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

安全完整性等级(SIL)是指工业过程中为达到可接受的风险水平而采取的安全措施的必要性能等级。所需的安全性能是以按需失效概率(PFD)来衡量的。SIL 一词在世界范围内使用，并在 IEC 61508中标准化，为安全仪器系统的设计、安装、操作、维护和测试提供了指导方针[114]。如表2.3所示，该标准提出了具有不同 PDF 值的4级 SIL。在安全过程中，SIL 被分配到基于风险降低量的安全措施中

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 30 | 第二章安全与保安/网络安全的比较 | | | | | | | | |
|  |  |  |  | | |  | | |  |
|  |  | 招标 | 低需求 | | | 高需求 | | |  |
|  |  | SIL | PDF 平均值 | | | 失败/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中的 SIL 值[114]

是保证系统安全的必要条件。根据 Summers [115]的工作，SIL 任务有以下几个基本技术:

修改的 HAZOP 是 HAZOP 分析的扩展。这是一个基于团队对严重程度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。因为这种方法是非常主观的，它要求团队成员不仅了解正在考虑的系统，而且了解公司可接受的风险容忍度。此外，它还需要 SIL 分配团队中各个项目的人员之间的一致性。

SIL 后果

4 社区死亡的可能性

3 多人死亡的可能性

2 潜在的重大伤害或一人死亡

1 潜在轻伤

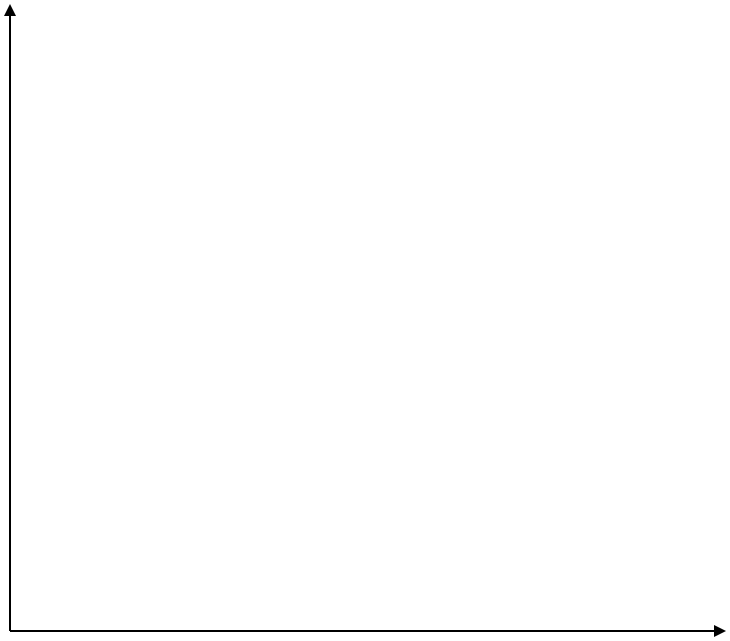
表2.4: 基于结果的 SIL 分配[115]

仅结果评价是一种基于结果严重性而忽略风险情景可能性的 SIL 分配技术。因此，所有导致可能死亡的情况都将被分配相同的 SIL，而不考虑其可能性。这是最简单的技术，因为可能性往往难以估计。当历史数据有限时，这种技术是值得赞赏的[115]。表2.4显示了 SIL 分配的表决策示例。

风险矩阵是炼油，化工和石化公司中最常见的技术之一[115]。与 result Only 不同，这种技术是基于 SIL 风险情景的严重程度和可能性的相关性。为了成功地应用这种技术，必须充分理解过程、系统和相关的风险，以便能够对可能性和严重程度做出定性估计。SIL 分配的风险矩阵的一个例子如图2.3所示

风险图是诊断 SIL 的一种定性技术。在这种技术中，SIL 通常基于四个因素进行分配: 后果或严重后果(c) ; 频率和

|  |  |
| --- | --- |
| 2.5. 安全分析技术 | 31 |



|  |  |
| --- | --- |
| 后果严重 | 小范围严重灾难 |

|  |  |  |
| --- | --- | --- |
| 3 | 3 | 没有 |
|  |  | 可接受的 |
|  |  | 风险 |
| 2 | 3 | 3 |
| 1 | 2 | 3 |
| 没有 | 1 | 2 |
| 必须的 |  |  |
|  |  |  |
| 很低 | 适度 | 很高 |

**可能性**

图2.3: ANSI/ISA 84.00.01标准中 SIL 分配的风险矩阵

如图2.4所示，暴露时间(f)、避免发生危险事件的可能性(p)及发生意外事件的可能性(w)[114]。最后三个因素: f，p，w 的组合表示风险情景的可能性。换句话说，SIL 总是根据风险的性质来分配: 结果和可能性，然而，可能性被它的贡献者参数(f，p，w)所取代。

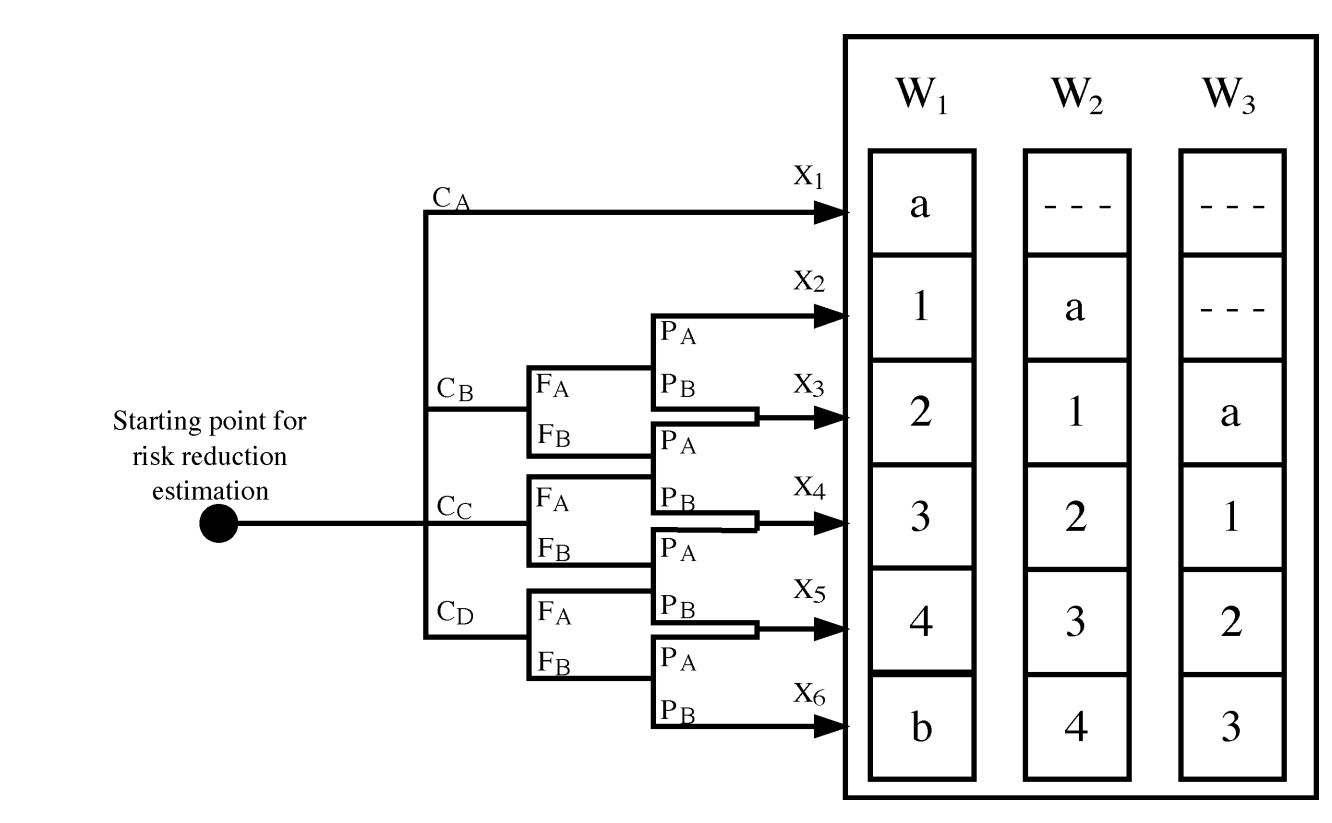
定量评估: 在这种技术中，安全措施的 SIL 是基于对相关事件可能性的定量估计来确定的。该方法需要彻底了解事件的潜在原因以及每个潜在原因的估计概率。因此，这种方法适用于有关事件的历史信息非常有限的情况，因此对可能性的定性确定非常困难[115]。为了确定所需的 SIL，接受或可容忍的风险概率除以计算的过程需求如下:

按需失败概率 = 可容忍的风险概率

过程需求

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程度和可能性相关，并可用于风险评估活动。然而，这些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，代表了系统或过程的本质。当安全措施实施时，风险水平可以改变(我们希望它降低到可接受的水平)。同时，SIL 代表性能

第三十二章安全与安全/网络安全的比较



A = 没有特殊的安全要求，b = 单一措施不够充分,-= 不需要

图2.4: SIL 分配的风险图[114]

安全措施的目标。当选择实施一项安全措施时，SIL 不会改变，但提出了一个问题:”选择的措施是否满足所要求的 SIL.

2.5.3故障树分析

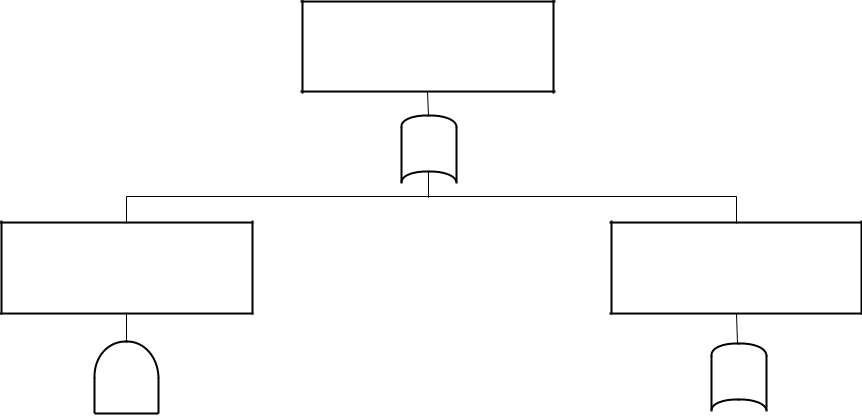
故障树分析(FTA)是一种基于图的系统安全分析技术。它最初是由贝尔公司在20世纪60年代开发和应用于航空航天应用[86] ，然后它成为流行和广泛应用于其他关键系统，如核动力，汽车，医疗系统[116]。这种技术有助于分析人员评估给定的系统，并了解和预防相关的风险。通过应用故障树，分析师可以创建一个可视化模型，说明设备故障和人为错误是如何导致事故发生的。基于这个模型，分析师可以识别出最危险的情况，并提出安全措施或建议。因此，FTA 通常在系统开发期间进行，其结果通过预测和预防未来问题来影响设计[93]。

FTA 过程包括两个步骤。第一步是展示不同的部件故障或特定的环境条件如何结合起来导致给定的系统故障。这一步是从选择一个不想要的事件(UE)作为图的顶部节点开始的。UE 是

|  |  |
| --- | --- |
| 2.5. 安全分析技术 | 33 |

任何被认为是令人反感和不想要的事件。然后，通过演绎推理，有助于 UE 的中间事件被识别出来并作为分支节点放入图中。分支节点和顶部节点通过不同的逻辑门进行连接，如图2.5所示的 OR，AND，XOR。重复演绎推理过程，以确定已识别的中间事件的原因，直到达到不能分解为较小事件的基本事件。在构造树图之后，应用布尔代数来识别截集，这些截集是导致 UE 的必要和充分的基本事件的最小组合。第二步是根据 cut-set 中基本事件的概率计算 UE 的概率。这一步骤的结果不仅有助于分析人员识别 UE 的可能性全局性，而且还有助于根据事件对 UE 概率的贡献来识别故障树中所有事件的重要性。

传统的故障树方法虽然取得了很大的成功并得到了广泛的应用，但也存在一定的局限性。传统的 FTA 无法在构建树图的过程中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，假设有两种情况:”如果组件 a 在 b 失效之前失效，系统就不会失效”和”如果组件 b 在 a 失效之前失效，系统就不会失效”; FTA 无法区分这两种情况。为了克服这个限制，提出了不同的方法来创建一个动态故障树分析，例如新的逻辑门[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 FTA 无法克服基本事件失败数据的不确定性。对于许多复杂和大型的系统，通常难以精确确定所有基本事件的概率。这导致了一个不可靠的结果。为了克服这个限制，Tanaka 等[121]提出在 FTA 中使用模糊理论。然后，这个想法被其他研究人员采用，进一步发展模糊故障树分析(FFTA)[122][123] ，[124]。



火灾失败

保护系统

或者

火灾探测器

系统失效

灭火

系统失效

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 还有 | | | | |  |  |  | 或者 | | | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 烟雾失效 | |  |  |  | 热量失效 | |  | 没有水 | |  |  | 喷头 | |
| 探测器传感器 | |  |  |  | 探测器传感器 | |  | 自动喷水灭火系统 | |  |  | 阻塞 | |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

图2.5: 故障树分析示例[125]

第二章安全与安全/网络安全的比较

2.5.4事件树

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| IE | |  |  |  | 安全措施 | | | | | |  |  |  |  | 结果 |  |
|  | |  |  |  |  |  |  | |  |  |  |  | |  |  |  |
| 煤气泄漏 | | Gas detection 气体检测 |  |  | 隔离阀 a |  | 隔离阀 b | | | |  | 放下 | |  |  |  |
|  |  |  |  |  | 关闭 |  | 关闭 | | | |  | 阀门打开 | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | |  | |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 成功 | | | |  | 结果1 |  |
|  |  |  |  |  |  |  | 成功 |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 成功 |  |  |  | 失败 | | |  |
|  |  |  |  |  |  |  |  |  |  |  | 结果2 |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 成功 | | |  |  |
|  |  |  |  |  |  |  | 失败 |  |  |  | 结果3 |  |
|  |  | 成功 |  |  |  |  |  |  |  | 失败 | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 结果4 |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 成功 | | | |  |  |
|  |  |  |  |  |  |  | 成功 | |  |  | 结果5 |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 失败 |  |  |  |  |  | 失败 | | |  | 结果6 |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 成功 | | | |  |  |
|  |  |  |  |  |  |  | 失败 | | |  | 结果7 |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 失败 |  |  |  |  |  |  |  |  | 失败 | | |  | 结果8 |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | 结果9 |  |
|  |  |  | 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，在20世纪70年代被引入到核反应堆项目中[127] ，然后被其他行业如航空、化学等采用。这种技术通常应用于系统设计和开发的早期阶段，以确定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]。它有助于确定归纳和评估由初始事件(IE)开始的潜在事故中的事件序列(或风险情景)。该方法以图解法为基础，着重从逻辑和概率的角度说明由工业工程引起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: Initial Event (IE)、 Pivot 事件和 Outcome。IE 位于图表的顶部，表示系统中的扰动(如火灾、气体泄漏、压力损失) ，需要操作员的响应或安全系统的响应，以避免不希望的后果。Pivot 事件是在图形树分支(有时称为分支点)中紧跟 IE 的直接点。Pivot 事件代表了安全系统在响应初始事件时的成功或失败。结果是树状图的终点，表示某些类型的损失，如人员的生命损失或伤害/疾病、设备或财产的损失或损失、任务的失败，其后果从轻微到重大不等。事件树的一个例子如图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。初始事件和枢纽事件的概率可以从历史数据或其他分析结果(如故障树分析)中揭示[126]。Outcome 的概率是通过将 IE 和 pivot 事件的概率相乘来计算的。

|  |  |
| --- | --- |
| 2.5. 安全分析技术 | 35 |

2.5.5蝴蝶结分析

领结分析是一种基于图形的安全风险评估技术，已经在石油天然气、航空、矿业等高危行业得到广泛应用。这种技术通过蝴蝶结形状的图形来模拟安全事故。该图的主要元素包括顶级事件、威胁、后果和障碍。Top 事件是领结的中心点，它通常被定义为某种损失，如石油和天然气中的“失控”和航空中的“失控”[128]。威胁位于 Top 事件的左侧，代表 Top 事件的原因，而后果位于 Top 事件的右侧，代表 Top 事件的后果或事故的后果。每个领结图只有一个 Top，即使这是由多种威胁引起的，并导致多种后果。障碍在 Top 事件的两边。它们说明了计划预防，控制或减轻事故的不同措施[129]

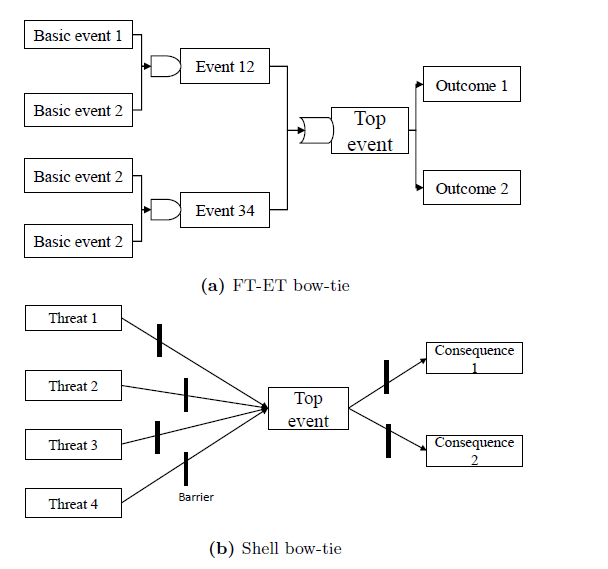
。

图2.7: 蝴蝶结图示例[128]

虽然领结一直很流行，但它缺乏一致的方法[128]。至少，我们可以认识到至少有两种方法也被称为“蝴蝶结分析”，它们在图形结构、目的、风险量化等方面是不同的。第一种方法是错误树和事件树的组合，如图2.7 a 所示。在这种方法中，领结图从一个故障树开始，在一个顶部事件中收敛，然后使用一个事件树发散。这种方法中的障碍通常不直接在图表中显示，而是以“失败/成功”的形式表示

36第二章安全与安全/网络安全的比较

安全措施事件。利用故障树和事件树分析的优势，这种方法允许分析师分解并详细分析可能发生的事故。因此，这种方法被用来计算结果的概率[130] ，[131]。在 Salvi 等[132]的工作中，该方法的定量结果被用来证明在安全完整性等级(SIL)下安全措施的性能要求。另一方面，这种方法与传统的 FT 和 ET 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]。第二种方法是壳牌的领结。这种方法不是 FT 和 ET 的结合，而是提供了一个简单的领结图，如图2.7 b 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，而不需要任何中间事件。顶部事件会在左侧产生单一的后果。在这种方法中，屏障元素直接显示在图的左右两侧。与基于 FT-ET 的图相比，壳结构图具有较高的抽象层和较少的具体信息，计算结果概率的能力较弱。然而，贝壳领结更容易理解。它有更少的符号，并且比基于 FT-ET 的图表更清楚地说明了安全屏障。这使得外壳领结成为沟通[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”的好工具。

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的技术，用于建模系统的状态转移和计算(故障)状态发生。系统状态是子系统或组件(工作/失败)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，如(a 工作，b 工作) ，(a 失败，b 工作) ，(a 工作，b 失败) ，(a 失败，b 失败)。在马尔可夫分析中，假设系统状态随时间不断地从一种状态变化到另一种状态，未来的系统状态只依赖于当前的状态。这些状态转换是由状态转换图来模拟的。该图显示了系统的不同状态，转换方向伴随着转换速率，如图2.8所示。状态转换图用于建立一组一阶微分方程，它表示不同状态随时间变化的概率之间的关系。通过解决这组方程，我们有失败状态的概率。

与其他技术相比，马尔可夫分析既有优点也有缺点。它的优点在于，它可以考虑到一些其他技术不可能考虑到的方面，如时间、修复活动、容错[93]。因此，这是进行精确定量分析的有力工具[138]。然而，这种技术相当复杂，需要分析人员具有良好的数学知识。此外，当所考虑的系统变大时，图表可能很大，难以阅读和跟踪[93]。基于这些原因，Bouissou 等[139]在2003年提出了布尔驱动的马尔可夫过程(BDMP)——故障树分析和马尔可夫分析的结合。这种技术利用了两种起源的优点: (1)容易理解,

|  |  |
| --- | --- |
| 2.5. 安全分析技术 | 37 |

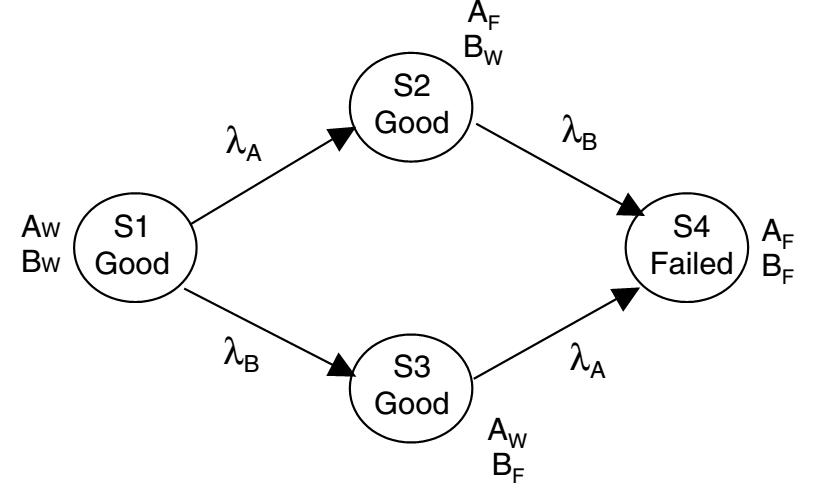


图2.8: 状态转换图[93]

创建和跟踪(故障树) ，(2)精确定量(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，而不是计算定量概率。为了识别危险，PN 分析提供了一个工具，可以在广泛的抽象层次上对系统进行图形化建模。与马尔可夫模型一样，PN 模型也可以描述不同的系统状态(包括故障状态) ，并处理时间、状态转换、修复活动。这些模型的优势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，它在系统安全分析中的应用并不像 Faul 树或 Event 树等其他技术那样广泛。随着系统规模的增加，PN 模型迅速变得庞大和复杂[93]。因此，它的使用很少应用于大型系统，并且仅限于软件控制系统的检查。

2.5.8 FMEA

失效模式和影响分析(FMEA)是一种自下而上的技术，用于分析系统的安全性，并对降低风险的行动进行优先排序。它最初于1949年由美国陆军引入，然后被广泛用于分析各种工业的安全性，如航空航天、汽车、核能、机械和医疗行业[140]。在 FMEA 中，分析侧重于检查/识别所有部件故障及其对作业，系统和环境的影响。然后，组件故障率和影响的严重程度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[141]提出了一个解决方案，从 UML/SysML 编写的系统设计中自动生成 FMEA 分析。这个解决方案有助于改善系统设计和分析过程之间的交互。在失效模式、影响和关键性分析(FMECA)的更详细版本中，信息

38第二章安全与安全/网络安全的比较

在评估风险时，还考虑了检测元件失效的能力。由于需要关于部件的信息(如故障模式、故障率) ，故障模态分析通常在系统的详细设计可用或新的详细设计发生变化时进行。这种技术的优点是相对容易理解，执行费用低廉，并提供有意义的结果[93]。但是，它也有一个弱点。第一个是分析质量取决于用户的体验，所以结果可能是主观的，不稳定[142] ，[138]。第二个是 FMEA 无法识别所有的风险情景。因为该技术着眼于单个部件故障，而事故可能由组合部件故障引起[93]。

2.5.9总结

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 技巧 |  | 风险评估 |  |  |
| 风险识别 | 风险分析 | 风险评估 |  |
|  |  |
|  | 基于指导词汇 | X | 与标准比较 |  |
| HAZOP | 表格 |  |
| (从其他来源) | 识别风险等级 |  |
|  | 原因-危害-后果 |  |
|  |  |  |  |
| SIL 分析 | X | X | 多方法 |  |
| 识别目标性能 |  |
| (不是焦点) | (从其他来源) |  |
|  | 措施 |  |
|  |  |  |  |
| 故障树 | 演推理, | 数量 | X |  |
| 图形模型 |  |
| 概率传播 | (不是焦点) |  |
|  | 基本事件-顶级事件 |  |
|  |  |  |  |
|  | 归纳推理 | 数量 | X |  |
| 事件树 | 图形模型 |  |
| 概率增殖 | (不是焦点) |  |
|  | 首要活动-成果 |  |
|  |  |  |  |
| 领结 | FT 与 ET 的结合 | FT 与 ET 的结合 | X |  |
| 说明安全屏障。 | (不是焦点) |  |
|  |  |  |
| 马尔可夫过程 | X | 数量 | X |  |
| (不是焦点) | 系统状态概率 | (不是焦点) |  |
|  |  |
| Petri 网 | X | 数量 | X |  |
| (不是焦点) | 系统状态概率 | (不是焦点) |  |
|  |  |
|  | 归纳推理 | X | 与标准比较 |  |
| FMEA | 表格 |  |
| (从其他来源) | 识别风险等级 |  |
|  | 失败模式-效果 |  |
|  |  |  |  |

表2.5: 风险评估技术比较

以上，我们介绍了风险评估中广泛使用的八种基本技术。每个方法都集中在风险评估的一些任务上(见表2.5)。对于风险识别任务，我们可以使用 HAZOP，Fault Tree，Event Tree，Bow-tie 和 FMEA。对于风险分析任务，故障树，事件树，蝴蝶结，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 比其他技术提供了更详细的说明。此外，每种技术在不同方面都有优势，如沟通、推理、文档等。因此，在一个关键系统的风险评估中，各种技术可以结合使用。例如，FMEA，Fault Tree，Hazop 可以用来进行初步的系统安全评估(PSSA)

|  |  |
| --- | --- |
| 2.6安全分析技术 | 39 |

- 在 ARP 4761航空电子系统标准中定义[143]

2.6安全分析技术

2.6.1从 SIL 水平到 SAL 水平

与安全纪律类似，安全纪律包括设计、实施和验证某种保护。因此，SIL 的概念在安全学科中是有用的。然而，最初的 SIL 分析在安全纪律方面有一个局限性[144] ，[145]。SIL 因子仅代表按需失效率方面的目标性能，而安全性通常需要对基于网络的攻击和可利用的软件或硬件条件具有弹性。Kube 等[144]在 SIL 概念的基础上提出了一个安全保证级别(Security Assurance Level，SAL)的基本概念，SAL 代表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，该标准涉及组织的操作技术(OT)领域的工业控制系统的网络安全。这些标准使用安全保证级别(SALs)来描述确保系统安全所需的保护。安全保护由七个基本要求描述: (1)访问控制，(2)使用控制，(3)数据完整性，(4)数据保密性，(5)限制数据流，(6)对事件的及时响应，以及(7)资源可用性。随着基础要求的严格程度的提高，SAL 被定义为4个不同的级别(1、2、3、4) ，如表2.6所示。

|  |  |  |  |
| --- | --- | --- | --- |
| SAL | 描述 |  |  |
|  |  |
|  |  |  |  |
|  | 防止因果或偶然的侵权行为 |  |  |
| SAL 1 | 因果或偶然的侵权行为通常是由于安全应用松懈造成的 |  |  |
|  | 政策 |  |  |
|  | 使用简单方法防止故意侵权 |  |  |
| SAL 2 | 这意味着攻击者不需要安全性、域或 |  |  |
|  | 被攻击的特定系统 |  |  |
|  | 使用复杂手段防止蓄意侵权 |  |  |
| SAL 3 | 攻击者必须具备安全和域操作方面的优势知识 |  |  |
|  | 目标系统的知识来进行这种侵犯 |  |  |
|  | 使用复杂手段防止蓄意侵权 |  |  |
| SAL 4 | 扩展资源 |  |  |
|  | 与 SAL 3类似，但攻击者拥有高性能等扩展资源 |  |  |
|  | 计算机，延长的时间 |  |  |
|  | 表2.6: IAS99/IEC62443中的 SALs [145] | |  |

40章第二章安全与保安/网络安全的比较

2.6.2安全中的 HAZOP

正如前面提到的，危险与操作(HAZOP)的基本原理是系统的行为偏差导致系统的不安全状态。为了使这种技术适应安全规则，它需要一些修改。Winther 等[146]提出了一种基于 hazop 的技术来识别与给定关键系统相关的不同安全威胁。安全威胁是基于新的指导词和安全属性的负面(如披露，操纵，拒绝)的组合来识别的。Wei 等[147]提出了另一种基于 hazop 的嵌入式系统方法。这种方法使用计算机应急响应小组(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[148]和 Daruwala 等[149]建议使用原来的 HAZOP 和用例模型来进行软件和硬件的安全性分析，而不是修改或改变原来的指导词。在这种方法中，指导词的手段应该被更广泛地理解，并且要求用户更有创造性。Hazop 概念的使用迫使分析师考虑不寻常的情况。然而，与预定义的指导词列表相关的抽象层也可能隐藏不会被考虑的风险[68]。

2.6.3从故障树到攻击树

攻击树分析是一种基于树图的技术，用于识别针对给定系统的可行攻击，并对安全对策进行优先级排序。这种技术被认为是安全技术故障树分析(FT)对安全学科的改编[148][68]。AT 分析的概念与 FT 分析的概念非常相似。攻击树将攻击的目标描述为树的顶部节点。攻击者达到攻击目标所需要达到的中间目标由图的中间节点表示。图的结尾是不同的叶子节点，代表基本的攻击行为。在 FT 分析中，节点只由两个逻辑门(AND/OR)连接，而不是至少由四个逻辑门连接。AT 分析的概念最早由 Schneier [150]于1999年提出，并在支付系统的背景下进行了说明[68] ，[151]。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对对策进行了优先排序。自从第一次演示以来，AT 树已经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[156] ，Kordy 等[157]将传统的攻击树图扩展到攻击防御树，以建立安全对策的模型。关于对策和风险评估，Jürgenson 等[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。模糊理论[159] ，博弈论[160]也被提出来改进分析。

|  |  |
| --- | --- |
| 2.6安全分析技术 | 41 |

2.6.4基于 fmea 的技术

失效模式效应分析是一种安全分析技术，用于识别和理解可行失效模式的影响。由于系统性、易于理解和“自我记录”，这项技术激发了安全学科的工作灵感。文献中介绍了几个采用 FMEA 的作品，并对其进行了一些修改。例如，Aagedal 等[161]在 CORAS European 项目的安全环境中使用了 FMEV; Gorbenko 等[162]提出了用于 Web 服务分析的入侵模式和影响分析(IMEA) ; Schmittner 等[163]将 FMEA 用于汽车安全; Bowles 等[164]提出了用于软件分析的威胁影响分析(TEA)。这些工作的原则是，他们的重点不是故障模式，而是检查可行的威胁/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，并且是由此推断出来的。Schmittner 等[73]提出了失效模式、脆弱性和影响分析(FMVEA)技术，用于系统的协同分析方法(包括安全性和安全性)。作者提供了一个安全-安全风险情景的可视化模型，以及进行安全和安全分析的 FMEA 的详细过程。

2.6.5安全性分析

领结(BT)分析是一个强大的工具，可以直观地模拟风险场景，并在不同的利益相关者之间进行交流。因此，采用这种技术进行安全分析是很有意思的。SANS Institute 公司的一份报告[165]认为，BT 分析可以用同样的方式进行安全分析，而不会改变任何概念。美国海岸警卫队还发布了一份关于如何应用 BT 技术识别和应对针对海上运输系统的网络攻击的指南

在本指南中，网络攻击以高度抽象的方式被提及，例如黑客活动家、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 蝴蝶结来建模视觉攻击路径和防御措施。然而，与其他安全分析技术相比，领结分析对安全学科的适应性相当有限，特别是在学术领域。通过使用 Google Scholar 工具，我们发现这方面的工作很少。与这个主题相关的最重要的工作是由 Abdo 等人和 Bernsmed 等人完成的[168]。Abdo 等人。

将 FT-ET 领结与 AT 相结合，对工业控制系统进行安全-安全协同分析。这种方法的优势在于，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情景。Bernsmed 等[168]使用通用的 Shell BT 图形可视化恶意活动，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程度来量化风险的方法。

42第二章安全与保安/网络安全的比较

2.6.6安全的马尔可夫过程

马尔可夫过程(BDMP)是安全学科中使用的一种精确的风险量化工具。这种技术也用于安全学科。Ye 等[170]使用马尔可夫过程来观察和分析计算机和网络系统的网络安全风险。这项工作的结果用于构建一个实时的网络攻击检测系统。小林等[171]提出了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。一种是对威胁传播进行建模并发现隐藏的风险，另一种是对系统管理员实现的修复过程进行建模。这个评估的结果被用来建立一个自动生成工具的防御方案。Lakhno 等[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性。与安全学科一样，马尔可夫过程的局限性是阅读，跟踪和建模复杂系统的困难。由于这些原因，Piètre-Cambacédès 等[173]将布尔逻辑驱动的马尔可夫过程(BDMP)概念从安全域调整到安全域。代替故障树，BDMP 的安全结合了马尔可夫过程和攻击树。攻击树本质上是静态的，只能检查独立事件而不考虑时间，而 BDMP 是动态的，可以检查简单的依赖关系。BDMP 允许攻击序列的建模，也允许安全对策的建模，如攻击检测[174]。

2.6.7 petri 网安全

Petri 网在安全性分析中的应用是由 McDermott 在2005年首次提出的

在这项工作中，作者提出了在渗透测试的背景下建立网络安全风险的模型，以及 Petri 网可以结合攻击树等其他基于图的技术难以实现的缺陷建立复杂攻击模型的论点。在 McDermott 的工作之后，基于 petri 网的安全技术在许多方向和不同的工业领域得到了进一步的发展。为了减少 Petri 网在复杂性和时间消耗方面的缺点，Zhou 等[176]提出了一种在 Internet 入侵分析中覆盖 Petri 网攻击树的方法。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[177]提出结合 Petri 网和大数据分析来评估网宇实体系统的网络安全性。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[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 网技术也被扩展到检查攻击时间(例如，时刻，持续时间)。

|  |  |
| --- | --- |
| 2.7. 安全和安保综合办法 | 43 |

2.7安全保障综合方法

正如在前面的章节中提到的，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。它们都指的是对系统的保护。安全保护的丧失可能导致安全的丧失。Lisova 等[179]认为，“一个连接的安全生命攸关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相同的概念。许多安全评估技术起源于安全领域的技术。最后，安全性和安全性都是系统开发和运行中必不可少的关注点。因此，自然而然地将安全和安保方面整合到一个综合的风险评估方法中。在学术界，有一些与这个主题相关的著作。例如，Reichenbach 等[180]介绍了一种基于具有安全完整性水平(SILs)的威胁脆弱性和风险评估(TVRA)技术的集成方法。这种方法允许解决安全问题对安全的影响。Plósz 等[181]提出了一种将 FMEA 技术与 STRIDE 模型相结合的方法——安全威胁分类(欺骗、篡改、拒绝服务、数据泄露、拒绝服务攻击、提升特权)。这种综合方法可以通过同时考虑安全评估和安全风险评估的共性来减少时间和工作量。Fovino 等人。

建议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，同时考虑到潜在的恶意攻击。基于同样的理想，Abdo [169]使用攻击故障树来共同分析安全性和安全性。然而，作者认为，安全方案和安全方案不应该基于相同的概率尺度来处理。因为决策者不能知道不可接受的风险是由安全相关的原因还是安全相关的原因产生的。因此，作者建议根据两项可能性来评估风险水平: 一项是安全性，一项是安全性。Puys 等[183]提出了一种基于安全风险评估评估工业控制系统网络安全的方法。在这种方法中，安全风险评估提供了建模网络安全攻击场景的特性。这种方法利用了这样一个事实，即工业系统通常在安全性方面得到很好的分析。

在行业中，安全与安保一体化的方法才刚刚开始引起人们的重视。例如，DO-326标准是在2015年开发的，旨在将 ARP4761标准中定义的基于安全的过程扩展到网络安全。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而制定的。

2.8结论

本章讨论两个不同的术语: 安全和安全/网络安全。安全指的是意外事件，而安全/网络安全指的是攻击(恶意意图)。To

第二章安全与安全/网络安全的比较

为了解决系统设计或操作中的安全问题，从业人员和研究人员通常使用一个基本概念: 风险——情景的可能性和严重性的组合。我们在文献中发现了不同的方法来评估与安全性相关的风险。在过去，安全和安保是通过分离的方法来考虑的。从上个世纪开始，安全方法学就已经发展起来。自上世纪80年代计算机和网络越来越流行以来，安全(网络安全)方法就已经发展起来。许多安全/网络安全方法是在现有的安全领域的基础上发展起来的。由于安全和安全之间的相互作用，集成方法目前是一个有趣的主题。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考虑。现有的风险评估方法致力于此应用: 特定操作风险评估。然而，这种风险评估方法只考虑安全性，而不考虑网络安全方面。在航空航天工业中，DO-326A 标准中提到了安全风险评估方法。然而，这种方法似乎过于庞大和昂贵，不适用于商用无人机。因此，本文旨在开发针对无人机的安全风险评估方法。第三章介绍了我们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

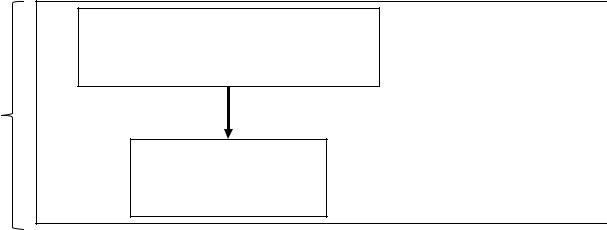
|  |  |  |  |
| --- | --- | --- | --- |
| 3.1 | 引言... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | | 46 |
| 3.2 | 提议的方法..。 | | 46 |
|  | 3.2.1 | 背景建立。 | 47 |
|  | 3.2.2 | 风险识别..。 | 49 |
|  | 3.2.3 | 风险分析和评估。 | 51 |
|  | 3.2.4 | 治疗..。 |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

45

46章3系统网络安全风险管理

3.1简介

正如在第二章中提到的，网络安全在系统开发过程中扮演着至关重要的角色。出于这个原因，许多风险管理方法已经被引入到学术界和工业界。然而，对于过度发展的无人机领域，目前还没有适当的方法。这是我们开发和引进一种网络安全风险管理方法的动机之一，该方法致力于无人机系统(UAS)。此外，通过这项研究，我们的目标是增加网络安全方面的开发过程中的 SOGILIS 公司-我们的工业伙伴。风险管理的输出被用作开发过程的输入，如图3.1所示



风险管理

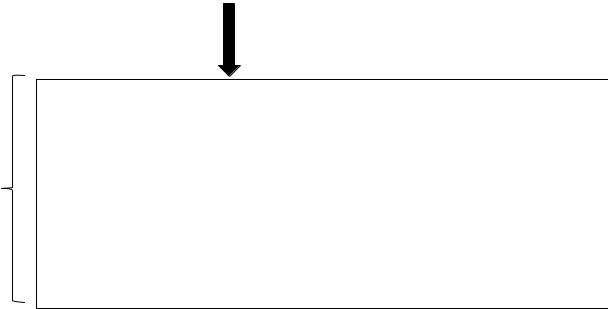
风险管理

方法安全方面

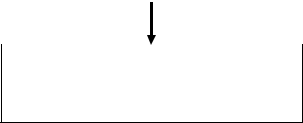
(这项研究的焦点)

保安

规定



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | 系统需求 |  |  |
| DO-178C |  |  | SOGILIS 的方法 |  |
|  |  |
| 标准 |  |  |  |
|  |  |  |  |
|  |  |  |
|  |  |  |  |  |



实施

图3.1: 一般方法

3.2拟议方法

通过激发其他领域现有的风险管理方法，我们开发了一个包括四个主要活动的简单方法。它们是“上下文建立”、“风险识别”、“风险分析和评估”和“治疗”，如图3.2所示。在设立活动的背景下，我们提出了一种收集和整理关于被保护系统情况的所有信息的方法，明确了风险管理的范围。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来识别可能的安全风险的方法。风险分析和评估活动是定义每个已定义风险的优先级。优先级最高的风险需要首先用稳健的解决方案来处理。在最后一个-Treatment 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。这些活动将在本节的剩余部分进行更详细的描述。

|  |  |
| --- | --- |
| 3.2拟议方法 | 47 |

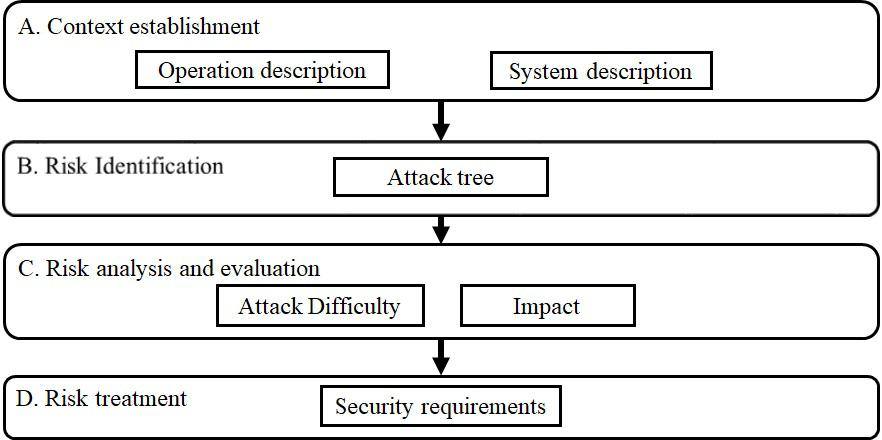


图3.2: 拟议方法的工作流程

3.2.1情境建立

在这种方法中，上下文建立(活动 a)旨在为其他风险评估活动做准备。这项活动包括以下步骤:

操作描述

考虑中的系统描述

3.2.1.1操作描述

这一步骤旨在从操作员的角度尽可能详细地描述已部署系统需要实现的目标和过程。为此，我们利用 JARUS-SORA [184]的指南收集和呈现操作信息如下:

包含所有信息的详细描述，以了解如何，在哪里，以及在哪些限制或条件下部署无人机。

详细描述操作类型(如可视视线或超越可视视线) ，操作员的参与，以及系统在飞行期间的自动化水平。

详细描述系统部署和维护的过程，以及参与这些过程的人员

应急程序的详细描述(如电池耗尽、断开连接)。

关于正在审议的系统的若干网络安全假设、允许缩小分析范围的环境以及忽视几种攻击的情况，例如,”所有工作人员都受到信任，因此内部工作人员故意发起的所有攻击都被忽视”。

48第3章系统网络安全风险管理

注1: 从这段描述中，我们可以提取进一步的信息，例如系统需要执行的功能(例如，按照特定的轨迹，将视频发送回地面控制站-地面控制系统) ，用于分析影响严重程度的参考因素(例如，无人机飞越人群时的死亡人数，无人机运送货物时的经济损失)。

注2: 网络安全假设需要仔细确定; 否则，潜在的攻击可能被忽略。

3.2.1.2考虑中的系统描述

此步骤的目的是获得有关受保护系统的必要知识。这一步着重于收集几种信息: 架构，网络安全环境，接口，功能。

架构: 一个系统可以被分解成子系统。它们包括基本的子系统(自动驾驶仪，ESC 等)和额外的子系统(相机，有效载荷等)。这些元素和它们之间的相互联系应该被识别出来。

环境: 所有人员，可以与所考虑的系统交互的外部系统。例如，一个无人机系统的环境可以由维护人员、制造商、互联网、操作员等组成。对于环境的每个元素，他们的访问能力和角色需要详细说明。

接口: 所有环境元素可以与系统交互的入口点。例如，在无人机的情况下，地面控制站通过 RF 通信向无人机发送指令数据。因此射频通信是无人机的一个接口。

函数: 实现系统目标所必需的所有离散动作(用动作动词描述)。关于系统功能的信息可以从体系结构描述中提供的系统运行信息中推导出来。例如，系统功能可以遵循预先确定的轨道，记录并将视频传回地面站。在功能描述中，它还应该详细说明这个功能的需求。例如，对于“将视频发送回地面站”功能，它应该详细说明视频的预期质量，视频数据的保密性等等。

每个组件或子系统都有自己的架构、功能、接口和环境。因此，所有提到的信息应该在许多抽象的层次上收集。例如，除了无人机的体系结构、接口、功能、网络安全环境外，还需要了解自动驾驶仪、射频模块、摄像机等部分。

注意: 根据开发过程(设计、测试、文档)和系统的状态(正在开发或准备使用) ，这些信息可能存在(文档化)

|  |  |
| --- | --- |
| 3.2拟议方法 | 49 |

或者不是。如果它们不存在，它们应该从现有的信息中推导出来，以确保信息的完整性

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详尽地识别风险。第二个是说明风险的本质及其演变(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，这个方法采用了一个新版本的攻击树 foridentiationthisstep。Processfordebuildrisquesngattacktrees 如图3.3所示。

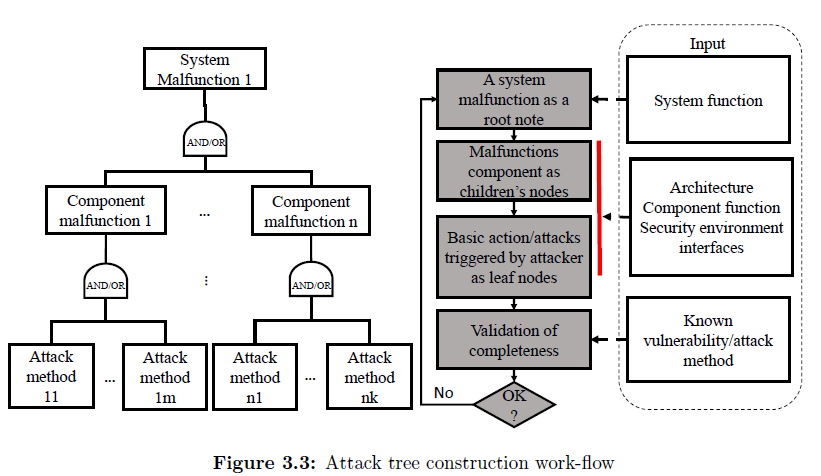


图3.3: 攻击树构造工作流程

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的期望功能中推断出来。每个故障被认为是三个安全属性(机密性，完整性，可用性)中的一个的丢失见表3.1。

例如，如果一架无人机按照预定的轨迹自动飞行，我们可以将“飞行并按照预定的轨迹飞行”视为系统功能。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)“偏离预定轨道——跟随攻击者定义的轨道”(完整性丧失)。

下一步，导致根故障的组件故障被推断出来，并表示为攻击树的子节点(例如，自动驾驶仪向电机提供了一个错误的命令)。为了推断组件的故障，我们使用组件函数列表

|  |  |  |  |
| --- | --- | --- | --- |
| 50 | 第三章系统网络安全风险管理 | |  |
| 表3.1: 由于安全属性丢失而导致的故障 | | |  |
|  |  |  |  |
| 安全属性 | 故障描述 |  |  |
| 可用性 | 出现故障，拒绝访问 |  |  |
| 功能 |  |  |
|  |  |  |
| 诚信 | 出现误用或不正确的故障 |  |  |
| 功能 |  |  |
|  |  |  |
| 保密 | 泄露的故障 |  |  |
| 资料/数据 |  |  |
|  |  |  |

和架构作为输入。

例如，我们将“无人机坠毁”故障视为一个根节点。这个系统故障与前面例子中提到的“按照预定轨迹飞行”系统功能有关。这个功能是基于不同组件的合作来实现的。它们是:

自动驾驶仪，可以估计飞行状态并提供发动机指令

GPS 提供位置数据

惯性导航系统(IMU) ，提供姿态数据。

我们使用三个 cybersecurity 属性关键字(Confidentiality、 Integrity、 Availability)来确定每个组件及以上组件可能出现的故障。它们可能是“ GPS 提供了错误的位置数据”、“ 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，我们重复这个过程，以确定组件的原因(被认为是子系统) ，直到达到最低级别的元素(其中的信息不可用于进一步的分析)。最后，攻击树以表达恶意行为或攻击方法的叶子节点结束，这些叶子节点可以被攻击者用来触发攻击。我们可以从 UAS 的环境信息中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表示。从叶子节点到根节点的每一条路径都表达了一个攻击者可以执行的攻击场景。每个攻击场景都是一个网络安全风险，我们需要在接下来的步骤中对其进行评估。因为建立攻击树的过程是演绎的，所以结果或多或少受到执行分析的人的能力的影响。因此，在最后，结果的完整性需要通过检查所有文档化的攻击方法是否已经在攻击树中被识别来验证。

注意: 在推理过程中，一些故障/漏洞被认为是非常难以发生的。如果它们和更高的故障/恶意行为之间的联系是合乎逻辑的，那么它们应该保留在攻击树上。例如，“使用 GPS 闪烁

|  |  |
| --- | --- |
| 3.2拟议方法 | 51 |

恶意软件通过其 USB 端口“很难发生，但可能发生，所以它需要显示在攻击树。

3.2.3风险分析及评估

这一步旨在确定哪些攻击场景需要考虑，哪些可以忽略。这一步骤的基本思想与安全分析中的基本思想相似，安全分析中的水平风险具有两个特征: 影响的可能性和拥有属性的严重性。然而，由于缺乏反馈，攻击的可能性很难确定。我们评估的不是可能性，而是攻击的难度(DOA)。DOA 表示攻击者完成一次成功攻击所需要的全部努力。应该首先处理易于实施但可能产生重大影响的攻击。难以执行的攻击可能影响较小，可能被忽略或处理的优先级较低。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 分别代表低、中和高风险水平)。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | 无 | L | M | M | H | H |  |
|  | 基础 | L | L | M | M | H |  |
| 到达时已死亡 | 适度 | L | L | L | M | M |  |
| 很高 | L | L | L | L | M |  |
|  | 非常高 | L | L | L | L | L |  |
|  |  | 没有影响 | 很低 | 中等 | 很高 | 非常高 |  |
|  |  | 攻击的严重性 | | |  |  |  |
|  |  | 表3.2: 风险水平 | | |  |  |  |

在这种方法中，攻击的难度和严重程度由不止一个人进行定性评估。攻击的严重性可以从上下文建立活动中收集的操作信息中推断出来。攻击的难度可以根据必要装备的性质(例如，便宜或昂贵，著名或不著名)、进行攻击所需的攻击技术和系统的知识来评估。

我们采用 ED202A/DO326标准中提出的指导方针——载人飞机的网络安全难度级别。在这个标准中，每个方案的难度是根据三个标准确定的:”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)。“ Execution Mean”表示执行攻击所需的资源、时间和知识(例如，破解加密算法所需的时间)。“机会之窗”代表与攻击时刻相关的难度(例如，如果可能的话，只有在系统重新启动时才发动攻击是困难的)。这些标准使用 ED202A/DO326标准中提供的刻度进行评估(见表3.3、表3.4和表3.5)。分配给这些标准的点的总和是该方案的总困难点。这个点与5个难度级别中的一个(无，基本，中等，高，和

52第三章系统网络安全风险管理

非常高) ，如表3.6所示。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | 知识 | | |  |  |  |  |  |
|  |  |  |  |  |  |  | 没有/公众 | | | |  | 不受控制 | | | | | 内部消息 | | |  |  |
|  |  |  |  |  |  |  | 资料及 | | | |  | 资料及 | | | | |  |  |
|  | 设备 | | |  |  |  |  | 或重要的 | | |  |  |
|  |  |  |  | 没有准备 | | | |  | 毫无意义 | | | | |  |  |
|  |  |  |  |  |  |  |  | 准备时间 | | |  |  |
|  |  |  |  |  |  |  | 时间 | |  |  |  | 准备时间 | | | | |  |  |
|  | 无/标准1 | | | | |  | 0 |  |  |  |  | 2 |  |  |  |  | 6 |  |  |  |  |
|  | Special COTS2特殊 COTS2 | | | | |  | 0 |  |  |  |  | 2 |  |  |  |  | 6 |  |  |  |  |
|  | 特别节目3 | |  |  |  |  | 不认识 | |  |  |  | 4 |  |  |  |  | 6 |  |  |  |  |
|  | 定制4 | |  |  |  |  | 不认识 | |  |  |  | 5 |  |  |  |  | 6 |  |  |  |  |
|  |  |  |  |  |  |  | 表3.3: 准备手段 | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 分数 |  | 描述 | | | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 0 |  | 攻击可以在任何时候进行 | | | | | | | | | | | | | |  |  |  |  |  |
|  | 1 |  | 攻击可以在定期巡航飞行中进行。 | | | | | | | | | | | | | | | | |  |  |
|  | 2 |  | 当飞机着陆时，攻击矢量是可用的。 | | | | | | | | | | | | | | | | |  |  |
|  | 3 |  | 强制性操作程序的最大效力 | | | | | | | | | | | | | | | | |  |  |
|  |  | 限制机会之窗。 | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | 6 |  | 攻击向量只能在有限的时间段内使用, | | | | | | | | | | | | | | | | |  |  |
|  |  | 例如地面维护模式 | | | | | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  | 攻击只能在非常有限的时间内进行 | | | | | | | | | | | | | | | | |  |  |
|  | 8 |  | 独立于飞行阶段的时间段(例如在系统 | | | | | | | | | | | | | | | | |  |  |
|  |  |  | 重启)。 | | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 表3.4: 机会之窗 | | | | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  | 专业知识 | | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 外行人 | | |  | 精通 | | 专家 | | | 多重专家 |  |  |
|  |  |  |  |  | 无/标准 | | | |  | 0 |  |  |  | 4 | |  | 6 |  | 10 |  |  |
|  | 设备 | | |  | 特殊胶床 | | | |  | 4 |  |  |  | 4 | |  | 6 |  | 10 |  |  |
|  |  |  |  |  | 很特别 | | | |  | 不认识 | |  |  | 6 | |  | 8 |  | 12 |  |  |
|  |  |  |  |  | 定制的 | | | |  | 不认识 | |  |  | 不认识 | |  | 10 |  | 12 |  |  |
|  |  |  |  |  |  |  | 表3.5: 执行意味着 | | | | | | | | | |  |  |  |  |  |
|  |  | | |  |  | | |  |  | | | | | |  | | |  |  |  |  |
|  | 从0到6 | | |  | 从7到12 | | |  | 从13岁到18岁 | | | | | | 从19岁到24岁 | | |  | 超过24个 |  |  |
|  | 无 | |  |  | 基础 | |  |  | 适度 | | | |  |  | 很高 | |  |  | 非常高 |  |  |

表3.6: 攻击难度等级

1没有装备或者其他常见的东西

可以很容易买到的东西，但通常还不是一般人所拥有的

不能轻易买到，但需要组装/建造的东西4需要一定资源才能组装的特殊设备

|  |  |
| --- | --- |
| 3.3. 个案研究 | 53 |

3.2.4治疗

对于上一步选择处理的每一种威胁情况，应该建立一套网络安全要求。网络安全要求并不是一项具体的安全措施，但它只是一个需要满足的安全目标，以确保系统的网络安全。对于每个网络安全需求，可以考虑一个或多个安全措施。他们需要经过测试/模拟和评估(成本，效率) ，然后才能被选中接入系统需求。

在这个方法中，我们采用了上面提到的安全需求分类

ED202A/DO326A [185]如下:

预防: 目的是阻止恶意用户导致故障

威慑: 目的是防止故障的发生

侦探: 目的是检测和报告攻击者的故障或恶意行为。

纠正: 目的是在故障发生时对其作出反应

修复性: 目的是使系统在发生故障后恢复到正常状态

3.3个案研究

在本节中，我们将介绍我们的方法论在一个案例研究中的应用: “基于无人机的公路观测”—— SOGILIS 公司的一个实际应用。在这个案例研究中，无人机被用来在自动飞行模式下观察高速公路。无人机捕捉到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，无人机将沿着高速公路飞行并沿着预先设定的轨道飞行。从飞行开始到结束，无人机在操作人员的超视距观察(BVLOS)下一直以自动模式飞行。操作员可以使用三个简单的命令: 开始飞行，结束飞行(回到待机模式) ，然后回家。这个无人机的架构如图3.4所示。为了简化案例研究，我们假设这个 UAS 是在没有任何网络安全关注的情况下开发的。这意味着在应用我们的方法之前，没有适当的措施来保护 UAS。

从系统运行的描述出发，我们定义了三个需要保护的系统功能:

功能1: 自动驾驶车辆跟随预定的交通工具

无人机必须按照制造商预先确定的飞行计划并嵌入自动驾驶仪。飞行计划包含几个方向点。每个路点包含坐标、海平面或地面高度的信息。

54第三章系统网络安全风险管理

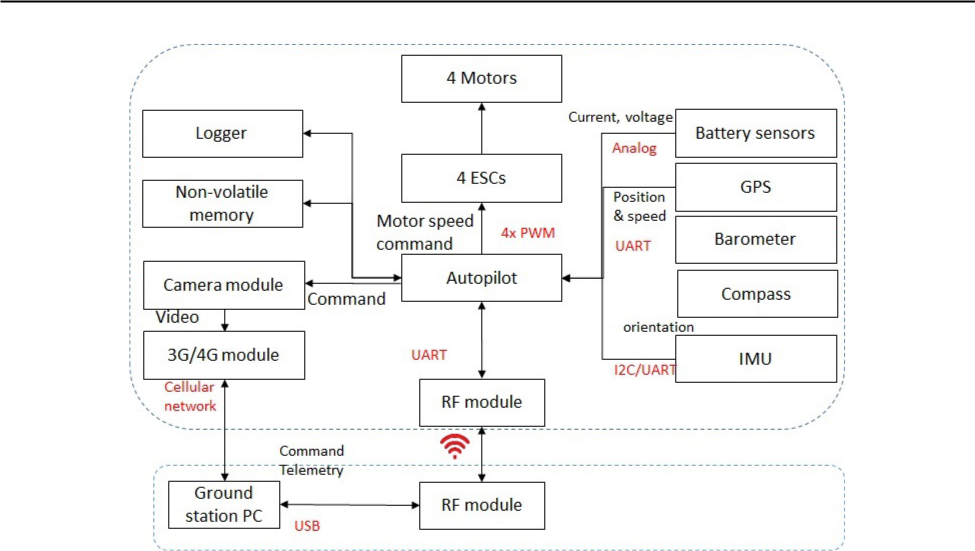


图3.4: UAS 的体系结构。

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、电池信息将被发送到地面并显示在 GCS 计算机的屏幕上。只有负责的操作员才有权访问这些信息。

功能3: 向操作人员提供观测视频: 将摄像机捕捉到的视频传送到地面，并在 GCS 计算机上显示。只有负责的操作员才有权访问这些信息。

基于上面的系统功能，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、保密性)的丢失有关。故障列表如下:

故障1-可用性-无人机坠毁: 由于恶意行为，无人机失去其姿态和坠毁。由于飞越高速公路，无人机的坠毁可能导致致命的事故。因此，我们认为这次故障的严重程度很高。

故障1——完整性——偏离预定轨道: 在攻击下，无人机偏离其轨道并按照攻击者定义的轨道飞行。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，攻击者可能会造成一起有意的致命事故。因此，我们认为这个故障的严重程度非常高。

故障1-保密-无关。

|  |  |
| --- | --- |
| 3.3. 个案研究 | 55 |

故障2——可用性——飞行信息不可用性: 在攻击下，飞行信息不再可用，操作员无法识别情况。这个故障可能会帮助攻击者发动其他的攻击，或者导致操作被取消。我们为这个故障设定了一个中等程度的严重性。

故障2-完整性-假飞行信息: 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，如触发故障安全功能。我们为此次故障设定了中等程度的严重性

机密性: 在攻击中，攻击者可以获得未经授权的飞行信息访问权，从而帮助攻击者发动其他攻击。我们为此次故障设定了中等程度的严重性

故障3-可用性-视频不可用性: 在攻击下，操作员无法访问观察视频。我们认为这次故障的严重程度较低。

故障3-完整性-假视频: 在攻击下，操作员接收到攻击者制作的假视频。这个故障并没有直接影响操作的安全。我们对这个故障的严重程度设置了一个较低的等级

机密性: 视频泄露: 在攻击下，攻击者可能获得未经授权的观察视频，从而影响被观察者的隐私。我们设置了一个高级别的严重性

对于每个系统故障，我们建立一个攻击树

一个开源软件来绘制具有相关要求的攻击树。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，我们只关注分析故障2——完整性“假飞行信息”。其他故障分析(包括攻击树、风险评估、需求)见附件 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-完整性 -1: 在这个场景中，敌人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，对手就可以制造假消息并将假消息发送到地面射频模块，用故障信息欺骗 GCS 和导频。因此，RF 模块应验证每个接收到的软件包在时间、有效载荷和来源方面的完整性(要求14-见附件 c. 2) ，以防御这种攻击。

场景2-完整性 -2: 这个场景类似于第一个场景，在这个场景中射频模块接收假消息。不同之处在于，对手不会创建假消息，而只是复制已发送的消息，并在事后对它们表示不满。这种攻击的结果是飞行员在时间方面被错误信息所欺骗。译注:

56第3章系统网络安全风险管理

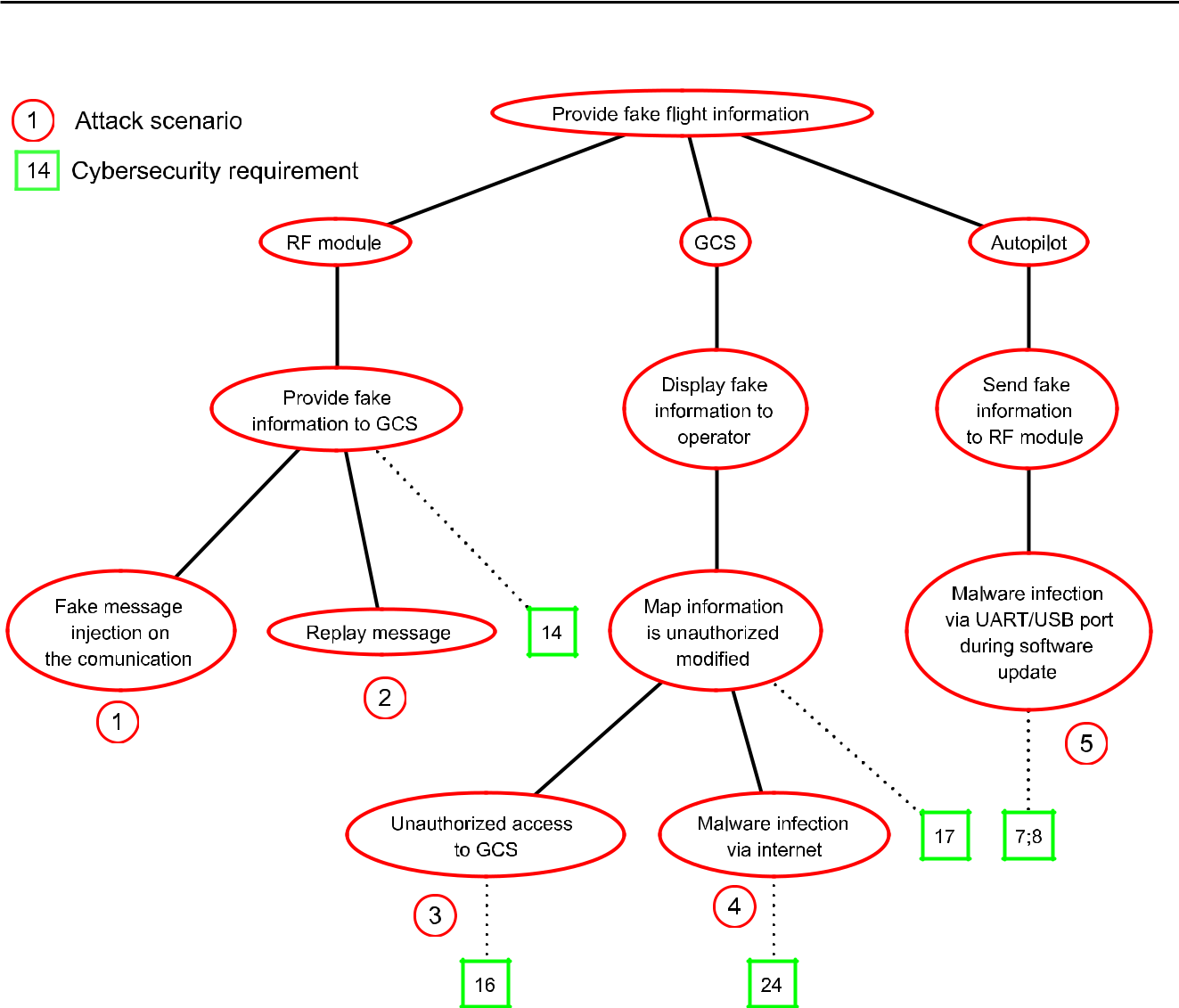


图3.5: 与故障相关的完整攻击树2- 完整性

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(如果有的话)。为了防御这种攻击，RF 模块应该根据转换时间/顺序来验证每个接收到的包的完整性(要求14)

见附件 c. 2)。

场景2-完整性 -3: 在这个场景中，敌人通过 GCS 攻击 UAS。如果对手能够到达地面控制站(GCS) ，他们就可以修改地面控制站存储的地图。有了故障地图，飞行员就会被关于飞行器位置的故障信息所欺骗。要成功进行攻击，攻击者不必具备高水平的技术知识，但必须有机会进入 GCS (例如心怀不满的员工)。这种攻击的适当对策可能是访问控制机制，它允许授权人员访问 GCS (要求16-见附件 c. 2)。

场景2-完整性 -4: 在这个场景中，GCS 计算机通过 Internet 感染了一个恶意软件，这个恶意软件可以修改存储的地图信息而不被检测到。译注:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 3.3. 个案研究 | | |  |  |  |  | 57 | |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 场景 |  | 到达时已死亡 |  |  | 严重程度 | 风险 |  |  |
|  | 准备工作 | 的窗户 | 处决 | 总计 | 水平 |  |  |
|  |  |  |  |  |
|  |  | 意思是 | 机会 | 意思是 |  |  |  |  |
|  |  |  |  |  |  |  |
|  | 2-integrity-1诚信-1 | 2 | 1 | 6 | 9 | 中等 | 中等 |  |  |
|  | (基本) |  |  |
|  | 2- 完整性 -2 | 2 | 1 | 6 | 9 | 中等 | 中等 |  |  |
|  | (基本) |  |  |
|  | 2- 完整性 -3 | 6 | 6 | 10 | 22 | 中等 | 很低 |  |  |
|  | (高) |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 2- 正直-4 | 6 | 6 | 10 | 22 | 中等 | 很低 |  |  |
|  | (高) |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 2- 正直-5 | 6 | 6 | 10 | 22 | 中等 | 很低 |  |  |
|  | (高) |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 表3.7: 与故障相关的攻击场景的风险评估2- 完整性 | | | | | | | |  |

如果攻击成功，攻击者必须对恶意软件和目标 GCS 有良好的技术知识。为了抵御这种情况，互联网和 GCS 之间的数据流需要被控制。只有制造商定义的数据才能从因特网到达 GCS 或通过 GCS 发送到因特网(要求24-见附件 c. 2)。

场景2-完整性 -5: 在这个场景中，自动驾驶仪应该在软件更新过程中被恶意软件感染。由于安装了恶意软件，自动驾驶仪在飞行过程中将假信息发送到 GCS (通过 RF 模块)。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。对于这种攻击，自动驾驶仪应该能够验证固件的完整性，以确保它是由制造商创建的(要求7-见附件 c. 2)。此外，访问控制机制可以到位，只允许制造商修改/更新固件(要求8-见附件 c. 2)。

上述攻击场景的风险级别如表3.7所示进行了评估。

3.3.1结果分析

基于攻击树，我们确定了49种可能的攻击方案，包括9种高风险方案、28种中等风险方案和12种低风险方案。这些方案涉及到 UAS 的不同组成部分。攻击场景在不同目标组件中的分布如图3.6所示。根据这张图表，攻击场景中最有针对性的组件是自动驾驶仪(11种场景)、地面控制站或 GCS (10种场景)、射频链路(7种场景)和3G/4G 链路(7种场景)。这个论点是合乎逻辑的，因为自动驾驶仪、 GCS 和通信链路涉及到无人机的所有功能。在这一点上，我们可能想知道这个场景是否与这些有关

第三章系统网络安全风险管理

与目标组件相关的攻击场景数

11



10



77



|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 3 | 3 |  | 3 |  | 3 |  |  |
|  |  |  |  |  |  | 1 |  | 1 |  |
|  |  |  |  |  |  |  |  |  |  |
| 3G/4G 模块 | 自动驾驶仪 | 晴雨表 | 指南针 | 格拉斯哥昏迷指数 | GPS | Gimbal 万向节 | IMU | 挥发性记忆 | 射频 |
|  |  |  |  |  |  |  |  | 没有 |  |



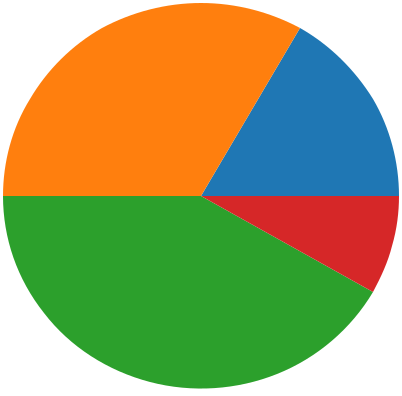
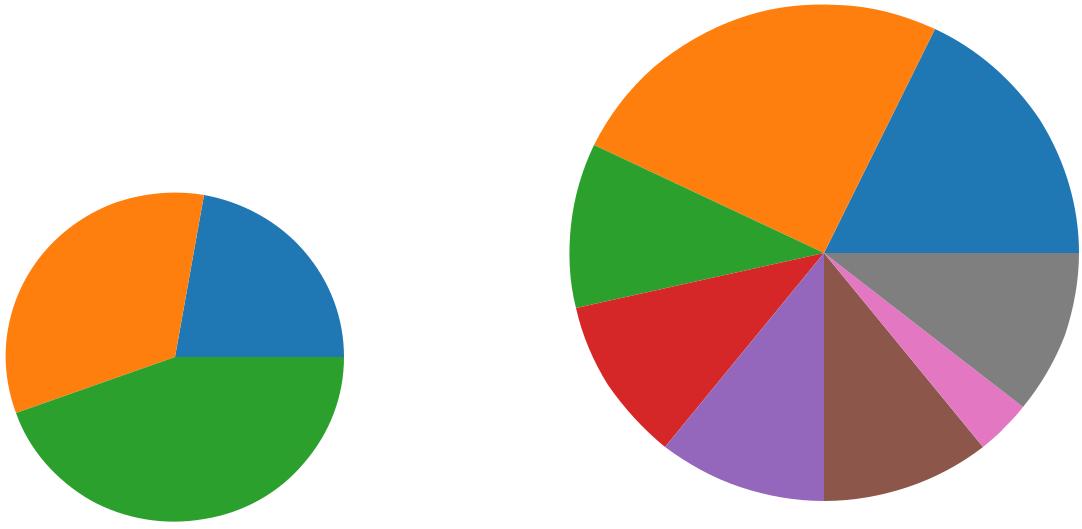
图3.6: 攻击场景分布到不同的目标组件

风险处理步骤中应考虑最多的组成部分。答案是“不确定”。特别是根据我们的方法论和整个风险管理的一般精神，在治疗步骤中，情景在治疗步骤中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情景在不同组件中的分布。

如图3.7所示，高风险情景仅涉及三个组件: GCS，GPS 模块和 RF 模块。射频模块和 GPS 模块都基于某些类型的无线通信。通过瞄准射频模块和 GPS 模块，攻击者可以远程发动攻击。同时，GCS 提供了一个完整的人机系统，可以轻松地控制车辆。这意味着当对手到达 GCS 时，他们可以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到无人机的基本功能: 保持飞行器在预定轨道上安全飞行。对于其他关键组件-自动驾驶仪，我们将相关的风险情景分配到中等风险水平或低风险水平。攻击者没有太多机会接近自动驾驶仪。此外，它需要复杂的工具和自动驾驶软件/硬件的知识来发动一次成功的攻击。此外

|  |  |
| --- | --- |
| 3.3. 个案研究 | 59 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 自动驾驶仪 | |  |  |  |  |
|  |  |  |  | 25.00% |  |  |  |  |
|  |  |  |  | (7) |  |  | 3G/4G 模块 |  |
|  |  |  |  |  |  | 17.86% |  |  |
|  |  |  |  |  |  | (5) |  |  |
| GPS | 格拉斯哥昏迷指数 | 晴雨表 | 10.71% |  |  |  |  |  |
|  | (3) |  |  |  |  |  |
| 33.33% | 22.22% |  |  |  |  | 10.71% | |  |
| (3) | (2) |  |  |  |  |  |
|  | 10.71% |  |  | (3) | 射频 |  |
|  |  |  |  |  |  |
|  |  |  | (3) |  | 3.57% | |  |
|  |  |  |  |  |  |
|  |  | 指南针 |  | 10.71% | 10.71% | (1) |  |  |
|  | 44.44% |  |  | (3) | (3) |  | 非挥发性记忆体 |  |
|  |  |  |  |  |  |  |
|  | (4) |  |  |  |  |  |  |  |
|  | 射频 |  | 格拉斯哥昏迷指数 | | IMU | |  |  |
|  |  |  |  |  |  |  |  |
| (a)高风险情况 | |  | (b)中度风险情况 | | | |  |  |
|  | 自动驾驶仪 | |  |  |  |  |  |  |
|  |  | 33.33% |  | 3G/4G 模块 | |  |  |  |
|  |  | (4) | 16.67% |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  | (2) |  |  |  |  |  |



8.33%

(1) Gimbal 万向节

41.67%

(5)

格拉斯哥昏迷指数

低风险情景

图3.7: 风险情景分布到不同的目标组成部分和风险水平

对于自动驾驶仪，我们还将涉及传感器(晴雨表、罗盘、 IMU)和有效载荷部件(Gimbal，3G/4G 模块)的风险场景分配到低或中等水平。我们认为基于传感器的攻击方案几乎是不可能的，因为这些攻击的有效范围有限，如第1.5节所述。同时，Gimbal 和3G/4G 模块只涉及非关键功能(获取和传输视频数据)。基于以上分析，我们应该首先处理与 GCS、 GPS 和 RF 模块(如 GPS 欺骗、数据泄露、去认证)相关的风险。然而，这个结论只适用于这个预期的操作和架构，这个架构是在“没有网络安全注意”的假设下开发的。

60第3章系统网络安全风险管理

3.4结论

本章介绍我们的风险管理方法，它解决了现有(或设计的)无人机系统的网络安全问题。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)风险治疗。在第一步-Context 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，我们确定可能的网络安全攻击场景。攻击场景是从第一步收集的系统信息(功能、组件、环境)中推断出来的。在这一步中，我们使用攻击树图来支持推理过程和可视化场景。在第三步-风险分析和评估，我们评估每个确定的攻击场景的风险水平基于其影响的严重程度和他们的困难水平。为了估计难度水平，我们采用 DO326标准中定义的规模。在最后一步-风险处理中，我们确定安全需求来防御攻击场景。这些需求是根据相关攻击风险级别的顺序来开发/实现的。为了说明这种方法，我们提出了一个简单的案例研究，其中使用 UAS 观察高速公路。在风险识别步骤中，我们共确定了49种不同的风险情景。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，我们分配了7种情景到高风险水平，28种情景到中等风险水平，12种情景到低风险水平。这一步骤在很大程度上取决于直觉判断，尽管这一步骤是根据航空标准 DO326A 中定义的分类等级执行的。这一步骤的稳健性可以通过结合不同专家的判断来提高。在最后一步，我们确定了24个需要考虑的网络安全需求。它们都是技术要求。其中一些需要对系统架构进行相当大的改变。架构的变化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到网络安全。这个论点是我们在第四章中提出的工作的基础

第四章

操作风险评估: 从安全到网络安全

目录

|  |  |  |  |
| --- | --- | --- | --- |
| 4.1 | 引言... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | | 62 |
| 4.2 | 关于 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 | | |
| 4.4 | 危害扩展: 隐私危害的 SORA。 | | 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 | 新的航帆确定... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 73 |
| 4.5 | 威胁扩展: 新的网络安全威胁 SORA。 | | 74 |
|  | 4.5.1 | 网络安全分类和风险模型扩展。 | 74 |
|  | 4.5.2 | OCSL 的判决..。 | 76 |
|  | 4.5.3 | OCSO 稳健性决定。 | 79 |
| 4.6 | 一个基于扩展 sora 网络的风险评估工具。 | | 79 |
|  | 4.6.1 | 描述和目的..。 | 79 |
|  | 4.6.2 | 设计与实施。 | 80 |
| 4.7 | 结论。 | | 81 |
|  |  |  |  |

61

62章第4章操作风险评估: 从安全到网络安全

4.1引言

在上一节中，我们介绍了一种加强现有无人机系统网络安全的方法。由于系统修改的成本，这种方法在解决网络安全问题上可能不具有成本效益。因此，我们的目标是在系统设计的开始阶段，尽快开发一种考虑网络安全方面的方法。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 是无人机领域一个著名的评估方法。该方法侧重于评估与操作安全相关的风险，但没有考虑到网络安全。本章剩下的部分组织如下。SORA 方法论的概念在第4.2节中有解释。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 方法论的两个扩展。第4.6节介绍了我们开发的基于网络的远程风险评估工具。我们在第4.7节结束了我们的工作。

4.2对 SORA 方法论的解释

特定操作风险评估(SORA)是由美国国家航空管理局-无人驾驶系统规则制定联合管理局(JARUS)的一组专家提出的一种以操作为中心的整体方法[187]。该方法是分析无人机操作的安全性，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，如训练、系统性能、操作员组织、系统开发。这种方法可能对不同类型的利益相关者有用。操作者(操作无人机的)和航空作者可以使用这种方法作为遵守欧盟规定的一种手段。制造商(设计和开发无人机)可以使用 SORA 方法来确定他们的设计需要达到特定类别下的目标操作的安全特性。本节解释了该方法的一般概念，包括两个部分: 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正在考虑的风险情景。这个模型在 SORA 方法学的第一版中详细介绍

但在第二版中没有明确提到[104]。然而，方法论仍然基于这个模型。因此，有必要了解模型来理解方法论的基本原理。这个模型的主要元素包括: (1)危害,

威胁、(3)危害和(4)障碍。

危险是领结图的中心点。它指的是在操作者的意图之外进行操作的情况(例如飞机飞到外面)

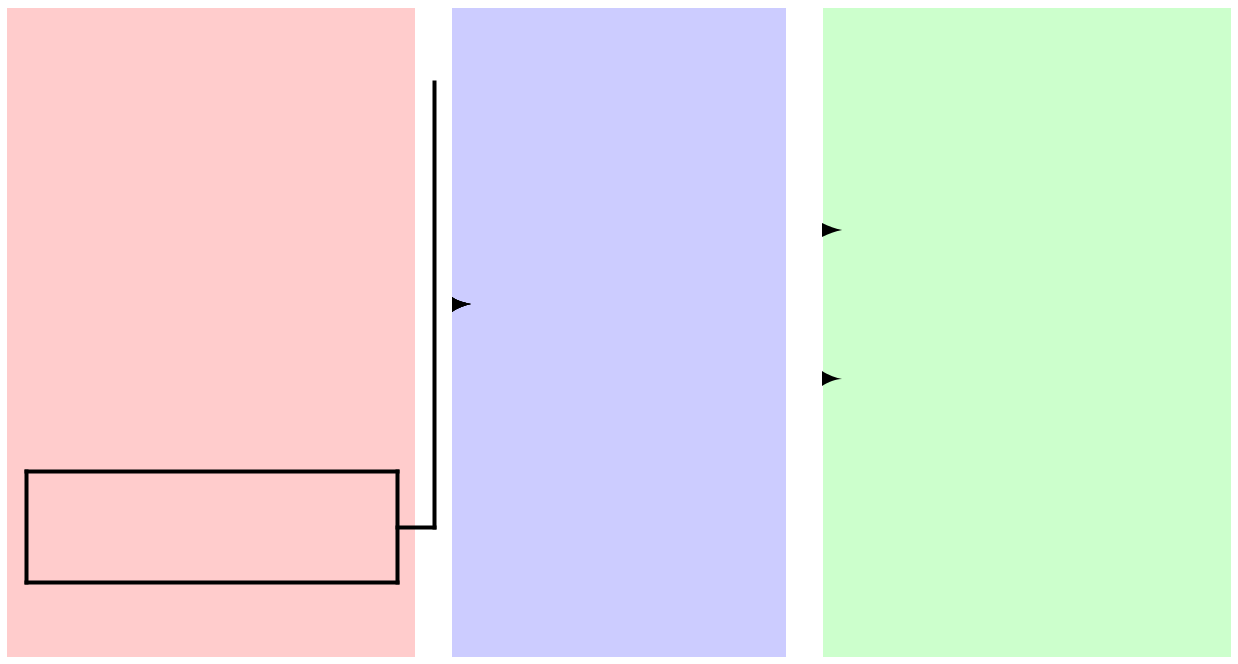
|  |  |
| --- | --- |
| 4.2. SORA 方法的解释 | 63 |

视线操作中飞行员的视觉观察)。

威胁位于“危险”的左侧，并被分为不同的类别。它们是危害的可能原因。因为 SORA 方法只考虑了安全方面，领结图只显示了一些无意识的威胁类别，如图4.1所示。

危害位于危害的右侧，代表危害的可能后果或情景的最终结果。目前，SORA 方法只考虑两种与个人生命有关的伤害:”对地面第三方的致命伤害”和”对空中第三方的致命伤害”(见图4.1)。为了减轻风险情景，几个障碍(或减轻手段)可以应用。

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的危害发生。威胁屏障防止危险发生。对于每一类威胁，不同的威胁屏障将在风险评估结束时以操作安全目标(OSO)的形式确定。每个 OSO 详细分为三个稳健级别(低，中，高)。一个例子是 OSO # 4-“ UAS 是为了授权公认的设计标准而开发的”。在这个 OSO 的低健壮性水平上，申请人只需声明所需的标准已经达到。同时，在高健壮性水平上，申请人必须提供支持性证据(如分析、仿真) ，这些证据将由有能力的第三方进行验证。该方法提供的 OSOs 列表见本文件附件 e。



|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 技术问题 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 人为错误 |  |  |  |  |  |  |  |  | 致命伤，第三名 |  |
|  |  |  |  |  |  |  |  | 地面人员伤亡 |  |
|  |  |  |  |  | 无人机操作 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |
|  |  |  |  |  | 失控 |  |  |  |  |  |
| 不良操作 | 致命伤，第三名 |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |
| 条件 |  |  |  |  |  |  |  |  | 空中派对 |  |
|  |  |  |  |  |  |  |  |  |  |  |

外部环境恶化

支持无人机系统

威胁，危险，危害

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，我们以定量和定性的方法解释了基于上述风险模型的 SORA 方法的评估过程。

64章操作风险评估: 从安全到网络安全

4.2.2评估过程

4.2.2.1量化方法

传统上，风险被定义为可能性和严重程度的组合。然而，SORA 方法中的风险仅限于可能性参数[103] ，因为该方法基本上只侧重于危害个人生命的风险。这些危害的严重程度可以被认为是极高的。换句话说，安全目标的确定是为了将每次伤害的可能性维持在可接受的值以下(每飞行小时106次致命伤害，相当于一次载人飞机操作[103])。如图4.2所示，这些危害的可能性被分解为单个组件。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 可能性 |  | 人的可能性 |  |  |  |
| 致命可能性 | = | 拥有无人机 | x | 被 UA 打击如果 UA | x | 很可能，如果 |  |
| 第三名受伤 | 行动结束 | 手术结束了 | 被击中，有人死亡 |  |
| 地面人员伤亡 |  | 控制 |  | 控制 |  |  |  |
|  |  | (1) |  | (2) |  | (3) |  |
|  |  |  |  |  |  |  |  |
|  |  | 可能性 |  | 其他可能性 |  | 很可能，如果 |  |
| 致命可能性 | = | 拥有无人机 | x | 飞机被 | x | 另一个被击中 |  |
| 第三名受伤 |  | 行动结束 |  | 如果操作是 |  | 飞机不可以 |  |
| 空中派对 |  | 控制 |  | 失控 |  | 继续安全飞行 |  |
|  |  | (1) |  | (2) |  | (3) |  |

图4.2: 根据 SORA [103] ，地面和空中致命伤害的可能性

每个方程的组成部分(1)“无人机操作失控的可能性”主要受威胁和威胁障碍的影响[103]。每个方程中的组成部分(2)和组成部分(3)的组合表示在无人机操作失控的情况下发生危害的可能性，这可以通过分析所考虑的操作性质(例如位置、高度、操作种类、设置危害屏障)来评估。在上述假设下，这种定量方法的一般概念可以解释如下:

目的: 给定一个无人机操作，我们需要保持每个危害的可能性

低于可接受的值: 每飞行小时106人致命伤。

首先，我们收集了无人机的作战区域、作战方式、飞行员、 UA 重量等有关无人机预期作战的信息。这个活动被称为操作概念(CONOPS)描述。CONCOPS 描述的形式在 SORA 方法的附件 a 中提供。

其次，我们根据收集到的资料，估计「无人机操作失控」情况下发生危害的可能性(例如每个危害104人在地面受伤，每个危害103人在空气中受伤)。

第三，根据上述估计值，计算出无人机操作失控可能性的可接受值(第一个方程为每飞行小时102个危险，第二个方程为每飞行小时103个危险)。更关键的

|  |  |
| --- | --- |
| 4.2. SORA 方法的解释 | 65 |

价值将被选择作为一个目标需要达到(例如103危险每飞行小时)。

最后，基于“无人机操作失控的可能性”的客观值，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 方法学提出了一种基于定量方法的主要思想的定性方法，如图4.3所示。定性方法可以解释如下:



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | CONOPS | |  |
|  |  |  | 描述 | |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  | GRC 测定 | |  |
|  |  |  |  |  |  |
|  |  |  | 地面风险 | |  |
|  | 是的 | | > 7？ | |  |
|  |  |  |  | 不 |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  | ARC 决心 | |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  | SAIL Level 帆船级别 | |  |
|  |  |  | 决心 | |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  | OSO 鲁棒性 | |  |
|  |  |  | 决心 | |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| 行动 | |  | 输入 | |  |
| 修改 | |  | 系统设计 | |  |
|  |  |  |  |  |  |

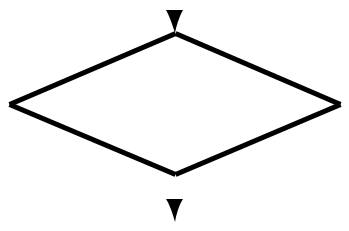


图4.3: 简化的风险评估过程

目的: 考虑到无人机操作，我们需要将每种伤害的可能性维持在可接受的水平。

首先，我们收集有关预期操作的信息(CONOPS 描述)

第四章操作风险评估: 从安全到网络安全

其次，确定了两个定性因素: 地面风险等级(GRC)和空中风险等级(ARC)。这些因素定性地表示在无人机操作失控的情况下发生危害的可能性。根据作战区域、姿态、飞机重量以及危害屏障的可用性等作战特性，确定了 GRC 和 ARC。

第三，我们确定了两个具体的保证和诚信水平(SAIL)值，这代表了无人机操作将处于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 值范围从 i 到 VI。然后，更高的 SAIL 值将被选择为与 UAS 操作相对应的置信水平或 SAIL。这个值被认为是驱动所需安全目标的一个目标。在 SORA 方法的最新版本中，通过使用表4.1简化了这些活动。

帆的确定

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | ARC |  |  |  |
| GRC | A (\* \*) |  | b | c |  | d |
| 2(\*) | I |  | 二 | 四 |  | V |
| 3 | 二 |  | 二 | 四 |  | V |
| 4 | 三 |  | 三 | 四 |  | V |
| 5 | 四 |  | 四 | 四 |  | V |
| 6 | V |  | V | V |  | V |

VI VI VI VI

表4.1: SAIL 确定 SORA 方法[104]

表4.1的解释: 第一个值线(\*)包含与 ARC 值对应的 SAIL 值。它们也可以理解为 GRC 可以忽略不计的操作的 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 可以忽略不计的操作的 SAIL 值。其他 SAIL 值是对应于 GRC 的 SAIL 值的最大值和对应于 ARC 的最大值。

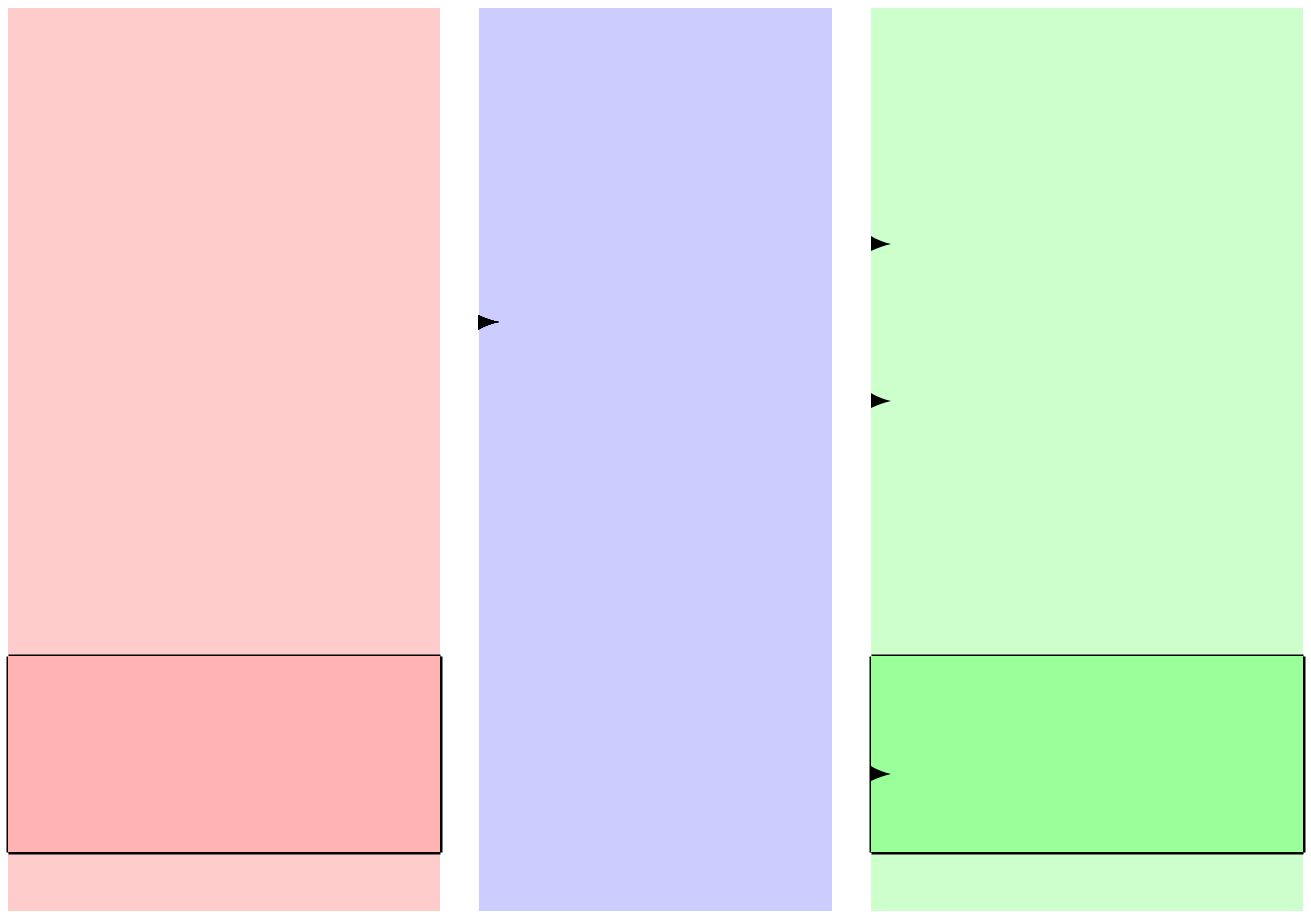
最后，我们选择了 Operation Safety Objective (OSO)及其对应于操作的 SAIL 水平的鲁棒性水平。SORA 附件 e 提供了所有可能的 OSOs 列表[98]。

在本节中，我们解释了 SORA 方法的原始概念。首先根据“无人机操作失控”情况下的危害可能性来评估无人机操作的临界水平，然后确定与操作临界水平相对应的威胁屏障。在下一部分，我们提出了一个解决方案，以扩展这种方法，涵盖网络安全方面的基础上这一概念。

|  |  |
| --- | --- |
| 4.3将 SORA 方法扩展到网络安全的解决方案 | 67 |

4.3将 SORA 方法扩展至网络安全的解决方案

我们提出的解决方案由两部分组成，分别称为危害扩展和威胁扩展。Harm Extension 用新的 Harm 扩展了正在考虑的风险场景; 并完成了给定 UAS 操作的临界水平的评估。Threat Extension 扩展了新的网络安全威胁所考虑的场景; 并确定了给定无人机操作的相应威胁屏障。



|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 技术问题 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 人为错误 |  |  |  |  |  |  |  | 致命伤，第三名 |  |
|  |  |  |  |  |  |  | 地面人员伤亡 |  |
|  |  |  |  | 无人机操作 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |
|  |  |  |  | 失控 |  |  |  |  |  |
| 不良操作 | 致命伤，第三名 |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 条件 |  |  |  |  |  |  |  | 空中派对 |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 外部环境恶化 |  |  |  |  |  |  |  |  |  |
| 支持无人机系统 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 威胁扩展 |  |  |  |  |  |  |  | Harm extension 危害扩展 |  |
|  |  |  |  |  |  |  |  |  |  |
| 网络安全 |  |  |  |  |  |  |  | 基础设施受损 |  |
| 威胁 |  |  |  |  |  |  |  | 和侵犯隐私 |  |
|  |  |  |  |  |  |  |  |  |  |
| 威胁 |  |  |  | 危险 | | | | 伤害 |  |
|  | 图4.4: 扩展风险模型 | | | | | | |  |  |

在 Harm Extension 中，我们关注风险模型的危害方(参见图4.4)。最初的 SORA 方法论只涉及对人的生命的危害。然而，除了对人的生命的危害之外，公众还关注其他危害[103] ，[189]-[191] ，例如:

侵犯隐私: 一个 UAS 可以有一个小型的，长的操作范围和高性能的板载传感器，所以它可以侵入自己的私人位置和收集信息[192]。这侵犯了所有者的隐私。侵犯隐私可能是由网络攻击或系统错误引起的。例如，警方运营的 UASs 系统可能经常在前往运营区域的途中穿越私人财产。下图

68第4章操作风险评估: 从安全到网络安全

一旦发生网络攻击，房产上的录像可能会被泄露，然后飞出来的业主的隐私可能会被侵犯。

对基础设施的实际损害: 据推测，由于网络攻击或事故，无人机可能会坠毁在关键的基础设施上，如高速公路、电力线路、核电站。这种伤害只涉及到 UAs 飞行在关键基础设施附近或上空的一些特定操作。

对基础设施的数字损害: 人们认为无人机系统可能成为对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来攻击基础设施。

因此，这些新的危害成为扩展方法中应当考虑的重要问题。在危害扩展中，我们解决新危害的策略包括以下四个步骤:

选择一个需要解决的新危害

确定影响所选危害可能性的无人机操作的因素/特点。

建立公式或表格，根据确定的因素定性评估可能性

扩大“ SAIL 确定”步骤，以涵盖新的危害的可能性。

在 Threat Extension 中，我们将关注风险模型的威胁方面。潜在的网络安全威胁需要被识别出来，并被归类为新的威胁类别。换句话说，这需要对与 UAS 操作相关的网络安全威胁进行分类。为了说明新的场景，新的威胁类别将被添加到风险模型的威胁端，如图4.4所示。对应于每个新的威胁类别，一个可能的威胁屏障列表也将被建立起来。给定的无人机操作的详细威胁屏障将根据 SAIL 因子的值从建议的清单中选择。我们发展这一扩展的战略可以描述如下:

在文献综述的基础上，创建网络安全威胁的分类。网络安全威胁将被添加到 SORA 风险模型的威胁一侧。

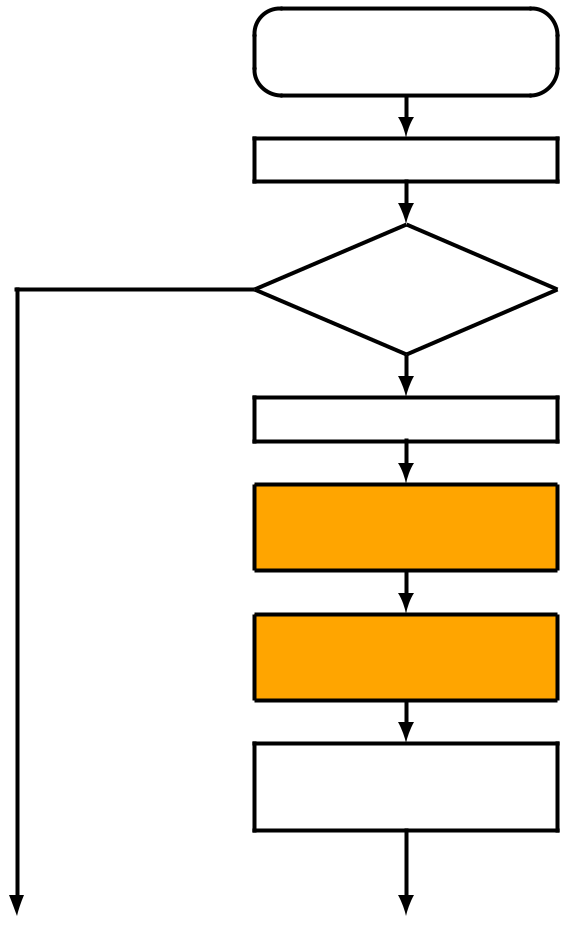
建立一个通用的威胁屏障的清单，为每个威胁类别在定义的分类-omy。根据 SORA 方法，每个障碍将被定义为三个级别的健壮性(低，中和高)。这项工作也是基于最先进的网络安全对策在“封闭”领域，如智能车辆，机器人..。

确定为给定的无人机操作选择网络安全威胁屏障稳健性的机制。

|  |  |
| --- | --- |
| 4.4. Harm 扩展: SORA 与隐私 Harm | 69 |

危害扩展和威胁扩展可以分开开发，然后可以整合成一个完整的方法。与隐私相关的危害扩展的细节在第4.4节给出，威胁扩展在第4.5节给出。

4.4危害扩展: SORA 与隐私危害



CONOPS

描述

GRC 测定

地面风险

是的 > 7？

不

ARC 决心

中国

决心

SAIL Level 帆船级别

决心

OSO 鲁棒性

决心

|  |  |  |
| --- | --- | --- |
| 行动 |  | 输入 |
| 修改 |  | 系统设计 |
|  |  |  |

图4.5: Harm Extension 的新步骤

如今，侵犯隐私是公众接受无人机应用程序最关心的问题之一[103] ，[191] ，[193]。因此，我们认为这是一个重要的问题，并首先在我们的工作中解决它。然而，一般隐私是一个非常大的术语。很难精确地定义[194]和广泛地处理这个术语，所以我们只关注这种伤害的三个方面: (1)披露个人信息; (2)非法的个人监视; (3)侵入私人场所。第一个方面在 Li 等人的工作中得到了说明[195]。作者根据无人机捕获的视频实验了密码窃取攻击。第二个方面在[196]-[198]中提到。在这些论文中，作者研究了监视无人机应用程序如何影响地面人员的隐私。此外，Park 等[197]和 Babiceanu 等[199]提出了基于捕获的图像/视频质量判断无人机操作侵犯隐私的标准。最后一个方面得到了解决

第四章操作风险评估: 从安全到网络安全

布兰克等[200]。作者提出了一种在创建飞行路径时识别私人空间的机制，并确保 UAs 不会飞越这些私人属性。

接下来，我们首先分析侵犯隐私的可能性，以确定与此危害相关的可能因素，这些因素可用于评估(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“隐私风险类别(PRC)确定”的新步骤，以评估在“无人机操作失控”的情况下这种危害的可能性; (4.4.3)一个“ SAIL 确定”步骤的扩展(见图4.5)。

4.4.1侵犯隐私的可能性

在考虑到隐私伤害的情况下，风险评估的目标扩大到保持隐私受到伤害的可能性也在一定的可接受水平之下。类似于危害个人生活的可能性，隐私危害之一可以被分解，如图4.6所示。该方程的两个组成部分(2)和(3)的组合表示“无人机操作失控”后第三方隐私权受到侵犯的可能性。

对于一个给定的行动，一个人暴露于不稳定环境的可能性(在感应范围内或在不稳定环境下)取决于行动区域的性质(城市区域对农村区域)和行动类型(视线以外与视线以外)。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，在城市地区有一个人或一个私人地点暴露在普通话中的可能性比在农村地区要高。在超视距视线(BVLOS)作业中，无人驾驶飞机的作业范围大于视线视线(VLOS)作业。因此，在 BVLOS 操作中，在 UA 下或接近 UA 的人数可能比在 VLOS 操作中更多。这就是为什么 BVLOS 操作中暴露于 UA 的人或私人位置的可能性高于 VLOS 操作。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 可能性 |  | 人的可能性 |  |  |  |
| 可能性 | = | 拥有无人机 | x | 暴露于 UA，如果 | x | 很可能，如果 |  |
| 行动结束 | 行动已经结束 | 暴露的，隐私的 |  |
| 侵犯隐私 |  |
|  | 控制 |  | 控制 |  | 人受到侵犯 |  |
|  |  |  |  |  |
|  |  | (1) |  | (2) |  | (3) |  |

图4.6: 侵犯隐私的可能性

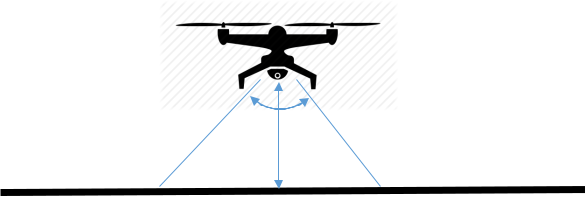
对于接触 UA 的人来说，侵犯隐私的可能性取决于机载摄像机捕捉到的图像的细节程度。例如，如果由无人机拍摄的照片分辨率太低，人的图像不够详细，无法识别她/他的脸，因此侵犯隐私的可能性很小。图像的细节级别可以通过像素密度来评估——在一张捕捉到的图像中，像素的数量代表地面上的一米。为了简化计算，我们假设地面是平的。因此，对于一个 UAS 操作，当摄像机的方向达到像素密度的最高值时

2小时晒黑

|  |  |
| --- | --- |
| 4.4. Harm 扩展: SORA 与隐私 Harm | 71 |

垂直于地面，如图4.7所示。在这种情况下，像素密度是 UA (h)地面高度、相机分辨率和相机最小视角()的函数，如下所示:

P d = 水平像素数(像素 = m)



H (m) : 无人机的高度

α: 摄像机的视角

h

图4.7: 最大像素密度位置

由于无人机应用程序与闭路电视应用程序在隐私问题上的共同点[191] ，[197] ，[198] ，我们采用了英国安全行业协会(BSIA)为闭路电视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 |  |
|  | 能够查看方向和速度 |  |
| 显示器(12.5像素/米) | 人的移动，如果知道他们的 |  |
|  | 存在感。 |  |
| 侦测(25像素/米) | 能够确定一个人是否在场 |  |
| 观察(62.5像素/米) | 对象的某些细节进行描述 |  |
| 个人 |  |
|  |  |
|  | 启用以确定是否存在 |  |
| 识别(125像素/米) | 显示的个人与某人相同 |  |
|  | 他们以前见过的 |  |
| 身份证(250像素/米) | 确认个人身份 |  |
| 排除合理怀疑。 |  |
|  |  |
| Inspect (1000 pixel/m)检查(1000像素/米) | 启用个人的身份 |  |

表4.2: 图像细节分类[201]

在此基础上，我们定义了无人机操作的三个内在特征，以评估在“无人机操作失控”的情况下侵犯隐私的可能性:

运行区域密度: 城市区域与农村区域

操作类型: BVLOS 与 VLOS

获取图像的细节级别。

72第4章操作风险评估: 从安全到网络安全

类似于原始方法中引入的危害，隐私危害的可能性可以通过应用一些危害屏障来降低。在这个扩展中，我们讨论了三种类型的伤害障碍，以减轻隐私伤害:

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、掩码化、扭曲[198]

对私人空间的限制: 操作员避免在私人空间中制造飞行路径[200]

关注无人机操作的公告: 观察无人机操作的公众应被告知此事。

在文件的下一部分，我们提供了中国确定步骤和 SAIL 确定步骤的细节。

4.4.2确定私隐风险类别的步骤

在此步骤中，“ UAS 操作失控”情况下侵犯隐私的可能性由 Privacy Risk Class (PRC)值定性地表示。我们根据操作的内在特征和应用的危害壁垒来确定操作的 PRC。正在考虑的内在特征包括操作区域(农村与城市)、操作类型(VLOS 与 BVLOS)和图像细节级别，如4.4.1所述。这些特征的组合表达了操作的内在 PRC，如表4.3所示。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| 类别 | 乡下 | 乡下 | 都市 | 都市 |  |
| 地带, | 地带, | 地带, | 地带, |  |
| 行动 |  |
| VLOS | BVLOS | VLOS | BVLOS |  |
|  |  |
| 图像细节 |  |  |  |  |  |
| 水平 |  |  |  |  |  |
| 监视器 | A | B | C | C |  |
| 侦测 | B | B | C | C |  |
| 观察 | B | C | D | D |  |
| 识别 | C | C | D | D |  |
| 识别 | C | D | E | E |  |
| 视察 | C | D | E | F |  |

表4.3: 内在 PRC 确定

“隐私保护过滤器”、“对私人空间的限制”和“向公众发布操作意识公告”等危害壁垒可以降低确定的内在中华人民共和国。每个危害屏障用表4.4所示的减少系数校正内在的 PRC。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 4.4. Harm 扩展: SORA 与隐私 Harm | | | 73 | |  |
|  |  |  |  |  |  |
|  | Harm Barrier 伤害屏障 | 中华人民共和国修正系数 | |  |  |
|  | 不适用 | 应用 |  |  |
|  |  |  |  |
|  | 隐私保护过滤器 | 0 | - 1 |  |  |
|  | 限制私人空间 | 0 | - 1 |  |  |
|  | 行动须知公告 | 0 | - 1 |  |  |

表4.4: 中华人民共和国危害壁垒修正系数

例如，一架无人驾驶飞机配备了1920x1080分辨率和10度视角()的照相机; 以 BVLOS 模式飞行，距离地面150米。在这个操作中，最大像素密度为36像素/米，它对应于 Detect 级别(见表4.2)。根据表4.3，内在的 PRC 在 c 级。在分析了隐私问题之后，操作员决定升级机载摄像头的数字滤波器，使人的图像模糊，无法识别。在这种情况下，PRC 从 c 级降低到 b 级(见表4.4)。

4.4.3新的 SAIL 确定

在这个扩展中，无人机操作的 SAIL 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，我们将新值称为3d-SAIL 和旧的 SAIL 值2d-SAIL。我们以类似于确定2D-SAIL 的方式确定3D-SAIL。首先，我们选择对应于给定操作的 GRC，ARC 和 PRC 值的三个 SAIL 值。目前，我们提出表4.5来确定对应于 GRC 值的 SAIL。相应的 SAIL 值与 PRC 值成正比。然后，给定操作的3D-SAIL 值是三个确定的 SAIL 值的最高值。3D-SAIL 的确定步骤描述如下:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 中国 | A | B | C | D | E | F |
| 对应的风帆 | I | 二 | 三 | 四 | V | 六 |

表4.5: 与 PRC 值对应的 SAIL 值

对于给定的操作，确定与 ARC 和 GRC 对应的 SAIL 值的最高值。这个值是2D-SAIL。我们可以使用原始 SORA 方法学提供的表格(见4.1)。

确定对应于 PRC 值的 SAIL 值(见表4.5)。

在2d-SAIL 值和对应于 PRC 的 SAIL 值之间选择较高的 SAIL 值(更关键)作为3d-SAIL 值或对应于操作的最终 SAIL 值(见表4.6)。

74章操作风险评估: 从安全到网络安全

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | 2D-SAIL | |  |  |
| 中国 | I | 二 | 三 | 四 | V | 六 |
| A | I | 二 | 三 | 四 | V | 六 |
| B | 二 | 二 | 三 | 四 | V | 六 |
| C | 三 | 三 | 三 | 四 | V | 六 |
| D | 四 | 四 | 四 | 四 | V | 六 |
| E | V | V | V | V | V | 六 |
| F | 六 | 六 | 六 | 六 | 六 | 六 |

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，没有考虑 PRC (隐私伤害)。同时3D-SAIL 考虑到了隐私伤害。但是两者都代表了需要实现的“无人机操作将在控制之下”的信心水平。因此，在3D-SAIL 和2D-SAIL 相同的值下，基于2D-SAIL 和3D-SAIL 确定的 OSO 鲁棒性水平是相似的。

例如，一个 UAS 操作被分配到 GRC 的6级、 ARC 的 b 级和 PRC 的 b 级。基于 ARC 因子和 GRC 因子，我们获得了2D-SAIL 因子的 v 值(见表4.1-来自原始方法)。然后，基于 PRC 因子和2D-SAIL 因子，我们得到了3D-SAIL: level v 的相同值(参见表4.6-来自扩展方法)。在这种情况下，扩展方法(3D-SAIL)确定的 OSO 的健壮性水平与原始方法(2D-SAIL)确定的健壮性水平相似。这就是为什么在 Harm 扩展中，我们保持“ OSO 鲁棒性确定”步骤不变的原因。然而，我们认为最初的 OSOs 列表不足以在网络安全方面保护无人机操作。因为最初的 OSOs 只针对无意的威胁(比如开发错误，飞行员的不正确行为)。同时，有意识的威胁被忽略(如网络攻击) ，这可能会损害隐私和个人的生活。这个差距被第4.5节中提出的威胁扩展所弥补

4.5威胁扩展: SORA 与新的网络安全威胁

在前面的讲座中，我们用新型的 Harm 扩展了 SORA 方法学的“蝴蝶结”风险模型的左侧。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

基于1.5节中的文献回顾，我们提出了一个由三个类别组成的网络安全威胁分类法(见表4.7)。第一个是“攻击”

|  |  |
| --- | --- |
| 4.5. 威胁扩展: 新的网络安全威胁 | 75 |

“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。第二个是“攻击通信”类别，涵盖了所有可能针对通信部分网络安全漏洞的威胁。第三个是“攻击传感器”类别。这个类别是典型的所有网络物理系统，如无人机，其中传感器提供系统的能力，以感知物理环境。尽管如此，传感器还是允许攻击者用虚假数据欺骗系统。因为我们的分类是建立在文献综述的基础上的，所提出的分类只能涵盖已经在现实生活或模拟中得到证实的网络安全威胁。这个分类法在未来可以扩展到未被发现的威胁。

|  |  |  |
| --- | --- | --- |
| 描述 | 类别 |  |
| 未经授权的修改路线点载入 |  |  |
| 自动驾驶仪[61] |  |  |
| 病毒在 GCS 上[2] | 攻击软件 |  |
| 未授权修改源代码[152] |  |  |
| 未经授权访问该软件[152] |  |  |
| 视频重放攻击[3] |  |  |
| 对通信的去认证攻击[4] | 攻击通讯 |  |
| 控制无人机 |  |
|  |  |
| 干扰通讯[57] |  |  |
| 视频资料披露[202] |  |  |
| GPS 干扰-欺骗[49] ，[50] |  |  |
| 摄像头欺骗[203] | 攻击传感器 |  |
| IMU 欺骗[51]-[53] |  |  |

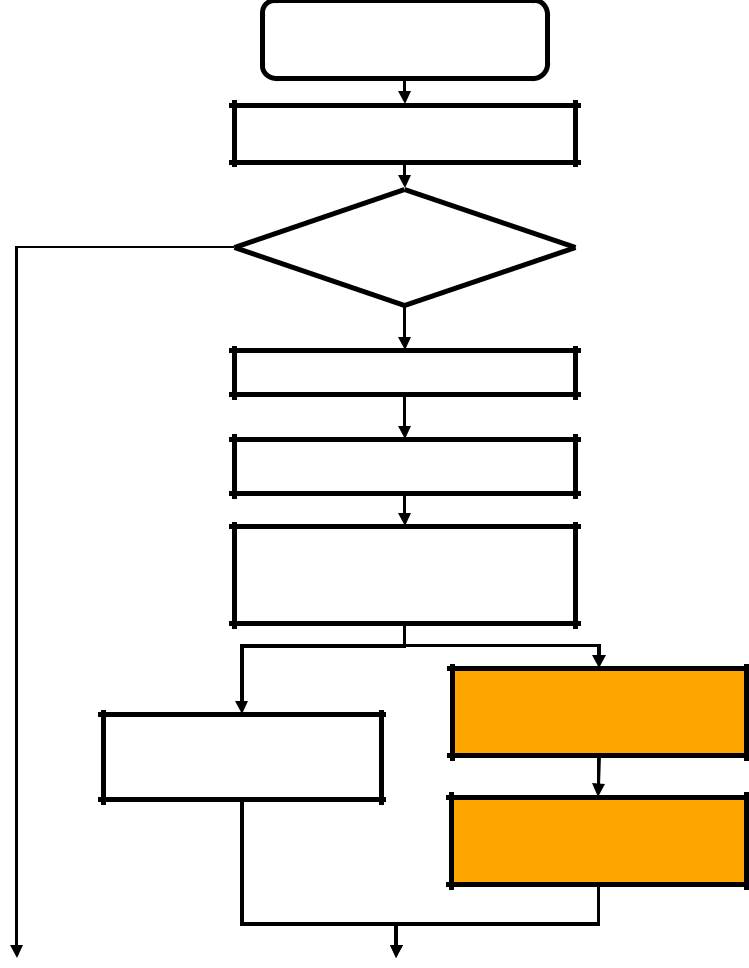
表4.7: 网络安全威胁的类别

通过提出的分类法，我们扩展了 SORA 风险模型的威胁一侧，并将其分为网络安全威胁类别，如图3.8所示。类似于经典 SORA 方法论的想法，由网络安全威胁引起的“失控行动”危险可以通过威胁壁垒来预防或减轻。我们称这些障碍为网络安全行动目标(OCSO) ，相当于原始方法论中的安全行动目标(OSO)。根据 MEHARI 方法的指导方针和 IEC62443的基本安全服务清单，我们提出了三个新的网络安全类别的 OCSOs 清单(见附录 a)。该列表由13个 OCSOs 组成。从1到7的 OCSOs 提供了保护软件的目标(包括存储数据，源代码，访问授权)。从8号到12号的 OCSOs 提供了在通信渠道内保护数据的可用性、完整性和机密性的目标。最后一个 OCSO-number 13是指与传感器提供的数据相关的保护。与原始方法学的 OSOs 类似，每个 OCSO 都详细定义了三个健壮性水平(低，中和高)。对于每个操作，OCSO 的鲁棒性水平是根据(1)无人机操作将处于控制(或 SAIL)所需的置信水平和(2)操作对网络安全攻击的易感性来确定的。例如，高鲁棒性 OCSOs 需要一个操作必须始终保持

76章操作风险评估: 从安全到网络安全

在控制之下(高 SAIL)并且非常容易受到网络安全攻击。我们通过一个新的因素来描述操作敏感性: Operation Cybersecurity Susceptibility Level (OCSL)。

CONOPS



描述

GRC 测定

是的，地面

风险 > 7？

没有

ARC 决心

中华人民共和国决定

SAIL Level 帆船级别

决心

OCSL

OSO 鲁棒性的确定

决心

OCSO 的鲁棒性

决心

|  |  |  |
| --- | --- | --- |
| 行动 |  | 输入 |
| 修改 |  | 系统设计 |

图4.8: Harm 扩展的新步骤

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的步骤: OCSL 确定和 OCSO 稳健性确定(见图4.8)。接下来，我们详细讨论这些步骤。

4.5.2 OCSL 的测定

给定的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本质。隔离的通信渠道越多，攻击者到达 UAS 的可能性就越小(为了发现、利用漏洞)。因此，这种操作不太容易受到网络攻击。例如，使用私人/专用/军事通信解决方案的操作比使用 in-internet 的通信解决方案更难实现。然而，在这一点上，我们应该清楚的是，我们不把“隔离”作为一个

|  |  |
| --- | --- |
| 4.5. 威胁扩展: 新的网络安全威胁 | 77 |

针对网络安全攻击的保护解决方案，但只是 UAS 操作的一个特征。考虑中的第二种操作的特点是操作类型(VLOS vs. BVLOS)。在 BVLOS 操作中，飞行器从相当远的距离操作，超出飞行员的视觉观察范围。因此，攻击者可能有更多的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，由于网络安全攻击导致的车辆异常行为可以被视觉检测到。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征是飞行员在操作过程中的监控。攻击者对在飞行员持续监视下飞行的无人机发起成功攻击的机会比没有持续监视的无人机要少。最后一次行动的特点与第三方服务/设备有关。为了实现操作，无人机操作员可以使用第三方提供的服务(如维护、导航、导航等)或辅助设备(摄像机、计算机、通信模块)。未经 UAS 构造商(或制造商)认证的第三方服务器/设备可能有未知的漏洞或后门。这种攻击可以利用/使用这些漏洞/后门对操作进行网络攻击。例如，第三方公司的维护人员可以合法地到达无人机系统并非法修改无人机系统的参数。当完整的 u- 空间概念可用的时候，这个特性将更加重要(见1.4)。在那个时候，许多与操作相关的任务和设备将由第三方供应商提供。

在 OCSL 的确定步骤中，我们通过分析通信、操作类型、监控水平和第三方(可靠性)四个特征来评估操作敏感性。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。在这项操作中，飞行器将在远离高速公路的地面站的飞行员持续监控下自动飞行。为了保持车辆与地面控制站之间的长距离通信，无人机采用互联网(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系统(包括所有材料和维护服务)。根据表4.8，这个操作被评估如下:

沟通: 因为操作使用互联网来维持沟通，我们给这个特征分配2。

操作类型: 由于 BVLOS，我们为这个特性指定1。

监控级别: 由于飞行员连续监控操作，我们为这个特性指定0。

第三方可靠性: 操作不使用任何第三方服务/设备，因此该特性被指定为0。

最后，操作网络安全敏感性级别或 OCSL 是3。

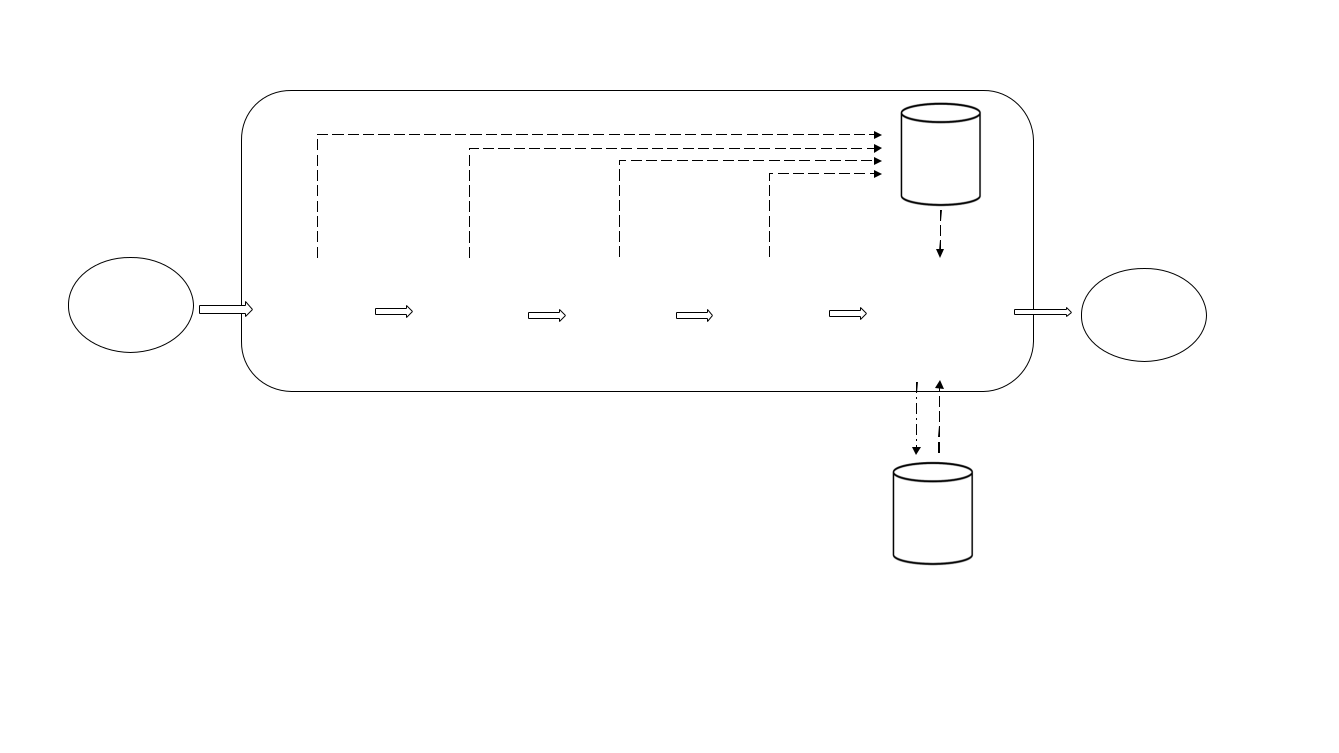
第四章操作风险评估: 从安全到网络安全

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 沟通 | 类别 | 监测水平 | 第三方(\*) |  |
| 行动 |  |
| - 2分 | - 1分 | - 1分 | - 2分 |  |
| 使用公共网络 | BVLOS | 如果不是连续的 | 如果不可信的第三者 |  |
|  |  | 监察 | 一方服务/设备 |  |
| 例如互联网。 |  |  | 用于无人机系统 |  |
|  |  |  | 行动 |  |
| - 1分 | - 0分 | - 0分 | - 1分 |  |
|  |  |  | 如果只相信第三名 |  |
| 使用共享网络 | VLOS | 如果连续的话 | 方服务/设备 |  |
|  |  | 监察 | 用于无人机系统 |  |
| 例如内部网络 |  |  | 行动 |  |
| 的公司 |  |  |  |  |
| 用于其他活动 |  |  |  |  |
| - 0分 |  |  | - 0分 |  |
| 使用专用的 |  |  | 如果没有第三方 |  |
| 网络 |  |  | 服务/设备 |  |

(\*) : 可信赖的第三方是由无人机制造商验证/训练或认证的第三方

表4.8: 与 CS 相关的操作特性

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 4.6. 基于网络的扩展 sora 风险评估工具 | | | | | | | | | | | | | 79 |  |
|  |  | 用户浏览器 | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | 浏览器 |  |  |
|  |  | 使用者 | | 与地面有关 | | | | |  |  |  | 记忆 |  |  |
|  |  | 与隐私有关 | | |  |  |  |
|  |  | 资料 | | 资料 |  | 与空气有关 | | |  |  |  |
|  |  | 资料 | |  |  | 资料 | | | 资料 | | | 所有数据 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 使用者 | 欢迎 |  | 地面风险 |  | 空气风险 |  |  | 隐私风险 |  |  | 结果页面 | 使用者 |  |
|  | 网页 |  | 网页 |  | 网页 |  |  | 网页 |  |  |  |  |
|  | 输入 |  |  |  |  |  |  |  | 收到 |  |
|  | 网站 | 提示到 |  | 提示到 |  | 提示到 |  |  | 提示到 |  |  | 确定航向 | 名单 |  |
|  | 提供 |  | 提供 |  | 提供 |  |  | 提供 |  |  | 决定 |  |
|  |  |  |  |  |  |  |  | 目标 |  |
|  |  | 资料 |  | 资料 |  | 资料 |  |  | 资料 |  |  | 目的 |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |



|  |  |  |
| --- | --- | --- |
| 航海 | 详细说明 |  |
| 水平, |  |
| 目标 |  |
| 用户数据 |  |
|  |  |
|  | 数据库 |  |
|  | 在 Wix |  |
|  | 云 |  |

图4.9: 应用程序的概述

4.5.3 OCSO 鲁棒性的确定

操作网络安全目标(OCSO)必要的健壮性水平是通过使用表4.9从操作的 SAIL 和 OCSL 确定的。有了获得的 OCSL，我们可以通过查阅附录 a 中的 OCSOs 列表来确定详细的网络安全目标。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 6 | 中等 |  | 中等 | 很高 | 很高 | 很高 | 很高 |  |
|  | 5 | 中等 |  | 中等 | 中等 | 很高 | 很高 | 很高 |  |
| OCSL | 4 | 中等 |  | 中等 | 中等 | 中等 | 很高 | 很高 |  |
| 3 | 很低 |  | 中等 | 中等 | 中等 | 中等 | 很高 |  |
|  | 2 | 很低 |  | 很低 | 中等 | 中等 | 中等 | 中等 |  |
|  | 1 | 很低 |  | 很低 | 很低 | 中等 | 中等 | 中等 |  |
|  |  | I |  | 二 | 三 | 四 | V | 六 |  |
|  |  |  |  |  | 航海 | |  |  |  |
|  |  |  | 表4.9: 法律事务厅的决定 | | | |  |  |  |

4.6一个基于扩展 sora 的风险评估工具

4.6.1说明及目的

这个工具帮助用户根据 SORA 方法及其扩展自动进行风险评估。首先提示用户提供关于扩展操作的输入信息。基于这些信息，我们的工具然后自动确定与这些操作相对应的 SAIL 级别和相关的安全目标。这个工具是为不同类型的用户开发的，具有不同的用途: (1)操作员可以快速确定与预期操作相关的目标; (2)操作员可以配置预期操作

80第4章操作风险评估: 从安全到网络安全

运营和平衡运营绩效和满足目标的成本;

无人机制造商/建造商可以迅速预测与其客户的具体操作有关的目标; (4)管理局也可以使用这一工具快速核实需要授权的操作。此外，开发这一工具是为了便于今后扩展这一工具，以便对 SORA 方法进行新的扩展，例如考虑到新的危害和新的威胁。

4.6.2设计和实现

图4.10: 一些必需的信息

这个工具是一个基于 Wix 平台开发的 web 应用程序。这个平台提供了必要的工具/服务来快速创建一个网站，它支持 java 脚本语言来创建定制的功能。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浏览这五个页面。在第一页，用户被提示提供一般用户信息(姓名，联系人，角色，目的)。在第二页，用户必须提供与地面风险有关的信息，例如飞机的大小、作业区域和缓解措施(该页的一部分如图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。这些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。基于这些信息，最后一个页面运行风险评估。首先，页面决定了 SAIL 水平。该页面允许用户选择考虑哪些风险以确定 SAIL 水平(见图4.11) ，例如，地面风险和空中风险(原始 SORA)或所有风险(扩展 SORA)。然后该页面向 Wix 云上的数据库发送一个请求，以获得与确定的 SAIL 水平相关的详细目标。此外，所有用户提供的信息也会发送到我们的 wix 云数据库并存储在其中。最后，所有与预期操作相对应的目标都会显示给用户。本应用程序的手册可在附录 b 中找到。

以目前的设计，我们的工具可以很容易地扩展到采用其他的 SORA 方法-

|  |  |  |
| --- | --- | --- |
| 4.7结论 | | 81 |
|  |  |  |
|  |  |  |

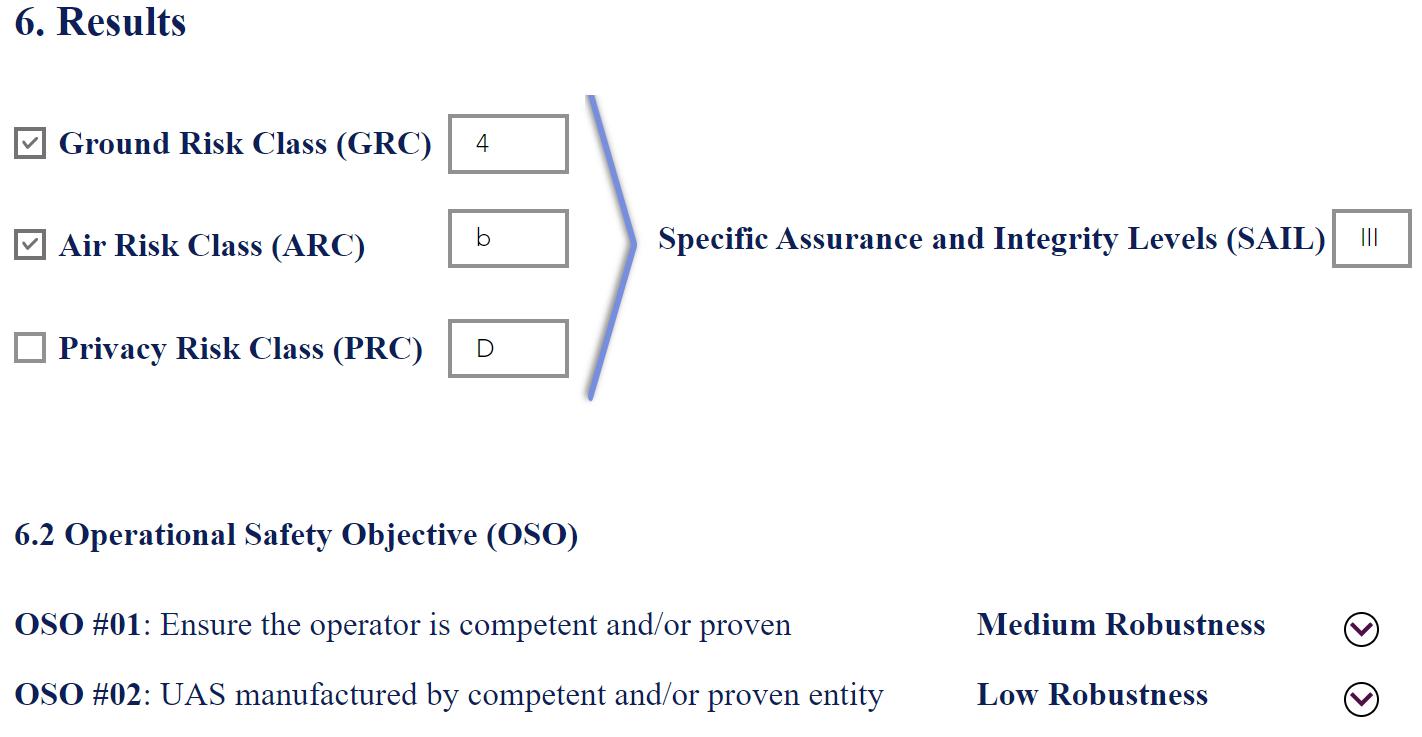


图4.11: 带有2D-SAIL 的结果页面

逻辑扩展。对于一个新的 Harm 扩展，我们只需要添加一个新页面来提示用户提供与此类 Harm 相关的信息，并对结果页面稍作修改。同时，我们只需要添加一个新的页面，提示用户提供与此类威胁相关的信息，并在数据库中添加新的威胁扩展目标。

4.7结论

在这项工作中，我们的目标是将原始的 SORA 方法论扩展到网络安全方面。SORA 方法的当前文档只解释了如何使用它，但没有解释它是如何工作的。因此，我们基于现有文档和我们对风险评估的了解来描述该方法的概念。然后基于这个概念，我们提出了一个扩展方法论的方法。该方法由两部分组成。第一个(Harm 扩展)是考虑网络安全/安全问题可能导致的新的危害。目前，我们关注的是“侵犯隐私”的危害——一个公众接受无人机操作的关键问题。但我们也可以将 SORA 方法扩展到其他类型的危害，使用相同的策略，如财务危害、材料销毁、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)(相对于原始方法所涵盖的意外威胁)以及相关的网络安全缓解。在此之后，我们提出了一个基于网络应用程序的风险评估工具。该工具旨在简化风险评估任务，并快速适应其他提议的 SORA 扩展。在本论文的下一章，我们用不同的案例研究来说明我们的方法。

第五章

扩展的 SORA 方法说明

目录

|  |  |  |
| --- | --- | --- |
| 5.1 | 引言... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ... ..。 | 84 |
| 5.2 | 将我们的方法与项目中使用的方法进行比较 |  |
|  | 多重无人机..。 | 84 |

|  |  |  |
| --- | --- | --- |
| 5.2.1 | CONOPS 的描述..。 | 84 |
| 5.2.2 | GRC 检测结果..。 | 85 |
| 5.2.3 | ARC 的决定..。 | 86 |
| 5.2.4 | 中华人民共和国的决心。 | 86 |
| 5.2.5 | 航海家号的决定。 | 87 |
| 5.2.6 | OSO 稳健性决定... ... ... ... ... ... ... ... ... ... ... ... ..。 | 88 |
| 5.2.7 | OCSL 的判决..。 | 89 |
| 5.2.8 | OCSO 稳健性决定。 | 89 |
| 5.2.9 | 结果讨论..。 | 89 |
| 5.3其他案例研究的应用。 | | 90 |
| 5.3.1 | ”无人机在市区运送”行动。 | 91 |
| 5.3.2 | 工业现场监控。 | 94 |
| 5.4利用扩展的 SORA 方法进行系统开发 | |  |
| (法语) | . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 97 |
| 5.4.1 | 初步行动描述。 | 98 |
| 5.4.2 | 扩展 SORA 分析。 | 99 |
| 5.4.3 | 最终行动描述。 | 101 |
| 5.4.4 | 系统描述..。 | 104 |
| 5.5结论。 | | 107 |
|  |  |  |

83

84第5章扩展的 SORA 方法的说明

5.1引言

在前一章中，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，我们使用这种方法来评估不同的操作。基于风险评估结果，我们讨论了方法的不同方面，并提出了一些改进建议。此外，SORA 方法首先被设计为运营商和管理当局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一个定义好的 UAS 操作和系统是否可以被批准。但它也可以用于开发目的。本章阐述了扩展的 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，我们应用我们的方法论对一个真实的操作进行评估，使用文献5.2节中的原始方法论。然后，我们在第5.3节考虑另外两个与市场有关的操作。接下来，我们将在第5.4节中说明如何在开发过程中使用从扩展的 SORA 获得的评估结果。我们在第5.5节结束了我们的工作

5.2将我们的方法与 MULTIDRONE 项目中使用的方法进行比较

在本节中，我们对一个由欧盟资助的项目—— MULTIDRONE 中引入的无人机操作进行风险评估。在这次行动中，一架无人机被部署在乡村地区与一些公众一起拍摄一场划船比赛。Capitán 等[204]的工作中引入了这一操作的风险评估。在这项工作中，作者使用原始的 SORA 方法进行了风险评估。在这个案例研究中，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 描述

操作的完整描述很长(如 SORA 方法学附件 a 所述)。因此，我们只给出了一个总结的描述，并提供了一些必要的信息，以便在这一步骤中进行风险评估。更详细的信息可以在[204] ，[205]中找到。

在这次行动中，无人机将跟随船只飞行拍摄照片。由于操作范围很大(比赛路径为15公里) ，无人机将在飞行员的超视距视线(BVLOS)模式下以自主模式飞行。这次行动是在人口密度较低的农村地区进行的。据推测，河流两岸可能有很多观众，而无人机不会飞越他们上空。表5.1总结了预期行动的基本信息。

5.2比较我们的方法与项目中使用的方法

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 多重无人机 | | 85 | |  |
|  |  |  |  |  |
|  | 主要无人机及操作规范 | |  |  |
|  | Frame 框架 | 大疆 S1000 + |  |  |
|  | 自动驾驶仪 | Pixhawk 2.1 |  |  |
|  | 沟通 | 泰利斯 LTE/Wi-Fi |  |  |
|  | 通信模块 |  |  |
|  |  |  |  |
|  | 降落伞 | Galaxy GRS 10/350 |  |  |
|  | 照相机 | BMMC + 松下 Lumix g x Vario Lens |  |  |
|  | 大小 | 1,45米 |  |  |
|  | 重量 | 11公斤 |  |  |
|  | 高度 | 10米 |  |  |
|  | 飞行模式 | 自主 |  |  |
|  | 行动类型 | BVLOS |  |  |

表5.1: UAS 和操作规范(来自 MULTIDRONE 项目)

5.2.2 GRC 测定

我们首先确定操作的内在 GRC，它指的是不考虑安全措施的地面人员的内在风险。因为无人机在农村地区飞行，不会飞越观众上空，所以我们将地面作战区域归类为人烟稀少的环境。根据操作区域和车辆大小(小于3米)的信息，我们为内在 GRC 分配了4，如表5.2所示。

内在地面风险等级

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 最大车辆尺寸 | 1米 | 3米 | 8米 | 超过8米 |  |
|  | Operation scenario 操作场景 |  |  |  |  |  |
|  | VLOS/BVLOS 飞越控制地面区域 | 1 | 2 | 3 | 4 |  |
|  | 在人烟稀少的环境中的 VLOS | 2 | 3 | 4 | 5 |  |
|  | 人口稀少环境下的 BVLOS | 3 | 4 | 5 | 6 |  |
|  | 人口密集环境下的 VLOS | 4 | 5 | 6 | 8 |  |
|  | 人口密集环境中的 BVLOS | 5 | 6 | 8 | 10 |  |
|  | VLOS over gathering of people 超过人群聚集的视频 | 7 | 没空 | | |  |
|  | BVLOS over gathering of people BVLOS 超过人群聚集 | 9 |  |
|  |  |  |  |  |

表5.2: SORA 方法的内在 GRC 表

然后，我们研究行动的危害障碍，包括应急响应计划，战略缓解和减少地面影响。预期的行动没有实施任何应急计划，也没有提到任何地面风险的战略缓解措施。这导致了 GRC 的增加(见表5.3)。操作员只是用降落伞作为伤害屏障来减少地面冲击。我们假设制造商测试了这种降落伞，在不利的激活情况下，降落伞不会影响操作的安全性。因此，这种危害屏障处于中等健壮性水平，有助于降低 GRC (见表5.3)。操作的最终 GRC 保持在4。

2小时晒黑

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 86 | 第五章，扩展的 SORA 方法的说明 | | | | | |
|  |  |  |  |  |  |  |
|  |  | 健壮 | |  |  |  |
|  | 伤害屏障 | 低/无 |  | 中等 | 很高 |  |
|  | 地面风险的战略缓解 | 0 |  | - 2 | ー4 |  |
|  | 减少地面撞击的影响 | 0 |  | - 1 | - 2 |  |
|  | 紧急应变计划 | 1 |  | 0 | - 1 |  |
|  | 完全修正 | 0 |  |  |  |  |

表5.3: 最终确定 GRC 的缓解措施

5.2.3 ARC 确定

由于飞机在离地面10米的高度飞行，在农村地区和不受控制的空域，与其他飞机相撞的风险很低。因此，预期操作的初始 ARC 为 b，广义飞行密度为1(按5级标度[104])。为了降低运营的空气风险，运营商实施边界缓解作为一个危害屏障，以限制运营量。然而，在这种情况下，根据 SORA 的方法，危害屏障是没有用的，因为初始的碰撞概率太低，无法降低。由于这个原因，最终的 ARC 保持在 b 级。

5.2.4中国的决定

正如我们在建议中提到的，我们分析了 UAS 的一些特性以及确定隐私风险类别(PRC)的操作。这一步骤的大部分输入数据已在表5.1中提供，除了关于相机最小视角(AOV)的数据/信息。操作描述没有提供 AOV 的信息，但是我们可以根据照相机的规格手动计算它。照相机的规格如表5.4所示。

BMMC 相机配备松下 Lumix g x Vario 镜头

|  |  |
| --- | --- |
| 解决方案 | 2432x1366 |
| 传感器大小 | 16.64 mm x 14.04 mm |
| 焦距 | 从14毫米到42毫米 |

表5.4: 摄像机规格(来自 MULTIDRONE 项目)

相机的最小 AOV 计算如下:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| minAOV = 2 arctan minAOV = 2 arctan |  | 传感器宽度 | = 11:2 |  |
|  |  |  |
| 2 | 最大焦距最大焦距 |  |
|  |  |  |  |

然后，我们得到无人机捕捉到的图像的最大像素密度如下:

P d = 水平像素数 = 1240(像素 = m)

|  |  |
| --- | --- |
| 5.2比较我们的方法与项目中使用的方法 |  |
| 多重无人机 | 87 |

因此，图像的细节处于“ Inspect”级别(见表4.2)。此外，UA 以 BVLOS 模式飞行，飞越了一个农村地区。因此，我们为这个操作指定了 d 的内在 PRC (见表5.5)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| 类别 | 乡下 | 乡下 | 都市 | 都市 |  |
| 地带, | 地带, | 地带, | 地带, |  |
| 行动 |  |
| VLOS | BVLOS | VLOS | BVLOS |  |
|  |  |
| 图像细节 |  |  |  |  |  |
| 水平 |  |  |  |  |  |
|  | A | B | C | C |  |
| 监视器 |  |
|  | B | B | C | C |  |
| 侦测 |  |
|  | B | C | D | D |  |
| 观察 |  |
|  | C | C | D | D |  |
| 识别 |  |
| 识别 | C | D | E | E |  |
| 视察 | C | D | E | F |  |

表5.5: 内在 PRC 确定

操作的最终 PRC 是初始 PRC 减去由损害壁垒提供的风险降低。然而，操作描述没有提到任何损害屏障的损失隐私的人在地面上。因此，我们假设经营者没有应用任何伤害壁垒，最终的 PRC 仍然是 d。

5.2.5航标的确定

操作被分配到一个 ARC 为 b，GRC 为4。因此2D-SAIL 的值(考虑到 ARC 和 GRC)是 III (见表5.6)。对于 III 的2D-SAIL 和 d 的 PRC，3D-SAIL (考虑 ARC、 GRC、 PRC)的值为 IV (见表5.7)。

帆的确定

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | ARC | |  |  |
|  | GRC | a | b | c | d |  |
|  | 2 | I | 二 | 四 | V | |
|  | 3 | 二 | 二 | 四 | V | |
|  | 4 | 三 | 三 | 四 | V | |
|  | 5 | 四 | 四 | 四 | V | |
|  | 6 | V | V | V | V | |
|  | 7 | 六 | 六 | 六 | 六 | |

表5.6: SAIL 的确定[104]

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 88 | 第五章。 | | 扩展的 SORA 方法说明 | | | | | | |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 2D-SAIL | |  |  |  |
|  |  | 中国 | I | 二 | 三 | 四 | V | 六 |  |
|  |  | A | I | 二 | 三 | 四 | V | 六 |  |
|  |  | B | 二 | 二 | 三 | 四 | V | 六 |  |
|  |  | C | 三 | 三 | 三 | 四 | V | 六 |  |
|  |  | D | 四 | 四 | 四 | 四 | V | 六 |  |
|  |  | E | V | V | V | V | V | 六 |  |
|  |  | F | 六 | 六 | 六 | 六 | 六 | 六 |  |

表5.7:3D-SAIL 测定

5.2.6 OSO 稳健性的确定

使用 IV 的最终 SAIL 值(3d-SAIL) ，我们可以确定每个 OSO 的鲁棒性水平，然后确定需要实现的详细目标。详细目标载于附件 e。由于 SORA 方法旨在支持经营无人机的授权申请，有些目标涉及经营者而不是制造商(例如评估天气状况和经营者的能力)。因此，在这个案例研究中，从制造商的角度出发，我们讨论了一些关键的 OSOs，这些 OSOs 可以被认为是无人机开发过程中针对预期操作的投入:

OSO # 04在低级别的健壮性。它要求无人机必须发展到主管当局认为足够的标准。这些标准应该应用于低水平的完整性(用这些标准定义)。制造商不必提供支持证据，只需宣布标准符合。尽管如此，现在还没有任何专门针对 UAS 开发的标准。或者，制造商可以应用一些在航空领域被广泛接受的安全标准，如 DO178C，DO256。制造商还必须考虑到与隐私和数据保护相关的标准。

OSO # 06在中等水平的健壮性。它要求通信链路的特性适合于操作。由于无人驾驶飞机在不受控制的空域飞行，飞行员不需要与空中交通管制中心(ATC)保持通信，因此通信链路只用于控制飞行器。无人机可以使用未经许可的频段进行通信，比如2.4 GhZ。然而，无人机系统需要为飞行员提供监控通信链路的手段(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 的这些保护特性必须得到有能力的第三方的验证。

OSO # 18处于中等健壮性水平。它要求无人机能够检测和防止导致无人机超过其飞行性能的不正确的飞行员输入(例如，飞行员让无人机下降得太快)。飞行包线的自动保护已经发展到主管当局认为足够的标准。

|  |  |
| --- | --- |
| 5.2比较我们的方法与项目中使用的方法 |  |
| 多重无人机 | 89 |

5.2.7 OCSL 测定

在这一步，我们分析了四个特点: 通信、操作类型、监控水平和第三方。对于通信，UAS 配备了 Thales LTE/wifi 通信模块。我们没有关于这个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无人机。在这次行动中，飞行器以 BVLOS 模式飞行，并在飞行员的持续监控下飞行。考虑中的无人机是基于一些开源组件(如自动驾驶仪)构建的，我们认为这是一个不可信任的第三方设备。基于这个分析，我们为这个操作指定 OCSL 为3(见表5.8)。

|  |  |  |
| --- | --- | --- |
| 特点 | 描述 | 分数 |
| 沟通 | 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 | 非可信设备 | 2 |
| OCSL |  | 3 |

表5.8: OCSL 测定结果

5.2.8 OCSO 鲁棒性的确定

对于这个操作，最终的 SAIL 为 IV，OCSL 为3，所有 OCSOs 应该满足中等的健壮性水平(见表4.9)。例如:

OCSO # 1-防止未经授权的个人进行恶意行为。在中等健壮性水平上，这种 OCSO 需要机制来验证试图进入地面控制站(GCS)或自动驾驶仪的人的身份。然而，目前，这些特性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，这种 OCSO 需要通过两种方法来验证传感器数据。第一种是检查来自传感器的数据是否超过了合理的阈值。这种方法目前被用于该操作中的自动驾驶软件所采用。第二种方法是检查不同传感器之间的交叉一致性。对于这个操作中使用的自动驾驶仪，我们没有关于这个机制的任何信息。

5.2.9结果讨论

对于这个案例研究，我们已经用我们的扩展 SORA 方法对欧盟资助的 MULTIDRONE 项目中提到的无人机操作进行了风险评估。作为前辈

90第5章扩展的 SORA 方法的说明

Capitán 等[204]基于原始 SORA 方法对同一操作进行了风险评估。表5.9列出了这些结果的总结。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 上尉和其他人 | 我们的评估 |  |
|  | 评估[204] |  |
| 方法 | SORA 网站 | 扩展 SORA |  |
| GRC | 2 | 4 |  |
| ARC | a | b |  |
| 中国 | 不适用 | D |  |
| Final SAIL 最终帆 | I | 四 |  |
| OCSL | 不适用 | 3 |  |

表5.9: 结果比较

根据上面的表格，我们的风险评估给出的 SAIL 的临界值比 Capitán 等人给出的临界值更大。因此，在我们的评估中，安全目标(OSO)需要更高的稳健性水平。例如，在我们的评估中，无人机必须设计为确定可能的故障并尽量减少其发生。同时，在 Capitán 等人的评估中，这个目标是不必要的。这种差异有两个原因。第一个问题是，Capitán 等人使用了原来 SORA 方法的旧版本，该方法在评估之时仍处于开发阶段，缺乏明确的指示。这导致了对障碍的健壮性水平(例如，降落伞)的高估。第二个原因是我们的评估考虑了隐私对地面人员的伤害。在这个操作中，隐私伤害是一个必不可少的方面，因为 UAS 配备了一个高性能的摄像头，并且操作发生在拥挤的事件中。此外，与 Capitán 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有关的目标。一些已确定的网络安全目标在考虑的操作中没有实现。为了实现这些目标，需要戏剧性地改变操作和无人机系统。这种改变可以使操作更加安全，但也会影响操作的成本效益。

5.3应用于其他案例研究

在上一节中，我们将我们提出的方法应用于一个真正的无人机操作，该操作在一个欧洲研究项目中得到了很好的记录。在这一部分，我们介绍了另外两个案例研究: “无人驾驶飞机在城市地区交付”和“工业现场监测”，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应用于其他案例研究 | 91 |

5.3.1”在市区运送无人驾驶飞机”行动

5.3.1.1行动描述

在此操作中，一家电子商务公司将使用 UASs 将货物从仓库运送到城市中的客户。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，并为仓库周围6公里内的客户提供服务。因此，飞机完全在市中心(市区)飞行。

飞行计划在40米的高空进行，超出了飞行员的视野范围(BVLOS 模式)。对于每次交付，飞机将根据客户的位置按照不同的轨道飞行。因此，飞行员应该在操作前准备好飞行计划并上传到无人机上。在操作过程中，飞机自动按照预定的飞行计划飞行，并在飞行员的监控下飞行。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，监测飞行，解决异常情况。飞机将配备一个小型 RGB 摄像头来帮助飞行员监控交付过程。该相机的分辨率为1920x1080像素，视角为40。我们假设该相机能够探测到地面上的人，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)。

经营者计划使用一架最大尺寸为1.5米、最大重量为10公斤的无人驾驶飞机。因为飞行是在人的上空进行的，所以飞机上装备了降落伞。我们假设操作员将建立一个应急响应计划(ERP)来应对紧急情况。这份操作文件阐明了每个船员在紧急情况下的任务和角色。据推测，降落伞和 ERP 系统都符合当局采用的标准。

5.3.1.2扩展 SORA 分析

我们基于扩展方法进行风险评估，以确定安全目标(OSOs)和网络安全目标(OCSOs)。

首先，我们确定预期操作的地面风险等级(GRC)。由于飞行发生在城市区域的 BVLOS 模式和飞机的尺寸小于3米，内在的 GRC 被分配到7。GRC 可以通过两个危害屏障来降低: 紧急响应计划(ERP)和降落伞。根据操作描述，这些障碍将是一个中等水平的健壮性，并有助于减少1点的 GRC。因此，这个操作的最终 GRC 是6。

92第5章扩展的 SORA 方法的说明



6公里

送货区

50m

图5.1: 运送作业

我们确定预期操作的风险等级(ARC)。飞机将在市中心上空150米的高空飞行，远离机场。因此，根据 SORA 的方法，这次行动的 ARC 是 c。

结合 c 的 ARC 和 GRC 的6，我们得到了 v 的2D-SAIL (见表4.1)。

我们确定预期操作的隐私风险类别(PRC)。基于相机的规格(1920x1080分辨率，40视角)和飞行高度，我们计算捕捉到的图像的像素密度。它是每米65.9像素，相当于“观察者”的细节水平(见表4.2)。由于航班发生在城市区域，采用 BLVOS 模式，因此本文给出了 d 的内在 PRC 值，此外，摄像机还能自动检测和模糊人的图像。这个功能有助于保护人们在地面上的隐私，并减少了中国1点。因此，该操作的最终 PRC 是 c。

结合 v 的2D-SAIL 和 c 的 PRC，我们得到了 v 的 SAIL 3D，利用这个 SAIL 值，该操作将在高鲁棒性水平上满足 OSOs 的要求。详细目标见 SORA 方法的附件 e [98]。

我们评估预期操作的网络安全敏感性(OCSL)。我们假设无人机将使用移动网络(4G)来维持飞机和地面站之间的通信。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 的4，如表5.10所示。

使用 v 型的3D-SAIL 和4型的 OCSL，操作应在高稳健性水平上满足 OCSOs 的要求。OCSOs 的详细资料载于附件一。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 5.3应用于其他案例研究 | | | 93 | |
|  |  |  |  |  |
|  | 特点 | 描述 | 分数 |  |
|  | 沟通 | 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 | 只有可信的设备 | 1 |  |
|  | OCSL |  | 4 |  |

表5.10: OCSL 测定结果

分析

Grc62d-sail v

ARC c 3D-SAIL v

中华人民共和国 OCSL 4

分析

Grc63d-sail v

ARC c 3D-SAIL v

中华人民共和国刑事诉讼法第4条

(a)设有私隐保护过滤器(b)没有私隐保护过滤器

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5.11 a 所示。根据上述分析，根据上述操作描述，操作员必须在高稳健性水平(20/24目标)达到大部分的操作安全目标，以及在高稳健性水平上达到所有的操作网络安全目标。据我们所知，目前市场上还没有一个系统能够满足这些目标。一方面，我们发现这种操作将会非常昂贵。因为它需要很多资源来实现复杂的网络安全解决方案，并符合不同的标准(开发、设计、维护等等)。另一方面，我们仍然可以稍微降低这种操作的成本。在操作描述中，我们假设摄像头可以识别地面上的人的图像，并将他们从视频中删除。这种相机可能比没有这个功能的标准相机更贵。如果我们移除这个功能会发生什么(隐私保护过滤器)。在这种情况下，操作的 PRC 将是 d 而不是 c。新的分析如表5.11 b 所示。我们有相同的3D-SAIL 值，然后相同的 OCSOs 和 OSOs。因为在这个操作中，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，我们可以使用一个标准的摄像头来降低运营成本，同时又不会增加 OCSOs 和 OSOs 的复杂性。

让我们考虑同样的案例研究，但较低的高度(20米)和较高性能的相机(分辨率为4000x3000像素，最小视角为11)。分析结果如表5.12 a 和5.12 b 所示。在操作描述中，如果没有提到隐私保护过滤器，3D-SAIL 从 v 增加到 VI，我们必须满足所有的 OSOs

1 Sogilis 公司的一个分公司正在参与 CEDSO 项目(安全作业认证无人机系统) ，以开发一种经认证的无人机，用于在与 SAIL VI 相对应的城市地区进行作业

94 Chapter 5第五章扩展的 SORA 方法的实例

在一个高度健壮的水平(而不是只有20/24目标)。这使得操作成本增加。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 分析 | |  |
| GRC | 6 | 2D-SAIL | V |
| ARC | c | 3D-SAIL | V |
| 中国 | E | OCSL | 4 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 分析 | |  |
| GRC | 6 | 2D-SAIL | V |
| ARC | c | 3D-SAIL | 六 |
| 中国 | F | OCSL | 4 |

(a)设有私隐保护过滤器(b)没有私隐保护过滤器

表5.12: 修改后的递送操作的分析结果

通过这些讨论，我们认为 SORA 方法(扩展或原始版本)应该以优化操作成本的方式使用。具体而言，如果可能的话，我们可以调整操作描述的一些参数，以获得具有较低鲁棒性水平的 OCSOs 和 OSOs。这个论点对于操作者和制造商特别有帮助。因此，当我们在开发过程中使用扩展的 SORA 方法论时，我们会考虑到这个论点(见5.4)。

5.3.2工业现场监控

5.3.2.1操作说明

在这次行动中，一家工业公司将使用无人机监控其工业场所。假设这个工厂远离居民区和机场。因此，我们可以认为飞机在农村地区上空飞行。飞机重约20公斤，最大尺寸为2米宽。

飞机将按照预定的轨道在30米的高度绕工厂飞行。飞机不允许飞越工厂区域。由于工业基地非常大，飞机将飞出飞行员的视线范围并自动操作。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。

如果出现故障，公司希望尽快在操作区域内确定飞行情况(操作区域内无人)。此外，降落伞不能用来防止飞机坠落到工厂。

这架飞机将配备一个 RGB 摄像头来监视工业现场。该相机的分辨率为1920x1080像素，最小视角为20

|  |  |
| --- | --- |
| 5.3应用于其他案例研究 | 95 |

5.3.2.2扩展 SORA 分析

我们执行基于扩展方法论的风险评估，以确定安全目标(OSOs)和网络安全目标(OCSOs)。

首先，我们确定预期操作的地面风险等级(GRC)。由于飞行发生在乡村地区(人口稀少的环境)的 BVLOS 模式和飞机的尺寸小于3米，内在的 GRC 被分配到4。

我们确定预期操作的空气风险等级(ARC)。这架飞机将在一个农村地区上空飞行，低于150米的高度，远离机场。因此，根据 SORA 的方法，这次行动的 ARC 是 b。

结合 b 的 ARC 和 GRC 的4，我们得到了一个 III 的2D-SAIL (见表4.1)。

我们确定预期操作的隐私风险类别(PRC)。基于相机的规格(1920x1080分辨率，20视角)和飞行高度，我们计算捕捉到的图像的像素密度。它是每米181像素，相当于“识别”的细节级别(见表4.2)。由于航班发生在农村地区，在 BLVOS 模式下，我们分配内在的中国 c。由于无人机是用来监视一个网站，没有隐私保护应用。因此，该操作的最终 PRC 保持在 c 级别。

结合 III 的2D-SAIL 和 c 的 PRC，得到了 III 的 SAIL 3D。有了这个 SAIL 值，操作应该以低或中等的鲁棒性水平满足 OSOs。SORA 方法的附件 e 列出了详细的目标[98]。

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

|  |  |  |
| --- | --- | --- |
| 特点 | 描述 | 分数 |
| 沟通 | 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 | 只有可信的设备 | 1 |
| OCSL |  | 2 |

表5.13: OCSL 测定结果

使用 III 的3D-SAIL 和2的 OCSL，操作应在中等健壮性水平上满足 OCSOs。OCSOs 的详细资料载于附件一。

96. 第五章扩展的 SORA 方法的说明

分析

Grc42d-sail III

ARC b 3D-SAIL III

中华人民共和国中华人民共和国 OCSL 2

表5.14: 隐私保护过滤器

5.3.2.3结果讨论

分析结果在表5.14中恢复。根据这个结果，运营商必须满足的目标只有一个低或中等的健壮性水平(相对于高健壮性水平的交付操作)。这个结果是典型的“工业现场监控”操作。工业场所通常分布在大片区域，远离居民区，远离机场。因此，“工业现场监控”操作有一些共同的特点，如农村操作区，BLVOS，低活动密度空域。根据 SORA 的方法，具有这些特征的操作通常并不重要。它不合理。例如，考虑到“核电站监测”、“太阳能发电计划监测”和“现场监测”这三种操作，我们得到了同样的结果。原因是，目前的版本(原版或扩展版)只考虑了对人类的直接伤害(生命或隐私的损失)。对基础设施或工业场所的伤害尚未开发。事实上，这个问题非常复杂，因为不同工业领域的危害评估可能是不同的。

目前，我们提出了一个临时解决方案来解决上述问题。对于“工业现场监控”操作，我们将在3D-SAIL 上增加“补充点”。这些点部分地表现了工业场所的关键性质。这些要点将根据以下两个问题进行评估: (1)工业场所是否生产或储存危险产品(如有毒、汽油、放射性物质) (2)“这个工厂是否存储敏感信息?”(见表5.15)。

|  |  |  |
| --- | --- | --- |
| 补充点 | |  |
| 工业用地类别 | 没有敏感信息 | 敏感信息 |
| 没有危险产品 | 0 | 2 |
| 危险产品 | 1 | 3 |

表5.15: “补充点”评估

对于上面提到的三个操作，使用这个解决方案，我们得到了新的结果，如表5.16所示。核电站是最重要的基础设施之一。因此，VI 的3D-SAIL 和 OSOs 在最高健壮性水平是合适的。如果我们不考虑可能的“财务”伤害，操作太阳能计划电力有相同的临界水平作为一个领域的操作。

利用扩展的 SORA 方法进行系统开发97

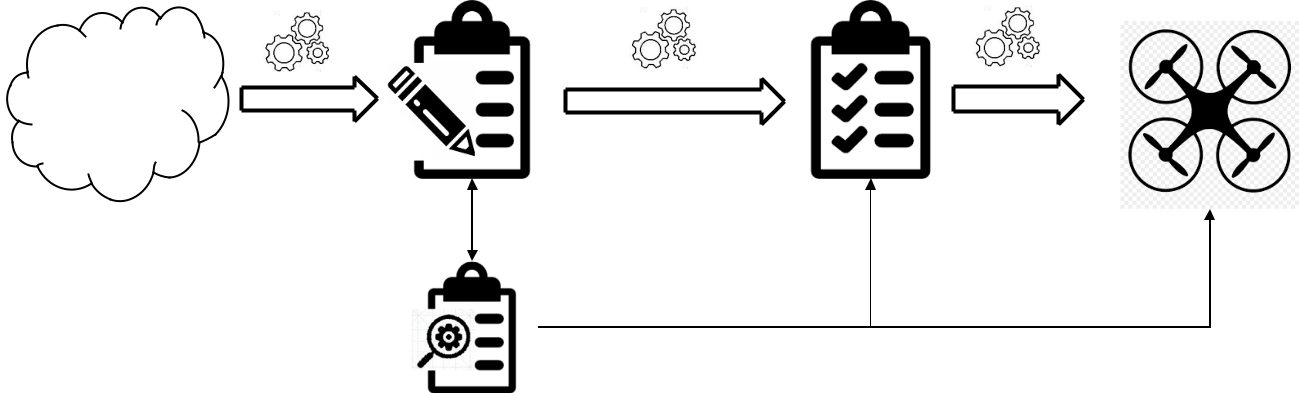
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 监察行动 | |  |  |
|  | 核电站 | 太阳能发电厂 | 一块田地 |  |
| 补充 | 3 | 0 | 不适用 |  |
| 分数 |  |
|  |  |  |  |
| 最终3D-SAIL | 六 | 三 | 三 |  |

表5.16: 应用补充点后三种监测操作的比较

5.4使用扩展的 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的简单信息(如操作区域，操作类型)来执行风险评估。这个评估的结果是一个安全和网络安全目标的列表。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 分析来完善操作描述和系统描述。因此，我们建议将扩展的 SORA 分析集成到开发过程的早期阶段，当客户的需求被转换成系统描述时。图5.2展示了我们的建议。本建议详细解释如下:

|  |  |  |
| --- | --- | --- |
| **1.** | **2.** | **3.** |
| 初步描述 | 最终描述 | 系统 |
| 行动计划 | 行动计划 | 描述 |



**客户的**

**要求**

奥索斯和奥索斯

**扩展 SORA 分析**

**(网络安全导向)**

图5.2: 将扩展的 SORA 分析集成到开发过程中的建议方法

初始操作描述: 在开发过程的开始，我们假设客户端只能提供关于所需操作的简单信息。这些信息可以是客户的需求或者关于操作的想法。例如，客户需要一个 UAS 来监控数千公顷的土地或者运送小包裹。这些信息不够详细，不足以执行扩展的 SORA 分析。因此,

98第5章扩展的 SORA 方法论的例证

我们首先建立初步的操作描述。本文件包括进行扩展 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、飞机大小、危害屏障等)。这些是在扩展的 SORA 方法中评估的操作参数。我们可以收集，理由，或选择这些参数基于与客户讨论他们的需求。

扩展 SORA 分析: 基于最初的操作描述，我们执行扩展的 SORA 方法。因此，我们得到了“操作”安全目标(OSOs)和“操作”网络安全目标(OCSOs)。在这一步，我们可以灵活应用方法论来优化操作成本，正如我们之前的结论(见5.3.1.3)。例如，我们可以添加新的危害屏障，在较低的健壮性水平上满足目标; 或者消除一些危害屏障，但在同一水平上满足目标。

最终操作描述: 在这一步中，我们基于 JARUS 在[184]中提供的表单建立最终操作描述。最终的操作描述应该符合安全/网络安全目标和上一步中定义的初始描述。此外，这个描述应该尽可能明确无人机将如何使用。

系统描述最后，我们描述满足最终操作描述、安全和网络安全目标的系统架构。

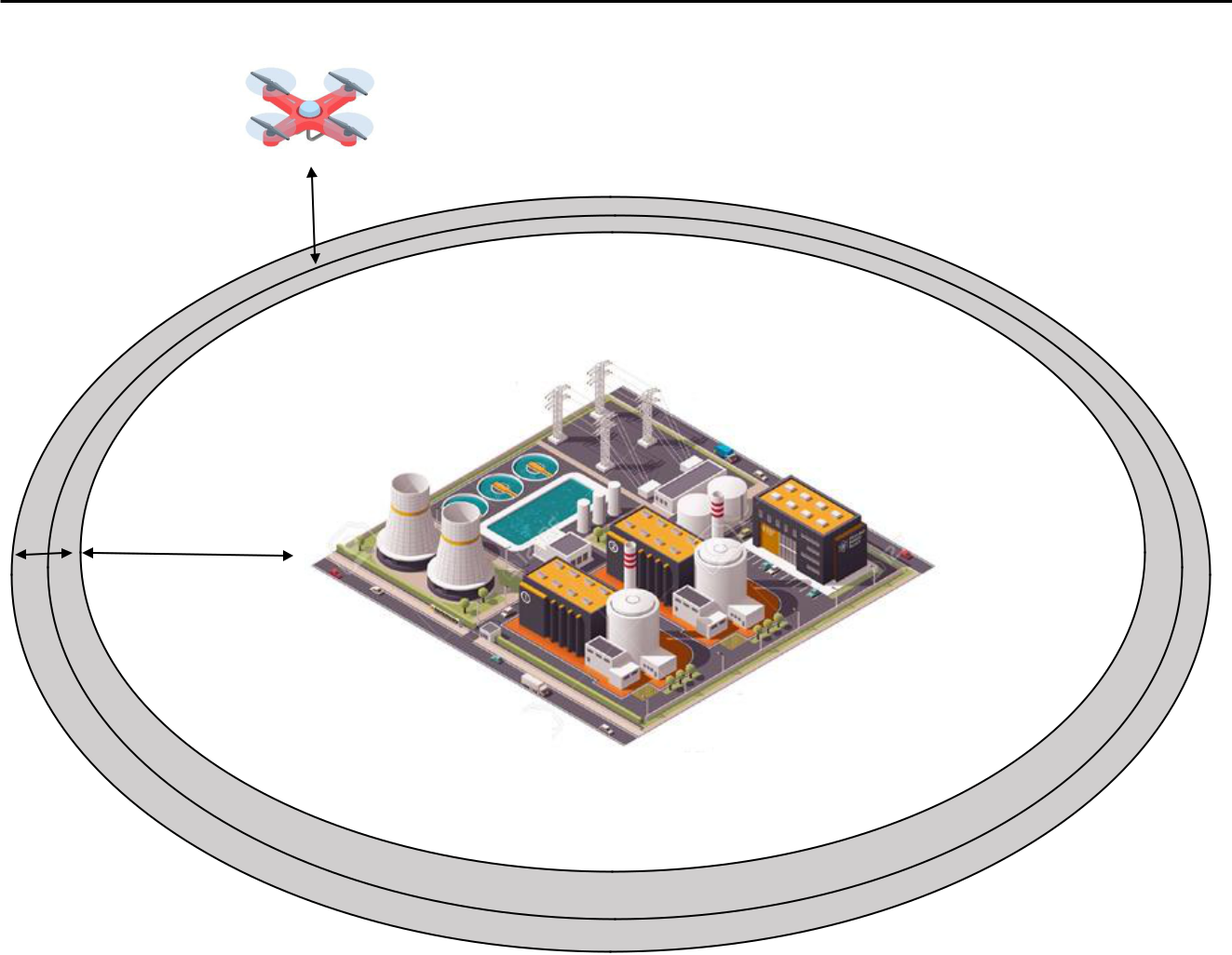
接下来，我们对“工业现场监控”的案例研究说明了上述方法。

5.4.1初始操作描述

为监察高度敏感的工业厂房(例如核电厂、化工厂) ，业主公司会安装一部装有热感应摄影机的无人机。无人机将被部署在位于农村地区的核电站周围进行飞行。飞行计划由业主公司定义，并在所有航班上重复执行。根据飞行计划，无人机不会飞越核电站，并与核电站保持200米的距离。检查区域附近没有任何机场。该无人机重20公斤，最大尺寸为2米宽，设计为在超视距视线(Beyond Visual Line Of Sight，BVLOS)上自动飞行，整个飞行过程的高度为离地面30米。

在飞行过程中，飞行员通过 GCS 计算机实时观察无人机的状态和高速公路。飞行员只需要执行三个简单的动作: 开始飞行，结束飞行(回到待机模式) ，回家。GCS 和飞机之间的数据交换是通过无线通信渠道传输的。

5.4. 利用扩展的 SORA 方法进行系统开发99



30米

20米200米

作业区

图5.3: 无人机操作系统

该架飞机装备有一部视像摄影机，其特性如下:

决议: 1920x1080

最小视角: 10度。

5.4.2扩展 SORA 分析

执行扩展的 SORA 分析，我们获得 VI 的3D-SAIL 和 OCSL (Operation Cybersecurity Susceptible Level)为2的给定操作。这个分析的细节在5.3.2中给出。根据该方法，我们应该在最高健壮性水平上满足 OSO，在中等水平上满足 OCSO。这些 OSOs 列于原始 SORA 方法的附件 e (读者可以在本论文的 e 部分找到它们) ，详细的 OSOs 列于表5.17。

|  |  |  |
| --- | --- | --- |
| 100 | 第五章，扩展的 SORA 方法的说明 |  |
|  |  | |
| 姓名 | 描述 | |
|  | - 定义过程/机制，以识别和认证试图 | |
| OCSO # 01 | 进入 GCS 和自动驾驶仪。 | |
|  | - 界定建立/修改/删除个人身份证的程序/机制 | |
|  | 定义组织中每个人的权利，这些人可以与 | |
| OCSO # 02 | 自动驾驶仪和昏迷指数。 | |
|  | - 界定分配/修改/撤销每个人权利的程序/机制 | |
|  | 个人 | |
| OCSO # 03 | 定义程序/机制来限制一个人可以执行的行为 | |
|  | 作为他被分配的权利 | |
|  | 定义安全机制来保护飞行计划，飞行的完整性 | |
| OCSO # 04 | 参数(PID 参数，滤波器 Kalman 参数，传感器校准等) | |
|  | 以及存储在 GCS 和自动驾驶仪中的记录数据(视频数据、日志数据)。 | |
| OCSO # 05 | - 界定保护数据/资料机密性的保安机制 | |
|  | 储存在 GCS 和自动驾驶仪中 | |
| OCSO # 06 | - 分析飞行后软件/硬件的异常行为，以检测 | |
|  | 飞行后检查中的异常行为。 | |
|  | 将软件/硬件架构划分为不同的“区域” | |
| OCSO # 07 | 不同的关键程度。一些硬件/软件可能易受 | |
|  | 网络攻击，但它们提供的功能没有其他攻击那么重要 | |
|  | 其他的 | |
| OCSO # 08 | - 定义机制，以确保通过 | |
|  | 通讯设备。 | |
| OCSO # 09 | - 界定机制，以确保每个数据包/电文的完整性 | |
|  | 通过通信设备传输 | |
|  | - 界定用以衡量通讯频道性能的参数。 | |
| OCSO # 10 OCSO # 10 | - GCS 会向飞行员显示已定义的参数 | |
|  | - 建立一个安全指令，飞行员可以用来检测降落 | |
|  | 通讯频道的表现 | |
| OCSO # 11 OCSO # 11 | - 确定重新建立通信或维持若干通信的机制 | |
|  | 基本服务，以防通信绩效下降。 | |
|  | - 定义用于诊断通信性能的参数 | |
|  | 这些参数将被记录在自动驾驶仪上 | |
| OCSO # 12 | 和格拉斯哥昏迷指数。 | |
|  | - 制定飞行员或维修人员可以使用的安全指示 | |
|  | 通过检查航海日志来发现异常 | |
| OCSO # 13 | ー根据《通讯条例》将通讯系统划分为不同的频道 | |
|  | 传输数据的临界等级和脆弱等级。 | |
| OCSO # 14 | - 通过分析异常传感器数据的一致性，确定探测异常传感器数据的机制 | |
|  | 和来自不同传感器的数据之间的一致性。 | |
|  | - 制定保护传感器免受环境干扰的解决方案 | |
| OCSO # 15 OCSO # 15 | (攻击者可以操纵加速器传感器的输出 | |
|  | 通过使用其共振频率的干扰) | |

5.4. 利用扩展的 SORA 方法进行系统开发101

表5.17: 具有中等健壮性水平的 OCSO 的定义

5.4.3最终操作说明

我们可以根据定义的 OCSOs 和 OSOs 以及初始操作描述建立最终的操作描述。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。关注本论文的主题——网络安全，我们在这里只提到与网络安全方面相关的信息。

5.4.3.1运算符

我们打算由三个人操作无人机: 一个操作经理，一个主要飞行员和一个次要飞行员。运营经理负责整个运营并管理飞行员。主要的飞行员负责观察和控制飞机。副驾驶负责操作摄像机，观察工厂。根据每个成员的角色，他们的权利被定义如下:

操作经理可以创建/修改/删除试点帐户

为了控制和观察飞行，主要的飞行员可以:

- 从 GCS 向飞行器发送命令(起飞、降落、按计划飞行、飞行终止)。

获取飞行信息(高度，位置，姿态，电池信息，通讯状态)。

控制和指挥车辆。

- 获取摄影机拍摄的影像资料。

- 查阅记录在案的文件，进行飞行后分析。

为了控制摄像头和观察工业现场，副驾驶员可以:

- 获取摄影机拍摄的影像资料。

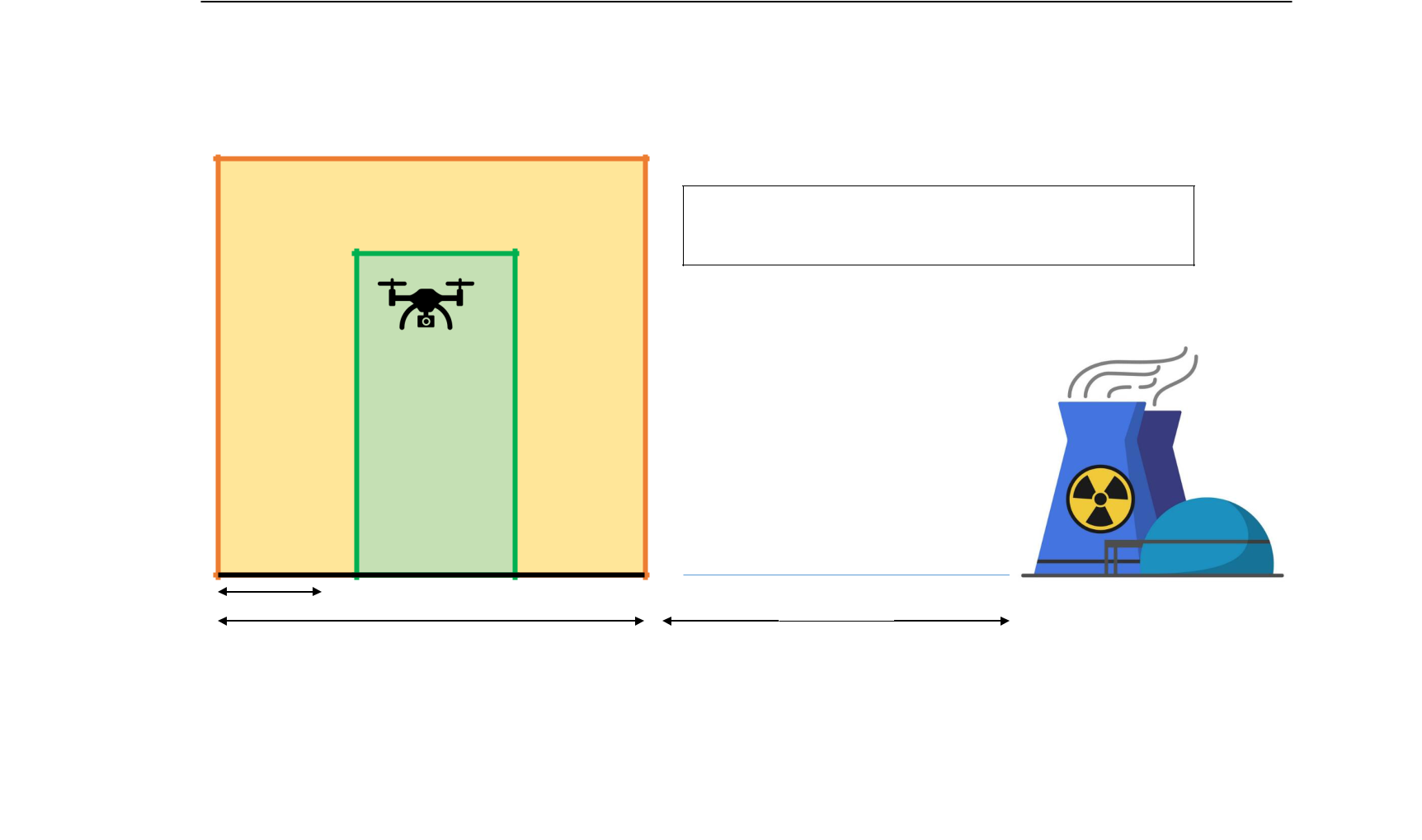
控制和指挥摄像机。

通过定义每个成员的具体权利，我们满足了 OCSO # 2。

5.4.3.2操作程序描述

操作程序包括由飞行员执行的逐步任务，以便对不同情况作出有效反应。操作程序包括正常情况、应急情况和紧急情况。这些情况是根据空域来区分的

102第五章扩展的 SORA 方法论的例证



|  |  |  |
| --- | --- | --- |
| 应变计划 | 业务量 |  |
| 音量 |  |

= 意外事故卷 + 飞行地理

航班

地理

10米

30米200米

图5.4: 运行量

飞机所定位的体积。我们在空间和时间上将操作容量分为两个空域容量: 飞行地理区域和应急容量，如图5.4所示。飞行地理是飞机正常运行和正常程序应用的空域体积。在这种操作中，飞行地理是一条10米宽的走廊，沿着预先确定的轨道飞行。这意味着在这次行动中，我们接受5米的飞机位置公差。应急容量是指飞行地理区域之外的空域容量，我们认为此次行动处于异常情况，但仍在控制之下。当行动处于异常状态时，飞行员应遵循应急程序恢复行动在控制之下。如果飞机超出了应急容量，则被认为是失去控制或处于紧急情况下。当操作失控时，飞行员应遵循紧急程序，以限制不断升级的影响。操作程序的细节如下。

正常飞行程序

当无人机按照操作员的意图正常运作时，就会有正常的程序。飞机自动飞行，飞行员只需要在地面站观察飞行

应急程序

当飞机运行异常，飞出飞行地理区域时，我们启动应急程序，进入应急卷。我们认为

5.4利用扩展的 SORA 方法进行系统开发103

操作区域是空的(没有人，没有建筑物，没有设施等)。.)并且受到保护。因此，当飞机飞出飞行地理区域时，我们打算取消飞行，并尽快将飞机降落在操作区域内。因为如果飞机继续飞行的话，它可能会飞出操作容量并在工厂坠毁。它应该自动进入着陆模式，让飞行员暖和起来。这个要求可以通过一个地理围栏解决方案来满足(限制飞行在确定的边界内)。假设飞机在着陆过程中仍然倾向于超出应急容量。在这种情况下，主要的飞行员接管手动控制飞机并将其降落在操作容积内。在这种情况下，无人机应该告知飞行员可能的原因。应考虑以下原因:

导航数据退化(来自 gps，IMUs) : 在这种情况下，导航数据不够精确，以保持飞机跟踪预定的轨道，但足够精确，以保持飞机飞行。

机械部件(马达、叶片、机身)的退化。

电池耗尽

通讯中断: 在这种情况下，飞行员无法识别情况，无法控制飞机。飞机应该进入着陆模式并自动着陆。

恶劣天气条件。

紧急程序

当飞机超出应急容量时，我们认为操作已经失控。这需要飞行终止。地理防护装置应该关闭所有的发动机，让飞机自动下降。如果自动飞行终止失败，主要飞行员应手动启动飞行终止。第二驾驶员应该在紧急情况下向管理人员和地面上的人员提供温暖。

飞机起飞后

在这个阶段，飞行员寻找飞机行为和通信链路的任何异常(例如，包裹掉包率，包裹失效，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，飞机的微小振动可能表明 GPS 退化或者 IMU 可能受到攻击。飞行员可能很难在飞行过程中立即发现这个问题。然而，通过观察和分析整个数据，飞行员可以很容易地在飞行后阶段识别振动。任何异常情况都必须记录下来，记录下来，并向制造商报告。飞行后程序使我们能够满足 OCSO # 06、 OCSO # 10和 OCSO # 14中提到的与飞行后分析中的异常检测有关的目标。

104第5章扩展的 SORA 方法的说明

5.4.4系统描述

通过分析定义的网络安全目标和操作描述，我们提出了一个 UAS 体系结构，如图5.5所示。在本节的剩余部分，我们将解释为什么我们选择这个系统。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 电源板 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | I2C | |  |  |  | 指标显示 |  |  |
|  |  |  | USB 接口 |  |  | 主频道 |  | Com 1 | | UART | | | 自动驾驶仪 | | | | | PWM | |  |  |  | 模块 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | GCS-PC1 |  | Com 1 |  | 加密数据 |  |  |  |  |  |  |  | ESC x4 |  |  |
|  |  |  |  |  | 遥测数据, | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 遥测数据, |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 冗余通道 |  |  |  | Com 的性能 | | |  |  |  |  |  |  |  |  |  |  | 导航 |  |  |
|  |  | Com 的性能 | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | (Mavlink v2) | | | |  |  |  |  |  |  |  |  |  | 照相机 |  |  |
|  |  |  | (Mavlink v2(\*)) | | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | I2C |  |  | UART | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | IMU x3 | |  |  | GPS | |  |  |  |  |  | GPS |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | 接收器 | | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 天线 x3 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | X 3 | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | RBG | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 照相机 | |  |  |  |  |  |  |  |  |  |
|  |  |  | 以太网 | Com 2 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | GCS-PC2 |  |  |  |  |  |  | Com 2 |  |  |  |  | Gimbal 万向节 | |  |  |  |  |  |  |  |  |  |
|  |  | 视频数据 |  | 加密数据 |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 热能 | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | 照相机 | |  |  |  |  |  |  |  |  |  |
|  | 地面站 | | | | |  |  |  |  |  |  |  |  |  | 飞机 | | | | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

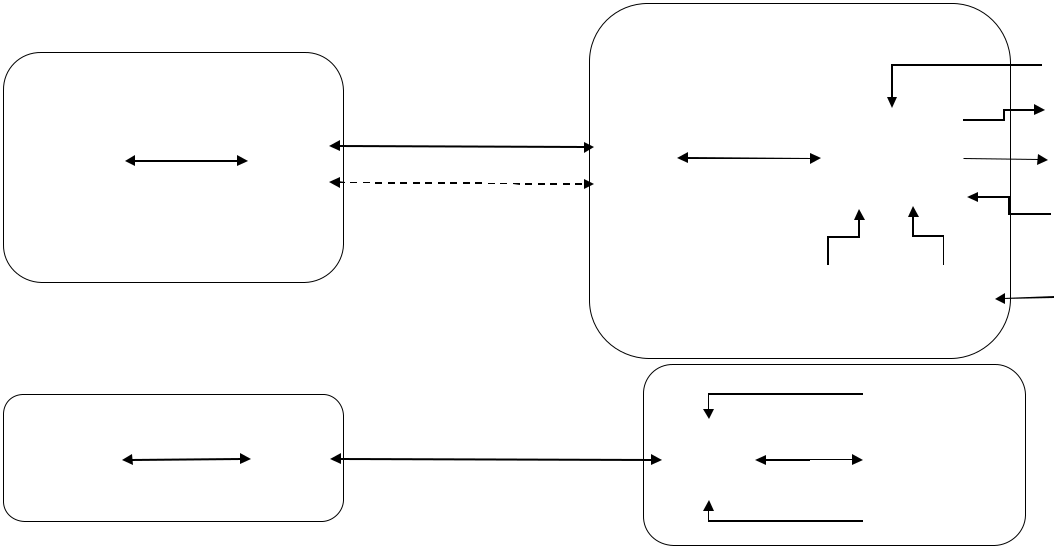


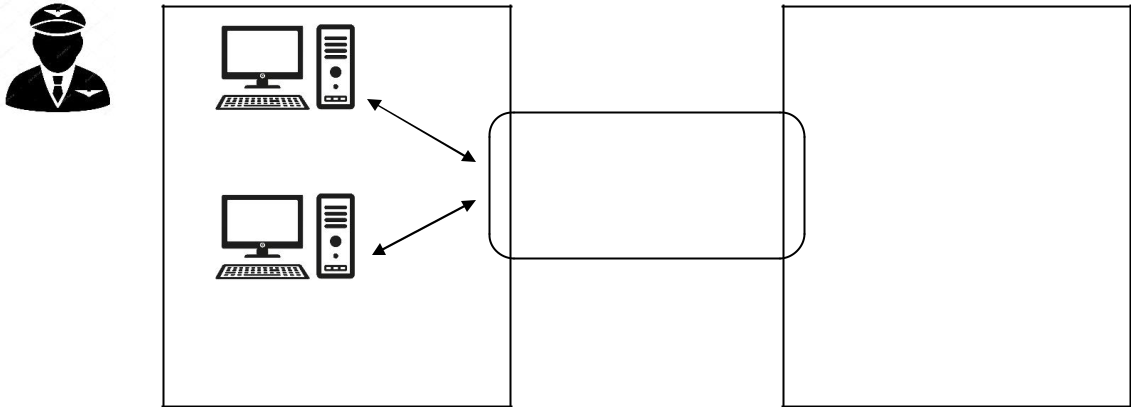
图5.5: 系统架构

5.4.4.1地面站

地面站为飞行员提供了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。为了确保飞行员只能执行为他们的角色定义的行动(OCSO # 03) ，地面站应该为他们提供不同的接口。将会有两个独立的接口。我们称之为主导航接口和次导航接口。主驾驶员界面允许主驾驶员识别飞行状态(位置、高度、姿态、电池状态)。这个界面还允许主要的飞行员操纵不同的屏幕按钮: Arm (启动) ，Disarm (停止发动机) ，起飞，着陆，回家，自动防故障。当飞行员点击这些按钮时，相关的命令就会发送到飞机上。第二个界面显示摄像机的视频、飞行器的位置、地理图和摄像机的方向。副驾驶员可以通过操纵杆控制摄像机的移动。

初级飞行员接口和次级飞行员接口为飞行员提供了不同临界级别的功能。主驾驶员界面提供了控制和指挥飞机的功能，这对操作的安全至关重要。与此同时

5.4利用扩展的 SORA 方法进行系统开发105



|  |  |
| --- | --- |
| 主驾驶员 | GCS-PC1 |

沟通



|  |  |  |
| --- | --- | --- |
| 二级飞行员 | GCS-PC2 |  |
|  |  |

地面站

飞机

图5.6: 地面站

二级飞行员接口几乎与控制、指挥摄像机的功能有关。这些功能被认为是实现操作目标(监控工业现场)必不可少的，但对于飞行来说并不重要。例如，假设对手操作延迟了次级飞行员界面。在这种情况下，飞行仍然可以控制，而不会对飞行器和工厂造成任何重大影响。因此，根据 OCSO # 07(软件/硬件分区) ，我们将 Ground Control 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)和相关软件来控制和指挥飞机(主要-飞行员界面)。第二部分由另一台计算机和相关软件组成，用于控制和指挥相机(二级飞行员接口)。GCS-PCs 的使用应该严格限于指定的飞行员，以避免误用或破坏。为此，GCS-PCs 应识别和认证试图访问的用户，如 OCSO # 01(用户识别和认证)所述。飞行员将被提示提供他们的飞行员帐户信息，包括访问 GCS-PCs 时的帐户 id 和密码。正如5.4.3.1中提到的，运营经理将管理飞行员帐户。因此，我们建议两个 GCS-PCs 都为操作经理提供一个特定的接口来创建、修改或删除试点帐户。这个接口只能通过管理员帐户访问。

为了支持飞行后分析(见5.4.3.2) ，GCS-PC1应记录和存储飞机的飞行信息，GCS-PC2应记录飞行过程中摄像机捕捉到的视频。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 SHA-224、 SHA-256、 SHA-384等密码哈希算法来保护数据的完整性，使用 AES-128、 AES-256等加密算法来保护数据的机密性。

5.4.4.2飞机段

自动驾驶仪

106 Chapter 5扩展的 SORA 方法的插图

在正常情况下，飞机将自动飞行没有飞行员的互动。自动驾驶仪将按照预定的轨迹导航飞机。重复飞行轨迹，并且不改变所有飞行的机身。因此，我们可以将飞行计划、操作音量边界(在5.4.3.2中提到)和飞行控制参数嵌入到自动驾驶仪固件中(对于某些商用自动驾驶仪，这些参数可以调整并存储在闪存中)。这有助于防止对手非法访问和修改这些参数。这个配置符合 OCSO # 04和 OCSO # 05(数据完整性和保密性保护)。为了给出更高的保护级别，我们还可以考虑保护固件完整性的机制，例如[206]-[208]中提到的那些机制。

正如在飞行后程序中提到的(见5.4.3.2) ，飞行员在每次飞行后进行飞行后分析。对于这一活动，自动驾驶仪应该记录并存储飞行信息，将其作为加密数据，并附带一个加密散列。这有助于保护数据的机密性和数据完整性(按照 OCSO # 04和 OCSO # 05的要求)

IMU 和 GPS

IMU (加速度计、陀螺仪和罗盘)和 GPS 接收器是为自动驾驶仪提供导航数据的重要传感器。如 OCSO # 15所述，传感器冗余应该就位。冗余有两种形式: 组件冗余和数据冗余。组件冗余提供了三倍 IMU 和三倍 GPS 接收器。如果其中一个 gps (或 IMUs)发生故障，自动驾驶仪应根据剩余的 gps (或 IMUs)发现故障，并向地面站发出警报。为了实现数据冗余，飞机将配备一个嵌入式摄像机模块，该模块除了 gps 和 IMUs 外，还提供第三个导航数据源。自动驾驶仪将检测三个数据源中是否有一个不可靠。这些冗余使得通过传感器(特别是 GPS 欺骗)进行攻击更加困难。

有效载荷

这架飞机配备了一个摄像机模块，包括一个 RGB 摄像机，一个热成像摄像机来拍摄监控现场，一个万向节来稳定和控制摄像机的方向。正如在5.4.4.1中提到的，我们认为与视频记录相关的功能不如与飞行相关的功能重要。根据 OCSO # 07(软件/硬件划分) ，相机模块应该独立于自动驾驶仪。

5.4.4.3通讯段

通信系统应确保地面控制部分和飞机部分之间的数据流。传输数据有两种: GCS 和自动驾驶仪之间的遥测数据(飞行状态和飞行员指挥) ; GCS 和自动驾驶仪之间的摄像头数据

|  |  |
| --- | --- |
| 5.5. 结论 | 107 |

相机模块。根据 OCSO # 08和 OCSO # 09，加密方案应该到位，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因其不同的性能要求而有所不同。对于遥测数据，低延迟传输是必要的，但低带宽是可以接受的。而对于摄像头数据，低传输延迟不是严格要求，但高带宽是必需的。此外，我们认为遥测数据比摄像头数据对于操作的安全性更为关键。因此，根据 OCSO # 13(通信分区) ，这些数据应该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段上传输。一个频率始终处于活跃状态，另一个则在第一个频率的通信性能下降时被激活。

为了支持飞行后程序(见5.4.3.2)并满足 OCSO # 12的要求，通信链路性能应当估算并存储在 GCS-PCs 和自动驾驶仪上。我们提出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，我们对不同的无人机操作进行风险评估。第一个是“农村地区航拍”操作——一个在欧洲资助项目中得到充分记录的真实操作。另一个是“城市地区的无人机交付”和“工业现场监控”操作，我们根据市场需求建立这些操作。分析结果，我们有以下一些论据:

扩展的方法要求安全目标比原来的方法更加有力。一方面，这意味着使用扩展方法的无人机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水平，它可能需要更多的资源，并影响无人机操作的成本效益。

SORA 方法(扩展或原始版本)可以灵活地用于优化操作成本。这个论点对于运营商和制造商尤其有帮助。

SORA 方法(扩展版或原始版本)目前不适用于与工业区有关的操作。我们引入了一个简单的解决方案来评估

108 Chapter 5第五章扩展 SORA 方法的实例

并改进 SORA 方法，为此类作业解决了这一问题。

除了用我们提出的方法论来说明风险评估之外，本章还定位了评估结果在开发过程中的使用。我们建议在将客户需求转换为系统描述时，使用这个风险评估来考虑网络安全(也是安全)方面。基于客户的需求，我们首先建立操作描述，然后系统描述符合已定义的网络安全目标。我们用案例研究“工业现场监控”来证明这个建议。记住，这个建议并不是为了引入一个完整的开发过程。它只是一个将网络安全整合到开发过程中的想法。

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。网络安全问题是妨碍公众接受无人机应用的问题之一。在这项工作中，我们致力于为 UASs 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，风险评估应该被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(第三章)。风险管理是一个比风险评估更大的术语。除了风险评估，风险管理还包括其他活动: 背景建立，治疗，以及可能的利益相关者之间的沟通活动。但是我们方法论的焦点是风险评估。在这种方法中，风险评估包括风险识别和风险分析/评估。一般来说，风险识别并不侧重于识别无人机的新型攻击。但它关注的是列出针对所考虑的无人机的可能攻击，并将它们呈现在攻击树图上。风险分析/评估旨在根据攻击的难度和影响来评估攻击的严重性。评估有助于确定应该首先考虑或处理的攻击，以及应该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，并建立一个无人机的网络安全需求。该方法的应用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率。我们可以在 UAS 架构定义好之后，在开发过程中实现之前，使用这种方法。这种方法的弱点是成本效益。实现由此产生的网络安全需求可能需要大幅度修改系统架构; 这可能是昂贵的。

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 方法最初是一种致力于操作安全的风险评估方法。最初的方法论考虑了一组安全风险，这是由一个蝴蝶结模型建模的。这个模型包括威胁，危害，危害和障碍。最初的方法论只关注安全; 因此，它只考虑意外或“非故意”威胁和危害人类生命。使用提供的评估表，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领域，我们首先扩展了风险模型，包括三个新的“故意”威胁和隐私伤害。然后，我们引入了我们的评估机制，它符合

109

110全球结论和展望

原始方法论的哲学。基于这种机制，用户可以评估风险，确定安全和网络安全目标。我们提出的策略可以用来扩展方法论，以涵盖其他未知的威胁和其他危害。最初的方法主要设计用于行政过程中的无人机操作验证，而不是用于开发过程。因此，我们引入我们的方法来将扩展的 SORA 评估集成到开发过程中。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)很容易进行风险评估(特别是使用我们的基于 web 的工具) ; (2)在系统架构设计之前就考虑网络安全问题。然而，它也有一个弱点。这种方法只考虑了风险模型中提出的一组有限的风险以及所提供的列表中列出的目标。因此，很难考虑到每天都在发展的新的攻击技术。

透视图

作为我们工作的视角，我们考虑以下作品:

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危害。因此，它不适用于与基础设施或工业场所相关的无人机操作，在这些场所，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，我们提出了一个简单的解决方案。然而，它应该被认为是一个临时的解决方案。未来需要更深入地分析这种运作，创造一种新的危害(如“工业基础设施损害”)。



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 扩展 |  | 系统 |  |
|  |  | 网络安全风险 |  |
|  | SORA 网站 |  |  |
|  |  | 管理层 |  |
|  |  |  |  |
| 客户的 |  | 系统 | 实施 |  |
| 规定 |  | 描述 |  |
|  |  |  |



图5.7: 开发过程中的两种拟议方法

结合开发过程中提出的方法: 我们提出了两种不同的方法。一种可以在开发过程的早期使用，但是它还没有发展到考虑新的攻击技术的程度。另一种可以在开发过程中晚些时候使用，并且足够灵活以考虑新的攻击(取决于用户的专业知识)。因此，我们可以在同一个开发过程中使用这两种方法-逻辑，如图5.7所示。这允许我们采用

|  |  |
| --- | --- |
| 全球结论和展望 | 111 |

考虑到网络安全方面，以及发展过程。目前，我们没有验证这一想法。

基于 web 的工具: 目前，我们只有一个基于 web 的扩展 SORA 方法的工具。在未来，它需要开发另一种方法学的工具。

反馈: 我们用一些案例研究来测试和评估我们提出的方法。然而，为了得到客观的评价和改进我们的工作，这些方法应该被传播，测试，并由工业专家评论。

附录 a

网络安全运作目标

113

**OCSOs 与攻击软件/硬件架构有关**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 描述 | |  |  |  |  |  | 诚信水平 | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 很低 |  | 中等 | |  | 很高 | |  |
|  | | | | |  |  |  |  |  |  | |  |
| OCSO # 1软件/硬件 | | | | | 可选项 |  | - 定义识别的过程/机制 |  |  | ー与媒体相同 |  |  |
| 识别 | 然后确认 | | | 是的 |  |  | 并验证试图访问的人的身份 |  |  |  |  |  |
|  |  | 进入 GCS 和自动驾驶仪。 |  |  |  |  |  |
| 实体(\*)试图访问 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 和自动驾驶仪 | | |  |  |  |  | - 界定工序/机制，以便 |  |  |  |  |  |
| 关键词: | 身份证明 | | | 及 |  |  | 创建/修改/删除某人的身份证 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 身份验证 | |  |  |  |  |  | 这些活动应符合 OSO # 02, |  |  |  |  |  |
|  |  |  |  |  |  |  | 要求界定职责和 |  |  |  |  |  |
|  |  |  |  |  |  |  | 操作人员的责任 |  |  |  |  |  |
| 注意: 实体可以是 | | | | |  |  |  |  |  |  |  |  |
|  | 例子 | | |  |  |  |  |
| 人类, | 或者 | *a* | 组件 | |  |  |  |  |  |
| (硬件/软件) | | |  |  |  | - 密码用于核实用户身分 | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 当有人试图进入 | | |  |  |  |  |
|  |  |  |  |  |  | 自动驾驶 | | |  |  |  |  |
|  | | | | |  |  | | |  | | |  |
| OCSO # 2 \_ 软件/硬件 | | | | | 可选项 |  | - 界定每个人的权利 |  |  | ー与媒体相同 |  |  |
| 管理 | 是的 | | 实体的 | |  |  | 组织，这些组织可以与 |  |  |  |  |  |
|  |  | 自动驾驶仪和昏迷指数。 |  |  |  |  |  |
| 授权。 | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | - 界定以下程序/机制: |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 分配/修改/撤销每个 |  |  |  |  |  |
| 关键词: |  | 授权 | | |  |  | 人。 |  |  |  |  |  |
| 管理层 | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 例子 | | |  |  |  |  |
| 注1: 这个目标集中在 | | | | |  | 定义了每个人的授权 | | |  |  |  |  |
|  | 如下: | | |  |  |  |  |
| 可操作的 | | 程序 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 定义/分配/ | | 修改/撤销 | | |  | 经理 | | |  |  |  |  |
| 实体的授权。 | | | |  |  | - 飞行员可以进入地面控制系统进行监测 | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 控制车辆。 | | |  |  |  |  |
|  |  |  |  |  |  | 维修人员可以使用自动驾驶仪 | | |  |  |  |  |
| 注2: 实体可以是 | | | | |  | 并在飞行后和飞行前下载数据。 | | |  |  |  |  |
|  |  |  |  |  |  |  |  |
| 人类, | 或者 | *a* | 组件 | |  | 为了拥有赡养费的权利 | | |  |  |  |  |
| (硬件/软件) | | |  |  |  | 员工，一个人必须向经理要求 | | |  |  |  |  |
|  |  |  |  |  |  | 这些权利。 | | |  |  |  |  |
|  | | | | |  |  | | |  | | |  |
| OCSO # 3 \_ 软件/硬件 | | | | | 可选项 |  | - 界定程序/机制，以限制 |  |  | ー与媒体相同 |  |  |
| 每个实体(\*)访问 | | | | |  |  | 一个人可以作为自己的行为进行的行为 |  |  | 此外 |  |  |
|  |  | 分配的权利。 |  |  |  |  |
| GCS 或自动驾驶仪，确保它 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  | ー界定程序/机制以限制 |  |  |
| 只能执行 | | | |  |  |  | - 这些活动应符合 OSO # 02, |  |  |  |  |
|  |  |  |  |  | 其他组件的动作 |  |  |
| 授权行为。 | | |  |  |  |  | 要求界定职责和 |  |  |  |  |
|  |  |  |  |  |  | 可以履行的权利 |  |  |
| 关键词: 访问控制 | | | |  |  |  | 操作人员的责任 |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| 注意: 实体可以是 | | | | |  | 例子 | | | 例子 | | |  |
| 人类, | 或者 | *a* | 组件 | |  | - 视乎使用者的角色而定 | | | ー自动驾驶仪的连接端口 | | |  |
| (硬件/软件) | | |  |  |  |  |
|  |  |  | 可以提供一个特定的人机 | | | 允许 GPS 模块发送位置 | | |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  | 接口，让用户执行 | | | 自动驾驶仪的数据，但不包括其他 | | |  |
|  |  |  |  |  |  | 授权行动 | | | 各种数据 | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| OCSO # 4软件/硬件 | | | | |  | 可选项 |  |  | - 界定保安机制，以保护 |  |  | ー与媒体相同 |  |  |
| 检测未经授权的实体(\*) | | | | |  |  |  |  | 飞行计划的完整性，飞行 |  |  | 此外 |  |  |
|  |  |  |  | 参数(PID 参数，滤波器卡尔曼 |  |  |  |  |
| 来自 | 修改 | | 是的 | 资料/ |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 参数、传感器校正等)及 |  |  | - 界定保护的安全机制 |  |  |
| 信息储存在 GCS 和 | | | | |  |  |  |  |  |  |  |  |
|  |  |  |  | 记录的数据(视频数据、日志数据)储存在 |  |  | 源代码的完整性 |  |  |
| 自动驾驶仪。 | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | GCS 和自动驾驶仪。 |  |  | 自动驾驶仪和昏迷指数 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| 关键词: 诚信 | | | |  |  |  |  |  |  |  |  |  |  |  |
| 注1: 这个目标是指 | | | | |  |  |  |  |  |  |  |  |  |  |
| 保障的情况 | | | | |  |  |  |  |  |  |  |  |  |  |
| OCSO # 3中定义的机制 | | | | |  |  |  |  |  |  |  |  |  |  |
| 被绕过 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 注2: 实体可以是 | | | | |  |  |  |  |  |  |  |  |  |  |
| 人类, | 或者 | *a* | 组件 | |  |  |  |  |  |  |  |  |  |  |
| (硬件/软件) | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 例子 | | | 例子 | | |  |
|  |  |  |  |  |  |  |  | - 自动驾驶仪和 GCS 产生一个 | | | - 自动驾驶仪可以检查 | | |  |
|  |  |  |  |  |  |  |  | 加密哈希，以保护 | | | 软件在启动时的完整性 | | |  |
|  |  |  |  |  |  |  |  | 飞行计划。 | | |  |  |  |  |
|  | | | | |  | | |  | | |  | | |  |
| OCSO # 5 \_ 软件/硬件 | | | | |  | 可选项 |  |  | - 界定保安机制，以保护 |  |  | ー与媒体相同 |  |  |
| 预防 | 未经授权的 | | | 实体 |  |  |  |  | 存储的数据/信息的保密性 |  |  |  |  |  |
|  |  |  |  | 还有自动驾驶仪 |  |  |  |  |  |
| (\*)进入 | | | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 数据/资料 | |  | 储存 | 在 |  |  |  | 例子 | | |  |  |  |  |
| 昏迷指数和自动驾驶。 | | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 关键词: 保密 | | | | |  |  |  | - AES 算法是用来保护 | | |  |  |  |  |
|  |  |  | 飞行计划的机密性 | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
| 注1: 这个目标是指 | | | | |  |  |  |  |  |  |  |  |  |  |
| 保障的情况 | | | | |  |  |  |  |  |  |  |  |  |  |
| OCSO # 3中定义的机制 | | | | |  |  |  |  |  |  |  |  |  |  |
| 被绕过 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 注2: 实体可以是 | | | | |  |  |  |  |  |  |  |  |  |  |
| 人类, | 或者 | *a* | 组件 | |  |  |  |  |  |  |  |  |  |  |
| (硬件/软件) | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | | | | |  | | |  | | |  | | |  |
| OCSO # 6软件/硬件 | | | | |  | 分析异常行为 |  |  | 和 Low 一样 |  |  | 和 Low 一样 |  |  |
| 分析异常行为 | | | | |  | 软件/硬件 |  |  |  |  |  |  |  |  |
|  | 检测异常行为 |  |  |  |  |  |  |  |  |
| 飞机起飞后的软件/硬件 | | | | |  |  |  |  |  |  |  |  |  |
|  | 飞行检查。 |  |  |  |  |  |  |  |  |
| (飞行后检查) | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| 关键词: 异常检测 | | | | |  | 注意: 此活动应与 |  |  |  |  |  |  |  |  |
|  | SORA 方法论的 OSO # 6, |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 这就需要定义飞行后 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 检查程序。 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 例子 | | |  |  |  |  |  |  |  |
|  |  |  |  |  | ー飞行结束后，飞行员应分析 | | |  |  |  |  |  |  |  |
|  |  |  |  |  | 飞行数据和飞行指令 | | |  |  |  |  |  |  |  |
|  |  |  |  |  | 飞行中的记录。 | | |  |  |  |  |  |  |  |
|  |  |  |  |  | - 为配合上述活动, | | |  |  |  |  |  |  |  |
|  |  |  |  |  | 自动驾驶仪及地面监察系统须记录数据 | | |  |  |  |  |  |  |  |
|  |  |  |  |  | 在飞行过程中发生的事件。 | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| OCSO # 7软件/硬件 | | | 可选项 |  | - 软件/硬件的划分 |  | ー与媒体相同 |  |
| 分区 | 的 | 是的 |  |  | 建筑物分成不同的「区域」 |  |  |  |
|  |  | 不同等级的临界性 |  |  |  |
| 软件/硬件架构 | | |  |  |  |  |  |
|  |  | 硬件/软件可能易受 |  |  |  |
| 进入不同的”区域” | | 和 |  |  |  |  |  |
|  |  | 网络攻击，但他们提供 |  |  |  |
| 不同程度的临界性。 | |  |  |  |  |  |  |
|  |  |  | 功能不如其他的那么重要。 |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| 关键词: | 硬件/软件 | | . | 例子 | | |  |  |
|  |  |  |  |  |  |
| 隔板 |  |  |  | - GCS 包括两个不同的2个电脑 | | |  |  |
|  |  |  |  | 一台个人电脑用于控制和 | | |  |  |
|  |  |  |  | 观察飞行器。这台电脑对于飞行器是至关重要的 | | |  |  |
|  |  |  |  | 另一个是用来控制 | | |  |  |
|  |  |  |  | 这个功能不那么重要。 | | |  |  |
|  |  |  |  |  |  |  |  |  |

**法律事务厅与攻击通信有关:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 描述 | | |  |  |  |  |  |  |  | 水平 |  |  |  |  |
|  |  |  |  |  |  |  | 正直 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 很低 | |  | 中等 |  | 很高 | |  |
|  | | | | |  |  | |  |  |  |  |  | |  |
| OCSO # 8沟通 | | | | |  |  | - 界定机制，以确保 |  | 和 Low 一样 |  |  | 和 Low 一样 |  |  |
| 预防 | a | 未经授权 | | 实体 | |  | 传送的每个数据的保密性 |  |  |  |  | 此外 |  |  |
|  | 通过通讯设备。 |  |  |  |  |  |  |
| (\*)由 | | 进入 | |  | 是的 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | - 界定机制，以确保 |  |  |
| 数据/资料 | | | 内心 |  | 是的 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 每条讯息的保密性 |  |  |
| GCS 之间的通信 | | | | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 在 GCS 软件之间传输 |  |  |
| 和飞机 | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 还有自动驾驶软件。 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 关键词: 保密 | | | |  |  |  |  |  |  |  |  | (申请级别) |  |  |
|  |  |  |  |  |  |  | |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 例子 | | |  |  | 例子 | | |  |
| 注意: | 安 | 实体 | 可以 | 可能 | *a* | - 在一个简单的情况下，GCS 和自动驾驶仪 | | |  |  | - GCS 软件和自动驾驶仪 | | |  |
| 人类, |  | 欧拉 | 组件 | | |  |  |  |
|  | 通过一对无线电通信 | | |  |  | 软件有自己的机制 | | |  |
| (硬件/软件) | | | |  |  |  |  |  |
|  |  | 数据的保密性是 | | |  |  | 的保密性 | | |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 基于加密的保护 | | |  |  | 在他们之间传输的信息。 | | |  |
|  |  |  |  |  |  | 算法和跳频 | | |  |  |  |  |  |  |
|  |  |  |  |  |  | 这个模块提供的机制。 | | |  |  |  |  |  |  |
|  | | | | |  |  | | |  |  |  | | |  |
| OCSO # 9\_ 沟通 | | | | |  |  | - 界定机制，以确保 |  | 和”低”一样 |  |  | 和 Low 一样 |  |  |
|  |  |  |  |  |  |  | 每个数据包/讯息的完整性 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 描述 | |  |  |  |  |  |  |  | 水平 | |  |  |  |  |
|  |  |  |  |  |  | 正直 | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 很低 | |  | 中等 | |  | 很高 | |  |
|  | | | | |  | |  |  |  |  |  |  | |  |
| 防止未经授权的实体 | | | | |  | 通过通讯传送 |  |  |  |  |  | 此外 |  |  |
| 来自 | 修改 | |  | 是的 |  | 设备。 |  |  |  |  |  | - 界定机制，以确保 |  |  |
| 数据/资料 | | 内心 | | 是的 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 发送的每条消息的完整性 |  |  |
| GCS 之间的通信 | | | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 在 GCS 软件和 |  |  |
| 和飞机 | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 自动驾驶软件。(通信 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 关键词: 诚信 | | |  |  |  |  |  |  |  |  |  | 之间的申请) |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 例子 | | |  |  |  | 例子 | | |  |
| 注意: 这是为了确保数据 | | | | | - 在一个简单的情况下，GCS 和自动驾驶仪 | | |  |  |  | - GCS 软件和自动驾驶仪 | | |  |
| 没有根据。。的条款修改 | | | | |  |  |  |  |
| 通过一对无线电通信 | | |  |  |  | 软件有自己的机制 | | |  |
| 内容, | 时间 | (防止重播 | | |  |  |  |  |
| 数据的完整性是 | | |  |  |  | 保护信息的机密性 | | |  |
| 攻击)和来源。 | | |  |  |  |  |  |  |
|  |  | 基于加密的保护 | | |  |  |  | 在他们之间传播。 | | |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 这个模块提供的算法。 | | |  |  |  |  |  |  |  |
|  | | | | |  | | |  | | |  | | |  |
| OCSO # 10 \_ 传播 | | | | |  | 定义用于测量 |  |  | 和 Low 一样 |  |  | 和 Low 一样 |  |  |
| 侦测 | 异常现象 | | 进去 | 是的 |  | 通信信道的性能。 |  |  |  |  |  | 此外 |  |  |
|  |  |  |  |  |  |  |  |  |
| 通讯 | |  | 频道 | |  | - GCS 显示定义的 |  |  |  |  |  | - 定义检测机制 |  |  |
| 在地面控制系统和飞机之间 | | | | |  | 参数 |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 异常情况自动出现 |  |  |
| 异常情况 | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | - 建立保安指示，确保 |  |  |  |  |  | 通讯渠道 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| 关键词: 异常点检测 | | | | |  | 飞行员可以用来探测降落 |  |  |  |  |  | 在这个水平上，异常指的是 |  |  |
|  |  |  |  |  |  | 沟通渠道的表现 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 通讯性能下降 |  |  |
|  |  |  |  |  |  | 通过观察沟通渠道 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 以及讯息/资料包的内容 |  |  |
|  |  |  |  |  |  | 状态。 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 通过通讯传送 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 在低层次上，异常指的是 |  |  |  |  |  | 频道。 |  |  |
|  |  |  |  |  |  | 只有沟通的减少 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 表演。 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 这些活动应该与 OSO 保持一致 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | # 6，要求操作员识别 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 通信特征 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | | |  |
|  |  |  |  |  | 例子 | | |  |  |  | 例子 | | |  |
|  |  |  |  |  | 用于计算 | | |  |  |  | ー使用防火墙，以防 | | |  |
|  |  |  |  |  | 通信质量是信号 | | |  |  |  | 无人机的通信是基于 | | |  |
|  |  |  |  |  | 强度、丢包率和比特率。 | | |  |  |  | 复杂的网络，用于 | | |  |
|  |  |  |  |  | 这些参数将显示给 | | |  |  |  | 其他应用程序、操作或 | | |  |
|  |  |  |  |  | 飞行员。 | | |  |  |  | 系统 | | |  |
|  | | | | |  | | |  | | |  | | |  |
| OCSO # 11\_ 沟通 | | | | |  | 一个计划或程序，允许 |  | - 界定机制，以重新建立 | |  |  | ー与媒体相同 |  |  |
| 保持 | a | | 最少 | |  | 用户、引航员、重建 |  |  | 沟通或保持几个基本的 |  |  |  |  |  |
|  | 沟通或保持几个 |  |  | 服务，以防通讯中断 |  |  |  |  |  |
| 沟通表现 | | | |  |  |  |  |  |  |  |  |  |
|  |  | 基本服务，以防认识到 |  |  | 表演。 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
| 关键词: 可用性 | | |  |  |  | 沟通能力的下降。 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 例子 | | | 例子 | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 以防通讯中断 | | | 以防通讯中断 | | |  |  |  |  |
|  |  |  |  |  | 的表现，飞行员应该改变 | | | 性能，通信模块 | | |  |  |  |  |
|  |  |  |  |  | 通信频率。 | | | 传递重要信息 | | |  |  |  |  |
|  |  |  |  |  |  |  |  | 信息/信息包(如位置、态度等) | | |  |  |  |  |
|  |  |  |  |  |  |  |  | 信息和飞行员指挥 | | |  |  |  |  |
|  |  |  |  |  |  |  |  | 信息)的优先级。 | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |



|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 描述 |  |  |  |  |  |  |  | 水平 |  |  |  |  |
|  |  |  |  |  | 正直 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 很低 | |  | 中等 |  | 很高 |  |  |
|  | |  |  |  | |  |  |  |  |  |  |  |
| OCSO # 12\_ 沟通 | |  |  |  | 定义用于诊断 |  |  | 和 Low 一样 |  | 和 Low 一样 |  |  |
| 分析 | 异常现象 | 进去 | |  | 沟通渠道的表现 |  |  |  |  |  |  |  |
|  | 这些参数将会 |  |  |  |  |  |  |  |
| 后的通信渠道 | | | |  |  |  |  |  |  |  |  |
|  | 自动驾驶仪及 |  |  |  |  |  |  |  |
| (飞行后视察) | |  |  |  |  |  |  |  |  |  |  |
|  |  |  | GCS. |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | - 建立保安指示，确保 |  |  |  |  |  |  |  |
| 关键词: 异常点检测 | |  |  |  | 飞行员或维修人员可以使用 |  |  |  |  |  |  |  |
|  |  |  |  |  | 通过检查测井来检测异常情况。 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 例子 |  |  |  |  |  |  |  |  |
|  | - 自动驾驶仪和 GCS 记录了 |  |  |  |  |  |  |  |  |
|  | 参数: 包裹丢失百分比, |  |  |  |  |  |  |  |  |
|  | 信号强度，延迟时间。 |  |  |  |  |  |  |  |  |
|  | - GCS 提供了一个接口 |  |  |  |  |  |  |  |  |
|  | 容许飞行员/员工分析 |  |  |  |  |  |  |  |  |
|  | 记录数据。 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| OCSO # 13 \_ 沟通 | 可选项 |  |  | 将通信系统划分为 |  |  | 和中号一样 |  |  |
| 通信的划分 |  |  |  | 不同的渠道 |  |  |  |  |  |
|  |  |  | 的关键程度和脆弱程度 |  |  |  |  |  |
| 系统进入不同渠道。 |  |  |  |  |  |  |  |  |
|  |  |  | 传送的数据。 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
|  | 例子 |  |
| 关键词: 沟通 | - 通信系统被划分 |  |
| 分成两个通道。一个用于传输 |  |
| 隔板 |  |
| 飞行数据，这是至关重要的。另一个是 |  |
|  |  |
|  | 用于传输视频数据 |  |
|  | 不那么挑剔了。 |  |

**OCSO 与传感器攻击有关**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 描述 |  |  |  |  |  | 诚信水平 | |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  | 很低 | |  | 中等 | | 很高 |  |
|  | |  |  |  |  |  |  |  |  |
| OCSO # 14传感器 | |  | - 界定传感器的特性(约 |  |  | ー与媒体相同 |  | 和中号一样 |  |
| 侦测异常 | 行为 |  | 输出值，采样频率，噪音) |  |  | 此外 |  |  |  |
|  | 可接受的临界值 |  |  |  |  |  |
| 传感器受到攻击 | |  |  |  |  |  |  |  |
|  | 这些阈值被认为是异常的 |  |  | - 定义探测异常的机制 |  |  |  |
|  |  |  |  |  |  |  |  |
| 关键词: | 异常点 |  | 行为。 |  |  | 通过分析传感器数据的一致性 |  |  |  |
| : 检测 |  |  |  |  |  | 和数据之间的一致性 |  |  |  |
|  |  |  |  |  |  | 不同的传感器。 |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  | 例子 | | 例子 | | |  |  |
|  |  |  | - 可接受的门槛值 | | - 比较 GPS 定位数据和 | | |  |  |
|  |  |  | 加速度计，例如 +-3m/s2 | | 数据来自 IMU 和一个立体摄像机 | | |  |  |
|  |  |  | 这个范围可以被认为是一个可能的 | | 探测 GPS 欺骗 | | |  |  |
|  |  |  | 攻击。 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| OCSO # 15传感器 | |  |  | - 定义保护传感器免受 |  |  | 和 Low 一样 |  | 和中号一样 |  |
| 确保 | 可用性 | 的 |  | 来自环境的干扰 |  |  | 此外 |  |  |  |
|  | 攻击者可以操纵 |  |  |  |  |  |
| 传感器 | 的资料 | |  |  |  |  |  |  |  |
|  | 加速度计传感器使用的干扰 |  |  | - 界定机制或架构 |  |  |  |
| 攻击。 |  |  |  |  |  |  |  |  |
|  |  |  | 在其共振频率) |  |  | 提供传感器数据的冗余 |  |  |  |
|  |  |  |  |  |  |  |  |  |
| 关键词: 可用性 | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 例子 | | 例子 | | |  |  |
|  |  |  |  | 加速度计(IMU)被炮弹击中 | | - 在 GPS 不可靠的情况下, | | |  |  |
|  |  |  |  | 装在一个金属盒子里来防御 | | 来自摄像头的数据可以提供位置 | | |  |  |
|  |  |  |  | 共振频率的干扰 | | 数据交替 | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

.

附录 b

网络工具手册

一般信息页面

这是我们申请的第一步。在这一步中，用户将被提示提供一些关于预期 UAS 操作的一般信息。所提供的信息并不用于风险评估，而是帮助我们改进应用程序。一般信息包括:



图 b. 1: 一般信息页面

申请人(或用户)姓名

电子邮件

组织类型有三种选择，如下:

ー制造商，如使用者是制造商的成员。

- 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

122附录 b 网络工具手册

无人机操作目的: 无人机将用于何种目的? 例如: 观察公路、运输货物。

这个风险评估的目的。有两种选择，如下:

- 核实现有的无人机操作。在这种情况下，我们假设预期的操作已经开发完成并且有良好的文档记录。如果操作涵盖了风险评估产生的所有安全和安保目标，则认为操作是有效的。

ー发展新的无人机操作系统。在这种情况下，在风险评估的开始，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，风险评估的结果(目标)将被用来完善和完成操作描述。

要开始风险评估过程，请点击“创建新的评估”按钮。

B. 2基本风险等级(GRC)的确定

我们应用程序的这个步骤对应于 SORA 方法学的两个步骤: 内在 GRC 的确定和最终 GRC 的确定。

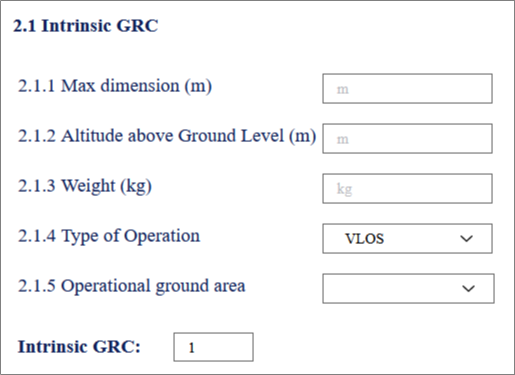


图 b. 2: 计算内在 GRC 的信息

为了确定预期操作的固有 GRC，提示用户提供以下信息:

|  |  |
| --- | --- |
| B. 2. Ground Risk Class (GRC)的确定 | 123 |

飞机的最大尺寸(单位: 米)。

飞机在运行期间的地面高度(单位米)。

飞机重量(单位: 千克)。

操作类型: 这个信息有两个选项:

- 如果飞机在飞行员的视线范围内飞行，则使用 VLOS 或 Visual Line Of Sight。

- BVLOS 或 Beyond Visual Line Of Sight，如果飞机在飞行员视线范围之外飞行。

地面作战区域，有四种情报可供选择:

控制地面区域，如果只有活跃的参与者直接参与行动的操作是。

- 人烟稀少的环境

人口稠密的环境

- 如果飞机飞过人群，人们就会聚集起来。

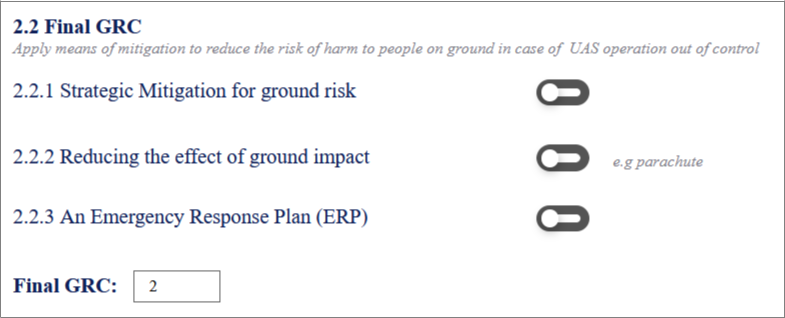


图 b. 3: 计算最终 GRC 的信息

为了确定预定操作的最终 GRC，提示用户提供信息，说明在”无人机操作失控”的情况下为减少地面上致命伤害的可能性而采取的措施。有三种潜在的缓解措施:

地面风险的战略缓解。如果无人机操作失控，这有助于降低人员进入危险区域的可能性。

减少地面撞击的影响。这有助于减少致命伤害的可能性，如果不幸的是，一个人在地面上被飞机撞击(例如，降落伞)。

紧急响应计划。应对紧急事件的行动计划按照特定的顺序或方式进行。

124附录 b 网络工具手册

如果在预期的操作中提到或考虑了缓解，用户可以通过点击/切换相应的按钮来激活所呈现的缓解。一旦缓解被激活，这个缓解的相关特征将会出现。然后用户可以选择激活预期操作中提到或考虑的特性。基于激活的特征，应用程序可以估计缓解的稳健性。

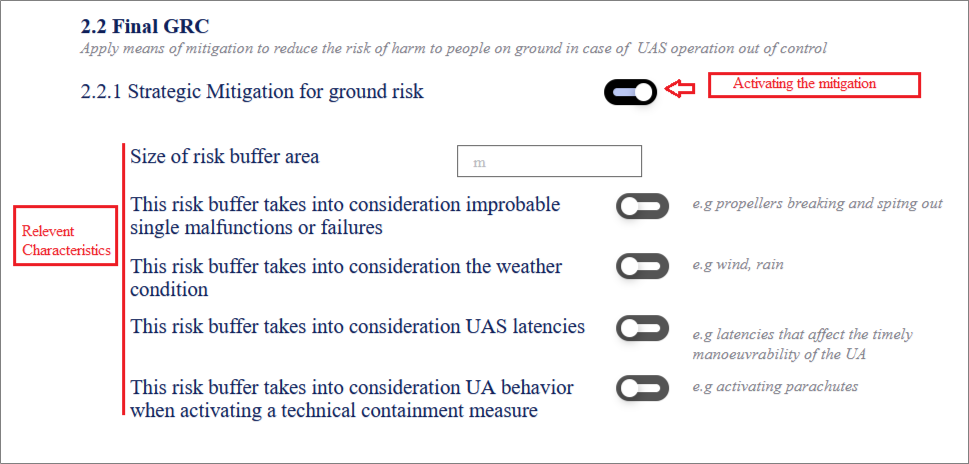


图 b. 4: 战略缓解的相关特征

对于每个激活的特性，用户可以提供更多的信息，如何相关的特性被提及或考虑在预期的操作。这些信息将用于生成最终报告，但不用于风险评估。

基于内在的 GRC 和应用缓解措施的信息，最终的 GRC 在页面底部计算。

B. 3空气风险等级(ARC)的确定

我们应用程序的这一步对应于 SORA 方法学的两个步骤: 初始 ARC 确定和最终 ARC 确定。初始 ARC 对无人机在特定空域环境中遇到载人飞机的概率进行了定性分类。假设一个申请者认为广义的初始 ARC 分配对于当地的操作容量条件来说太高了。在这种情况下，可以考虑减少初始 ARC 值。如果初始 ARC 不正确，最终 ARC 等于初始 ARC。

|  |  |  |
| --- | --- | --- |
| B. 3. 空气风险等级(ARC)的确定 | | 125 |
|  |  |  |
|  |  |  |

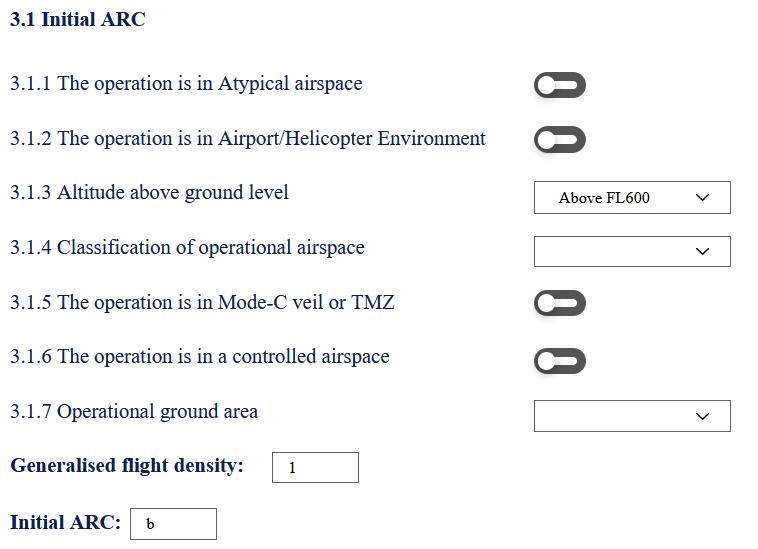


图 b. 5: 计算初始 ARC 的信息

为了确定预期操作的初始 ARC，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? 非典型空域的定义是:

ー禁区或危险区;

- 普通载人飞机无法飞行的空域(例如建筑物或结构100英尺以内的空域) ;

- 空域角色塑造，有人驾驶飞机在作业期间遭遇率可显示低于每飞行小时1E-6;

飞机是否在机场/直升机环境中飞行？

飞机在地面高度的哪个高度飞行? 有三种选择:

- 海拔600米以上(离地面约18000米)

ー高于500英尺(约150米)及海拔600米

低于500英尺

这架飞机在哪个空域飞行? 有三种选择:

126附录 b 网络工具手册

A 类或 e 类

- b 类，c 类或 d 类

- f 类或 g 类

这些类别由国家航空当局根据飞行规则以及飞机与空中交通管制(ATC)之间的相互作用来定义。它们可以因国家机关而异。

飞机是以 c 模式运行还是以 TMZ 模式运行？

飞机是否在受管制的空域飞行？

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



图 b. 6: 减少 ARC 的缓解方案

为了减少最初的 ARC，可以考虑两种类型的缓解措施。

他们是:

通过操作限制缓解

通用结构和规则的缓解

基于最初的 ARC 和应用缓解的信息，最终的 ARC 在页面底部计算。

|  |  |
| --- | --- |
| B. 4. 私隐风险级别(PRC)的确定 | 127 |

B. 4隐私风险等级(PRC)的确定

我们应用程序的这个步骤涉及到 SORA 方法的扩展版本，其中考虑了侵犯隐私的风险。

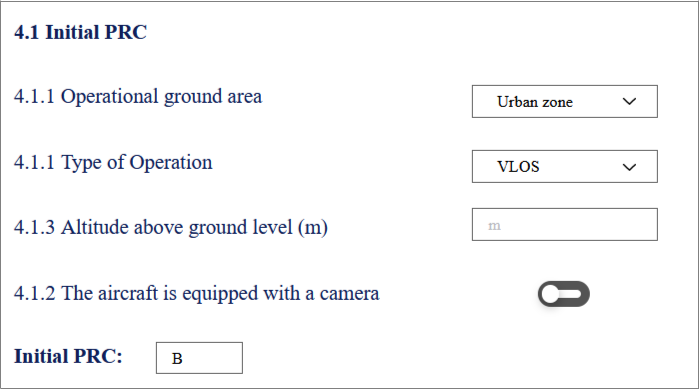


图 b. 7: 计算初始 PRC 的信息

首先，要求用户提供以下信息来计算操作的初始 PRC 值:

操作区域: 城市区域与农村区域。

操作类型: VLOS vs BVLOS

飞机是否配备了摄像头？如果是的话，打开这个选项的按钮，提供更多关于分辨率和最小视角的信息。

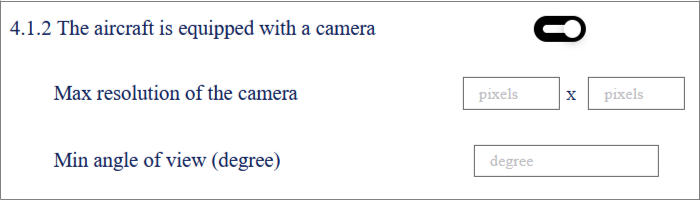


图 b. 8: 摄像机特性

128附录 b。 Web 工具手册

然后提示用户提供信息，说明在”无人机操作失控”的情况下为减少侵犯隐私的可能性而采取的措施。在这里，我们提出了三种类型的缓解措施:

隐私保护过滤器。

私人空间限制

对公众发布操作知情通告

对于每个选定的缓解措施，用户可以提供更多信息，说明在预期的操作中如何提及或考虑缓解措施。这些信息仅用于生成最终报告，而不用于风险评估。

基于内在 PRC 和应用缓解措施的信息，最终 PRC 在页面底部计算。

B. 5确定网络安全易受影响程度行动

我们应用程序的这一步涉及到我们扩展的 SORA 方法，其中网络安全威胁被考虑在内。

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，这些信息有助于评估预期操作的脆弱性。它们是:

沟通链接的性质有三种选择:

- 专用通讯链路: 地面控制站通过只用于无人机操作的通讯链路(例如射频模块)与飞机通讯

共享网络: 地面控制站通过运营商组织的内部网络与飞机进行通信。除了无人机操作，这个网络还可以为组织的其他活动提供服务。

- 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进行通信。(例如互联网连接，云服务)。

监控水平。有三种选择:

|  |  |  |
| --- | --- | --- |
| B. 5. 确定网络安全易受影响等级(OCSL)行动 | | 129 |
|  |  |  |
|  |  |  |

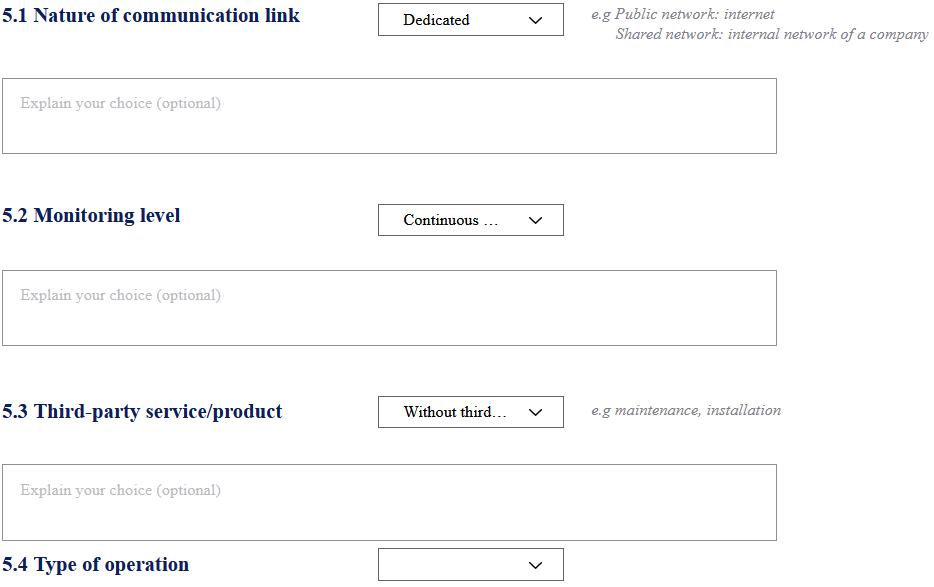


图 b. 9: 计算 OCSL 的信息

- 持续监测: 地面控制站和飞机在作业期间经常通信。数据传输是实时的或者几乎是实时的。

- 没有连续监测。地面控制站和飞机在操作过程中定期通信。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，维修服务、安装服务) :

ー没有第三者: 如果没有使用第三者服务/设备。

- 受信任的第三方: 如果只有受信任的第三方服务/设备用于无人机系统的操作。

非信任第三方: 如果非信任第三方服务/设备用于 UAS 操作。

操作类型: VLOS vs BVLOS。

根据提供的信息，OCSL 是在页面底部计算的。

130附录 b 网络工具手册

B. 6结果

本页将显示预期操作的风险评估结果。

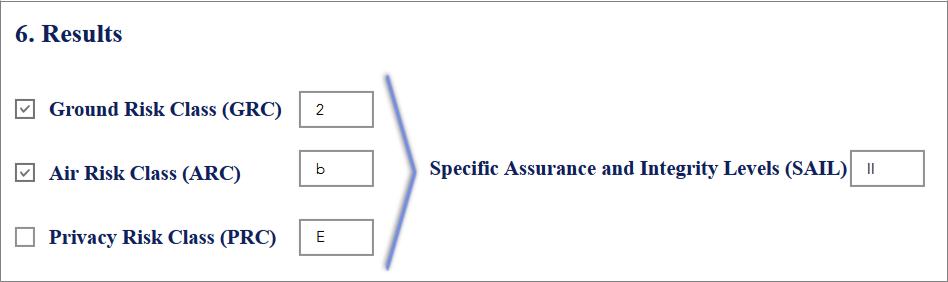


图 b. 10: 基于 GRC 和 ARC 值计算的 SAIL

首先，计算与所提供信息对应的 SAIL 值。在经典的 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，SAIL 值是基于 GRC，ARC 和 PRC 值计算的。要选择用于计算 SAIL 值的参数，用户可以点击参数左边的复选框。

显示了基于 SAIL 水平确定的不同 OSOs 和 OCSOs 的鲁棒性水平。要查看详细的目标，点击 fletch 按钮。

附录 c

风险管理结果

C. 1故障

在这个文档中，我介绍了我的24个安全需求，这些需求可以用来保护 UAS 操作。这些要求用于处理或减轻以下系统故障的影响。

无人机坠毁: 由于恶意行为，无人机失去姿态，坠毁。因为在高速公路上飞行，无人机的现金可能会导致致命的事故。(可用性丧失)

偏离轨道: 在攻击下，无人机偏离轨道，按照攻击者定义的轨道飞行。(完整性损失)

无法获取航班信息: 在攻击下，操作员无法获取航班信息。

假航班信息: 在攻击下，假航班信息被提供给运营商，使他们做出不正确的决定。(诚信缺失)

飞行信息披露: 在攻击下，攻击者可以获得未经授权的访问飞行信息，这可以帮助攻击者发起其他攻击。(保密性的丧失)

假视频: 在攻击下，操作员收到攻击者制作的假视频。这个故障并没有直接影响操作的安全，但是它使得操作的目标完全失败了。(完整性的丧失)

视频不可用: 在攻击下，操作员无法访问观察视频。(可用性丧失)

视频泄露: 在攻击下，攻击者可以获得未经授权的观察视频，这会影响被观察者的隐私。(保密性的丧失)

131

132附录 c 风险管理结果

C. 2网络安全要求

C. 2.1安全要求1

(防故障装置)

目标: 在 GPS 模块不可用的情况下，自动驾驶仪需要检测这个问题，并根据可用传感器的数据降落车辆。

相关故障: 1

C. 2.2安全需求2

目的: 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降落车辆。

相关故障: 1,2

C. 2.3保安要求3

(故障模式)

目的: 在 IMU 模块不可用的情况下，自动驾驶仪需要检测故障并终止飞行

相关故障: 1

C. 2.4保安要求4

目标: 无论何时从 IMU 模块接收原始加速度和角速度数据，自动驾驶仪都需要验证这些数据的完整性。当检测到不正确的数据时，自动驾驶仪需要终止飞行

相关故障: 1,2

C. 2.5安全需求5

对象: 自动驾驶仪需要验证导航数据的完整性，需要检测伪造数据。

|  |  |
| --- | --- |
| C. 2网络安全要求 | 133 |

相关故障: 1,2

C. 2.6安全需求6

目的: 在操作开始时，自动驾驶仪需要验证飞行计划、飞行控制参数、导航参数没有被未经授权的人修改。

相关故障: 1,2

C. 2.7保安要求7

目标: 自动驾驶仪需要验证固件是否在内容和来源方面没有被修改。

相关故障: 1,2,3,4,5,7

C. 2.8安全需求8

目的: 自动驾驶仪需要访问控制机制，只有获得授权的一方才能访问自动驾驶仪，并根据其属性权利执行操作(如只有人工制造商才能修改固件，操作者可以启动/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保安要求9

(防故障装置)

目的: 如果气压计模块不可用，则应根据其他可用传感器的数据估算飞行器的高度，以使飞行器着陆。

相关故障: 1

C. 2.10保安要求10

目标: 无论何时接收气压计模块的气压数据，自动驾驶仪都应验证这些数据的完整性。当检测到不正确的数据时，自动驾驶仪应该使飞行器着陆。

134附录 c 风险管理结果

相关故障: 1,2

C. 2.11保安要求11

(防故障装置)

目标: 如果罗盘模块不可用，自动驾驶仪需要检测这个问题，并根据可用传感器的数据着陆车辆。

相关故障: 1

C. 2.12保安要求12

目标: 无论何时从罗盘模块接收磁场数据，自动驾驶仪都需要验证这些数据的完整性。当检测到不正确的数据时，自动驾驶仪应该能让飞行器着陆。

相关故障: 1,2

C. 2.13安全需求13

目的: 每当从非易失性存储器读取罗盘标定数据时，自动驾驶仪都需要验证数据的完整性。

相关故障: 1

C. 2.14保安要求14

(securedc2链接)

目的: 为了保护自动驾驶仪与 GCS 之间的通信，需要实现一个安全的协议。该协议确保:

交换数据的完整性。无论何时接收来自 RF 模块的数据，自动导航和 GCS 都可以验证数据包在内容、时间(顺序)、原始来源(认证)方面没有被修改。

交换数据的保密性。只有经过授权的设备(自动驾驶仪，GCS)才能从交换的数据中解释信息。

|  |  |
| --- | --- |
| C. 2网络安全要求 | 135 |

交换数据的可用性。自动驾驶仪和 GCS 都有自我控制通信质量的机制。他们需要验证每条信息是否到达目的地。如果通信链路不可用，自动驾驶仪就会启动故障安全程序，自动驾驶仪就会降落在车辆上。

相关故障: 1,2,3,4,5,7

C. 2.15保安要求15

目标: 无论何时接收来自 GCS 的命令，自动驾驶仪都需要验证该命令是否对操作的安全性没有任何影响(例如，改变飞行参数，飞行期间的飞行计划等)。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，并在执行前提示他验证这个命令。

相关故障: 1,2

C. 2.16安全需求16

目标: GCS 只允许授权方进入。GCS 需要验证他们的身份(认证)和访问控制机制(访问控制)。每个参与方的角色需要被详细定义。

相关故障: 1,2,5,8

C. 2.17保安要求17

目标: GCS 需要验证存储在 GCS 计算机中的地图和飞行计划没有被恶意修改。这些数据的完整性违反需要向操作员报告。

相关故障: 4

C. 2.18安全需求18

对象: 自动驾驶仪与外部环境之间通过连接端口的数据流需要加以控制。不同种类的数据需要通过独立的端口发送或接收。这个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

136附录 c 风险管理结果

C. 2.19保安要求19

目标: 当摄像头不可用时，3G/4G 模块需要向 GCS 发送警报信息。

相关故障: 7

C. 2.20安全需求20

对象: 当视频数据不可用时，GCS 需要向操作员显示警报消息。

相关故障: 7

C. 2.21保安要求21

目标: 万向节只允许授权人员访问和修改其固件。访问控制机制应该实现。

相关故障: 6,7

C. 2.22安全需求22

目的: 万向节的参数需要保护在完整性方面。在操作开始时，万向节需要验证这些参数是由授权人员创建的，并且没有被修改。

相关故障: 7

C. 2.23保安要求23

(视频传输安全协议)

为了向 GCS 传输视频数据，需要实现安全通信协议。该协议需要确保:

交换数据的完整性。无论何时从 Internet GCS 接收视频数据，都可以验证数据是否在内容、时间(顺序)、原始来源(认证)方面被修改过。

|  |  |
| --- | --- |
| C. 3. 风险水平 | 137 |

交换数据的保密性。只有经过授权的 GCS 才能解释数据中的信息。

交换数据的可用性。 GCS 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保安要求24

目标互联网和 GCS 之间的数据流需要被控制。只有制造商定义的类型的数据可以从互联网到达 GCS 或发送到互联网的 GCS。

相关故障: 6,7,8

C. 3风险水平

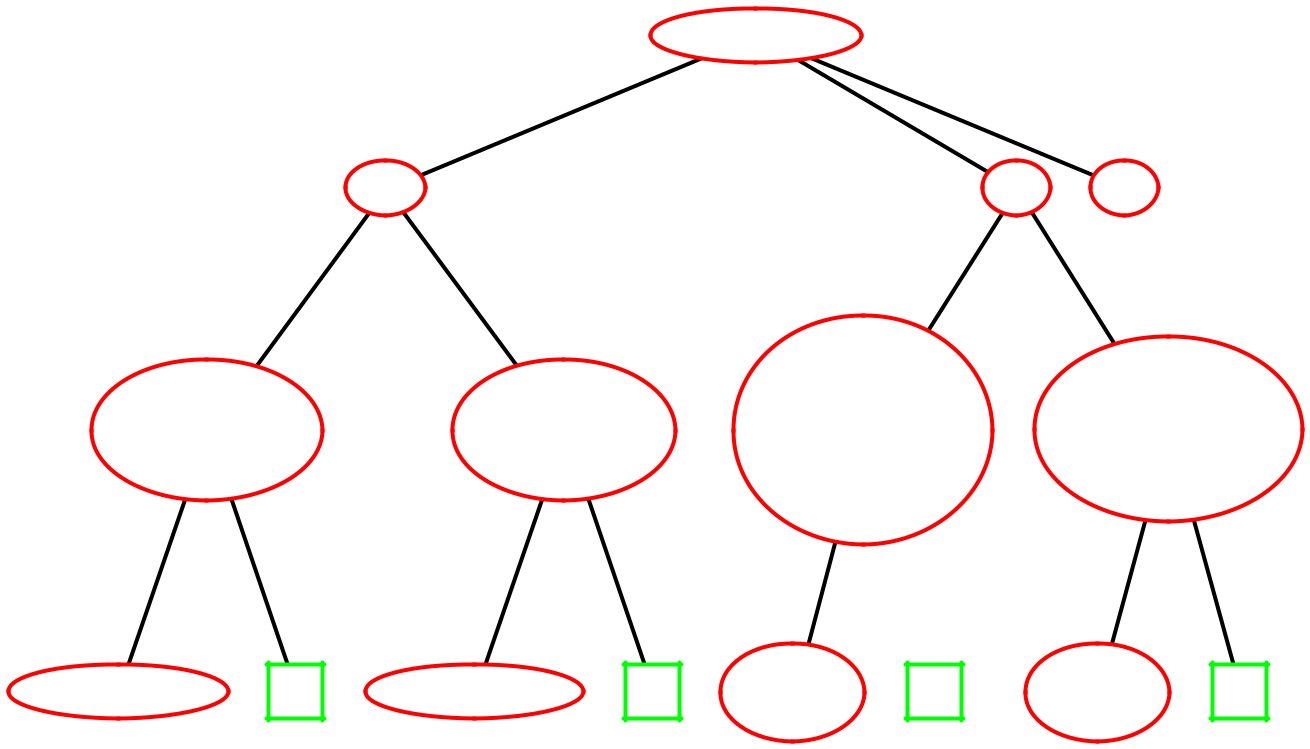
(见下一页)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 场景 | 准备 | 机会 |  | 处决 | 总计 | 到达时已死亡 | 严重程度 | 水平 | 目标组件 | 规定 |
| 1可用性1 | 2 |  | 1 | 4 | 7 | 基础 | 很高 | 很高 | GPS | 1 |
| 1 \_ availability \_ 2 | 2 |  | 1 | 8 | 11 | 基础 | 很高 | 很高 | GPS | 2 |
| 1 \_ availability \_ 3 | 6 |  | 1 | 12 | 19 | 很高 | 很高 | 中等 | IMU | 3 |
| 1 \_ 可用性 \_ 4 | 6 |  | 1 | 12 | 19 | 很高 | 很高 | 中等 | IMU | 4 |
| 1 \_ availability \_ 5 | 6 |  | 8 | 10 | 24 | 很高 | 很高 | 中等 | 自动驾驶仪 | 七，八 |
| 可用性 | 6 |  | 6 | 10 | 22 | 很高 | 很高 | 中等 | 自动驾驶仪 | 18 |
| 1\_availability \_ 7 | 6 |  | 8 | 10 | 24 | 很高 | 很高 | 中等 | 自动驾驶仪 | 7,8,6,5 |
| 1 \_ availability \_ 8 | 6 |  | 8 | 10 | 24 | 很高 | 很高 | 中等 | 自动驾驶仪 | 7,8,6 |
| 1 \_ availability \_ 9 | 6 |  | 8 | 10 | 24 | 很高 | 很高 | 中等 | 自动驾驶仪 | 7,8,6 |
| 1\_availability \_ 10 | 2 |  | 1 | 12 | 15 | 适度 | 很高 | 中等 | 晴雨表 | 9 |
| 1可用性11 | 2 |  | 1 | 12 | 15 | 适度 | 很高 | 中等 | 晴雨表 | 10 |
| 1\_availability \_ 12 | 6 |  | 1 | 12 | 19 | 很高 | 很高 | 中等 | 指南针 | 11 |
| 可用性13 | 6 |  | 1 | 12 | 19 | 很高 | 很高 | 中等 | 指南针 | 12 |
| 1\_availability \_ 14 | 6 |  | 2 | 6 | 14 | 适度 | 很高 | 中等 | 非挥发性记忆体 | 13 |
| 可用性15 | 5 |  | 1 | 6 | 12 | 基础 | 很高 | 很高 | 射频 | 1415 |
| 可用性16 | 5 |  | 1 | 6 | 12 | 基础 | 很高 | 很高 | 射频 | 1415 |
| 可用性17 | 6 |  | 3 | 2 | 11 | 基础 | 很高 | 很高 | 格拉斯哥昏迷指数 | 14151624 |
| 完整性 | 2 |  | 1 | 8 | 11 | 基础 | 非常高 | 很高 | GPS | 2 |
| 正直 | 6 |  | 8 | 10 | 24 | 很高 | 非常高 | 中等 | 自动驾驶仪 | 5,6,7,8 |
| 诚信3 | 6 |  | 8 | 10 | 24 | 很高 | 非常高 | 中等 | 自动驾驶仪 | 6,7,8 |
| 正直 | 6 |  | 1 | 12 | 19 | 很高 | 非常高 | 中等 | IMU | 4 |
| 1 \_ integrity \_ 5 | 5 |  | 1 | 6 | 12 | 基础 | 非常高 | 很高 | 射频 | 1514 |
| 正直 | 5 |  | 1 | 6 | 12 | 基础 | 非常高 | 很高 | 射频 | 1415 |
| 正直 | 6 |  | 1 | 12 | 19 | 很高 | 非常高 | 中等 | 指南针 | 12 |
| 诚实正直 | 6 |  | 1 | 12 | 19 | 很高 | 非常高 | 中等 | 晴雨表 | 10 |
| 2诚信1 | 2 |  | 1 | 6 | 9 | 基础 | 中等 | 中等 | 射频 | 14 |
| 诚信2 | 2 |  | 1 | 6 | 9 | 基础 | 中等 | 中等 | 射频 | 14 |
| 诚信3 | 6 |  | 6 | 10 | 22 | 很高 | 中等 | 很低 | 格拉斯哥昏迷指数 | 17 |
| 诚信 | 6 |  | 6 | 10 | 22 | 很高 | 中等 | 很低 | 格拉斯哥昏迷指数 | 24 |
| 正直 | 6 |  | 6 | 10 | 22 | 很高 | 中等 | 很低 | 自动驾驶仪 | 七，八 |
| 2保密 | 5 |  | 1 | 6 | 12 | 基础 | 中等 | 中等 | 射频 | 14 |
| 2保密2 | 6 |  | 6 | 10 | 22 | 很高 | 中等 | 很低 | 自动驾驶仪 | 7,8,18 |
| 保密协议 | 6 |  | 6 | 10 | 22 | 很高 | 中等 | 很低 | 自动驾驶仪 | 7,8,18 |
| 保密协议 | 6 |  | 3 | 2 | 11 | 基础 | 中等 | 中等 | 格拉斯哥昏迷指数 | 1624 |
| 3 \_ 可用性 \_ 1 | 6 |  | 6 | 10 | 22 | 很高 | 很低 | 很低 | 格拉斯哥昏迷指数 | 24 |
| 3可用性2 | 6 |  | 6 | 10 | 22 | 很高 | 很低 | 很低 | 格拉斯哥昏迷指数 | 1624 |
| 可用性 | 6 |  | 3 | 2 | 11 | 基础 | 很低 | 很低 | 格拉斯哥昏迷指数 | 1624 |
| 可用性4 | 6 |  | 6 | 10 | 22 | 很高 | 很低 | 很低 | 自动驾驶仪 | 七，八 |
| 可用性 | 4 |  | 1 | 6 | 11 | 基础 | 很低 | 很低 | 3G/4G 模块 | 23 |
| 可用性 \_ 6 | 6 |  | 8 | 12 | 26 | 非常高 | 很低 | 很低 | 3G/4G 模块 | 23 |
| 可用性 | 6 |  | 6 | 10 | 22 | 很高 | 很低 | 很低 | Gimbal 万向节 | 2122 |
| 3保密1 | 6 |  | 1 | 12 | 19 | 很高 | 很高 | 中等 | 3G/4G 模块 | 23 |
| 3保密2 | 6 |  | 1 | 10 | 17 | 适度 | 很高 | 中等 | 3G/4G 模块 | 23 |
| 机密性 | 6 |  | 1 | 10 | 17 | 适度 | 很高 | 中等 | 格拉斯哥昏迷指数 | 24 |
| 保密协议 | 6 |  | 3 | 2 | 11 | 基础 | 很高 | 很高 | 格拉斯哥昏迷指数 | 16 |
| 3诚信 | 6 |  | 6 | 10 | 22 | 很高 | 很高 | 中等 | 格拉斯哥昏迷指数 | 24 |
|  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 正直 | 6 | 1 | 12 | 19 | 很高 | 很高 | 中等 | 3G/4G 模块 | 23 |
| 完整性 | 6 | 1 | 12 | 19 | 很高 | 很高 | 中等 | 3G/4G 模块 | 23 |
| 诚实正直 | 6 | 1 | 12 | 19 | 很高 | 很高 | 中等 | 3G/4G 模块 | 23 |
|  |  |  |  |  |  |  |  |  |  |

140附录 c 风险管理结果

C. 4攻击树木



无人机坠毁

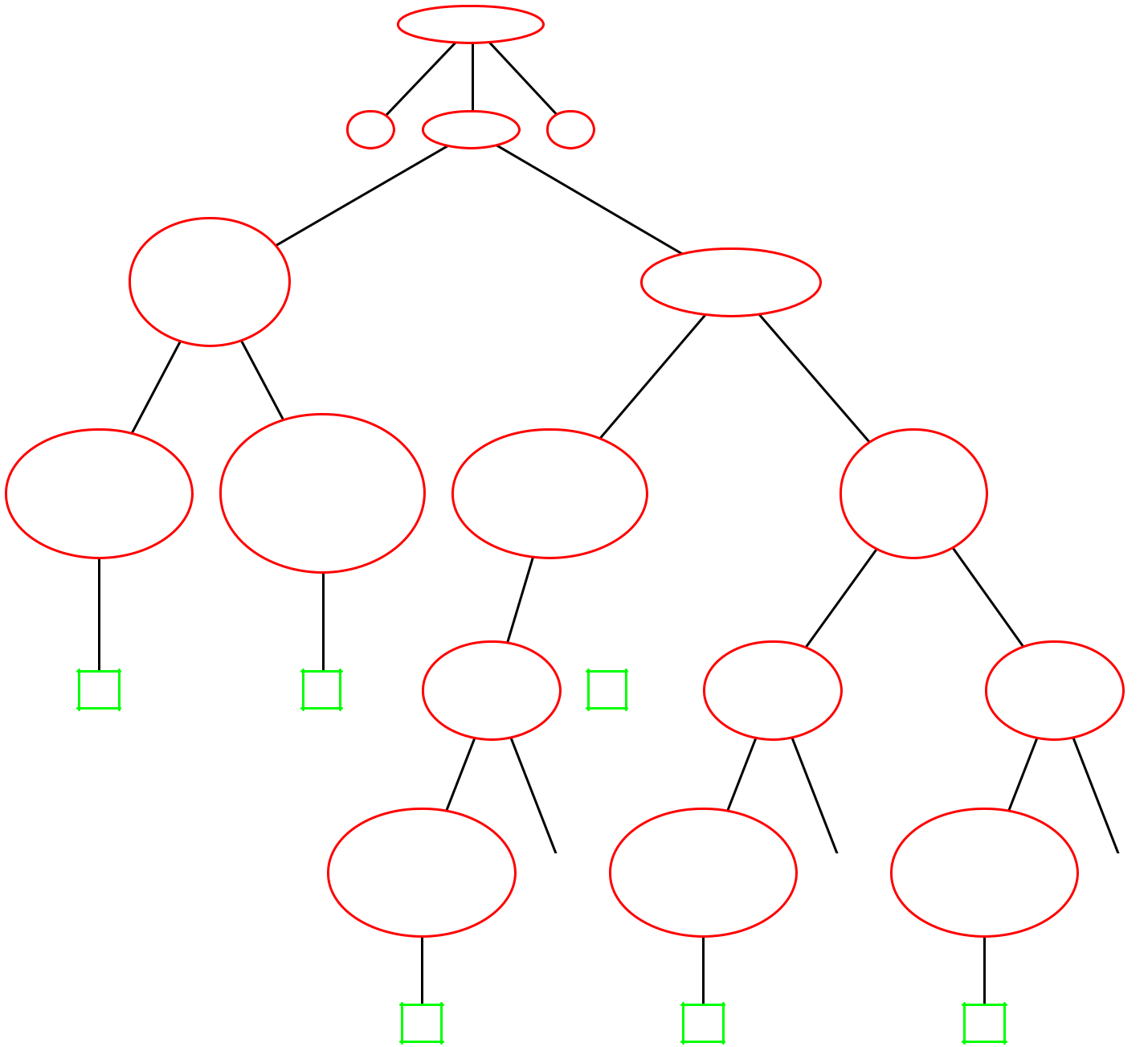
GPS IMU ooo

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | 没空 | 提供不正确/ |  |
| 没空 | 提供 | 提供 |  |
| 假加速 |  |
| 提供 | 不正确/伪造 | 加速度和 |  |
| 和角度 |  |
| 位置数据 | 位置数据 | 角速度 |  |
| 速度数据 |  |
|  |  | 资料 |  |
|  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| GPS 干扰 | 1 | 全球定位欺骗 | 2 | 噪音 | 3 | 信号 | 4 |  |
| 注射。 | 注射。 |  |
|  |  |  |  |  |  |  |

图 c. 1:1- 可用性故障的攻击树-第1部分

|  |  |
| --- | --- |
| C. 4攻击树 | 141 |



无人机坠毁

自动驾驶仪

|  |  |
| --- | --- |
| 没空 |  |
| 提供 | 提供错误信息 |
| : 马达 | 发动机指令 |
| 命令 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| 恶意软件感染 | 伪命令 | 计算 |  |
| 估计 |  |
| 通过 UART/USB | 是由其他 | 姿态/推力 |  |
| 姿态/航向/ |  |
| 端口 | 组件通过 | 校正 |  |
| 速度/高度数据 |  |
| 软件更新 | 开放的港口 | 错误的。 |  |
| 错误的 |  |
|  | 自动驾驶 |  |  |

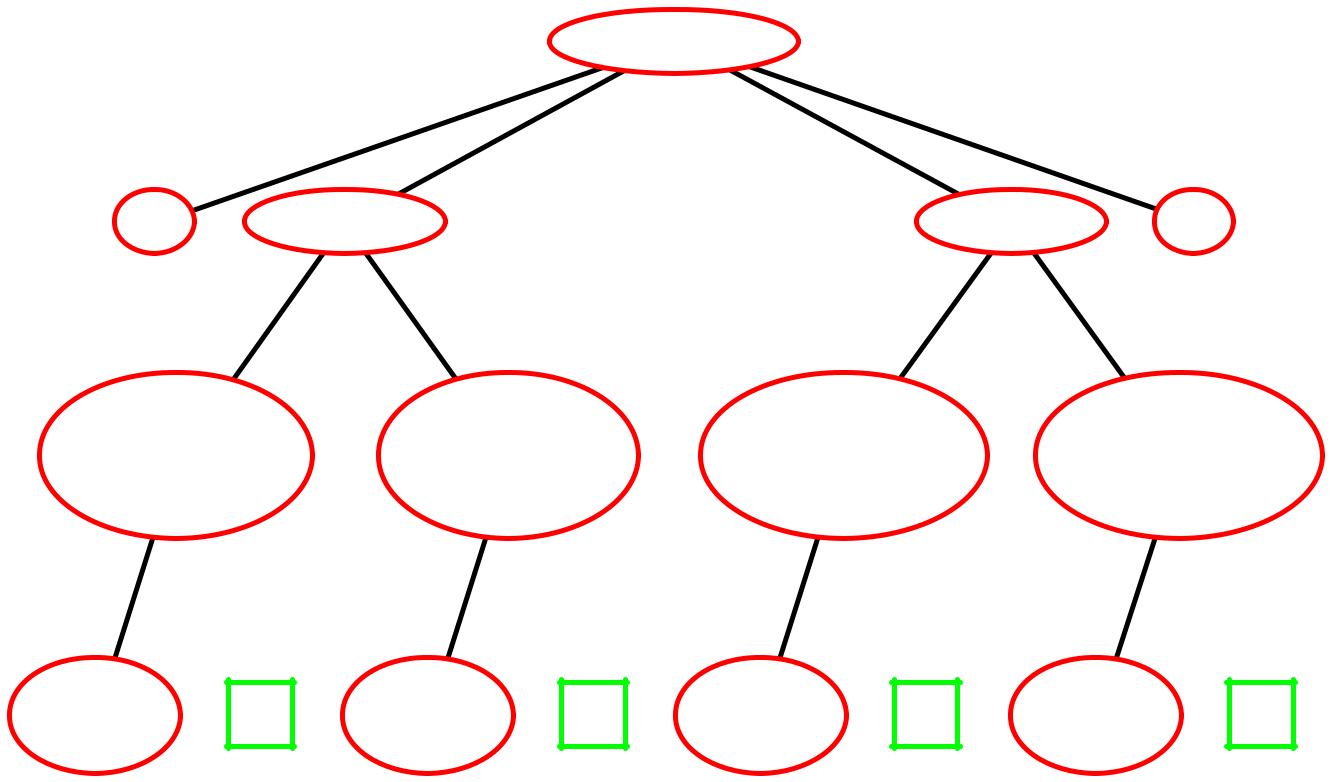
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | 导航 |  | 飞行计划 | PID 控制 |
| 7; 8 | 18 | 参数 | 5 | 参数 | 参数 |
|  |  | 都被修改了 |  | 都被修改了 | 都被修改了 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 恶意软件感染 | | 恶意软件感染 | | 恶意软件感染 | |  |
| 通过 UART/USB | 6 | 通过 UART/USB | 6 | 通过 UART/USB | 6 |  |
| 端口 | 端口 | 端口 |  |
|  |  |  |  |
| 软件更新 | | 软件更新 | | 软件更新 | |  |

|  |  |  |
| --- | --- | --- |
| 7; 8 | 7; 8 | 7; 8 |

图 c. 2:1- 可用性故障的攻击树-第2部分

142附录 c 风险管理结果



无人机坠毁

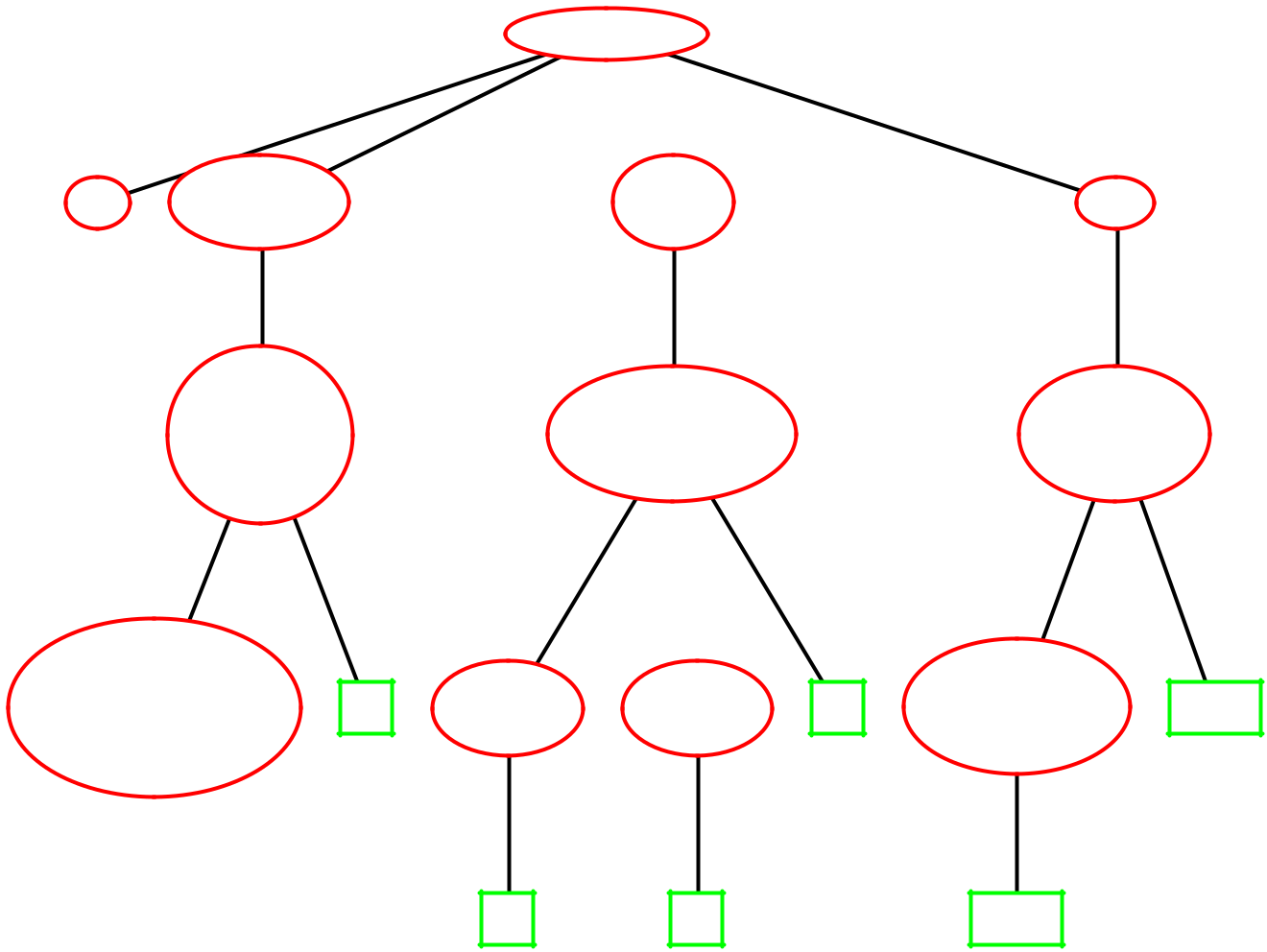
气压计指南针

|  |  |  |  |
| --- | --- | --- | --- |
| 没空 | 提供 | 没空 | 提供 |
| 提供空气 | 不正确的空气 | 提供 | 不正确/伪造 |
| 压力数据 | 压力数据 | 定位数据 | 定位数据 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 噪音 | 9 | 信号 | 10 | 噪音 | 11 | 信号 | 12 |  |
| 注射。 | 注射。 | 注射。 | 注射。 |  |
|  |  |  |  |  |

图 c. 3:1- 可用性故障的攻击树-第3部分

|  |  |
| --- | --- |
| C. 4攻击树 | 143 |



无人机坠毁

哦

不易挥发

记忆

射频

模块

格拉斯哥昏迷指数

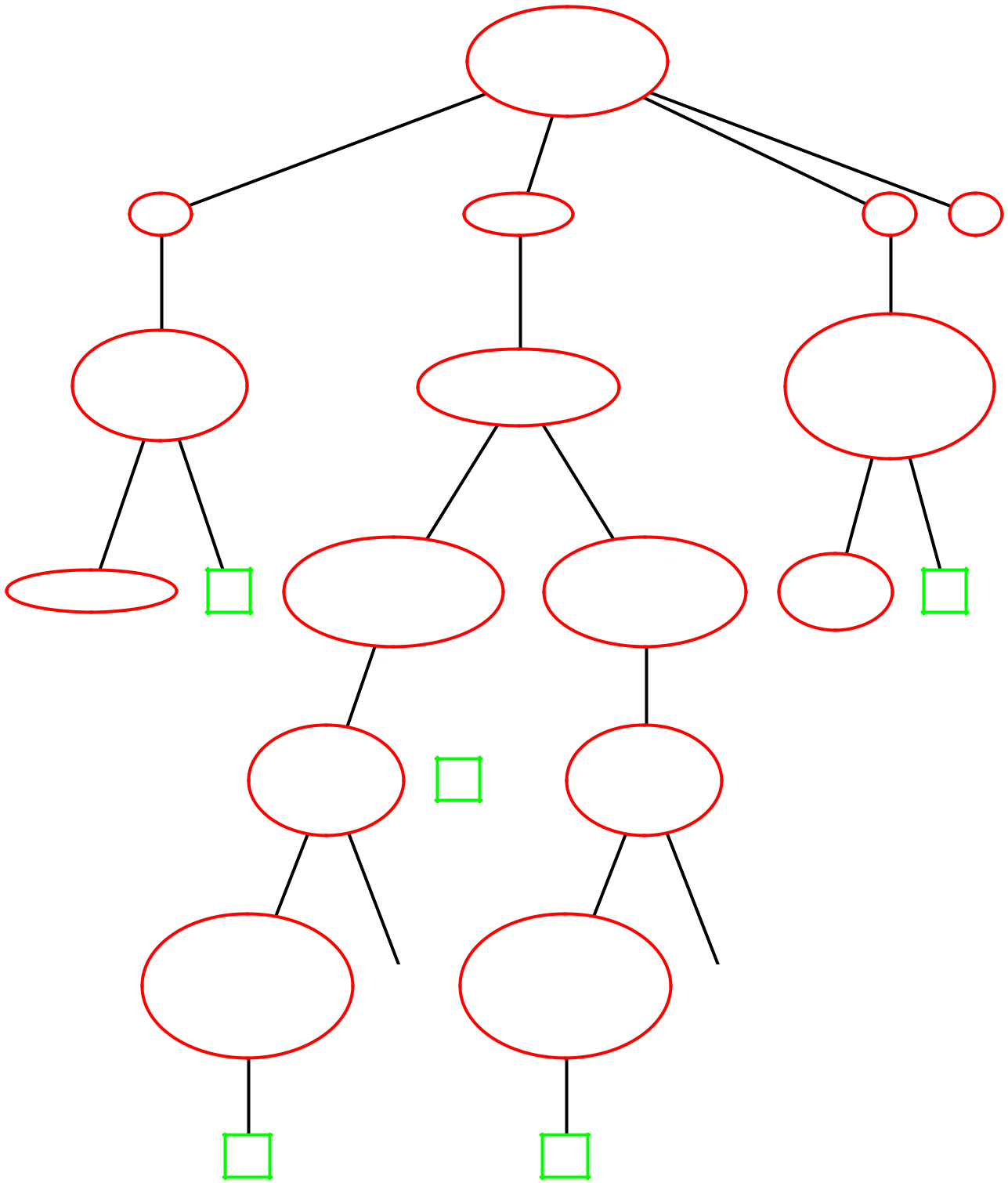
|  |  |  |
| --- | --- | --- |
| 提供假货 | 发个假的 |  |
| 提供错误信息 |  |
| 传感器 | 命令 |  |
| /伪命令 |  |
| 校准 | 那辆车 |  |
| 资料 |  |
| 资料 |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 未授权 |  |  |  | 未授权 |  |  |
| 通过自动驾驶仪进入 | 假的 | 重放 |  |  |  |
| 15 | 进入昏迷控制系统 | 14; 15 |  |
| 13 | 信息 | 信息 |  |
| 及未经授权 |  | 电脑 |  |  |
| 修改 |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 14 | 14 | 16; 24 |

图 c. 4:1- 可用性故障的攻击树-第4部分

144附录 c 风险管理结果



从

预先确定的

弹道

|  |  |  |  |
| --- | --- | --- | --- |
| GPS | 自动驾驶仪 | IMU | 哦 |

|  |  |  |  |
| --- | --- | --- | --- |
| 提供 |  | 提供不正确/ |  |
| 提供错误信息 | 假加速 |  |
| 不正确/伪造 |  |
| 发动机指令 | 和角度 |  |
| 位置数据 |  |
|  | 速度数据 |  |
|  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | 提供错误信息 | 提供错误信息 | 信号 |  |  |
| 全球定位欺骗 | 2 | 姿态/航向/ | 姿态/推力 | 4 |  |
| 注射。 |  |
|  |  | 速度/高度数据 | 纠正一下。 |  |  |
|  |  |  |  |  |

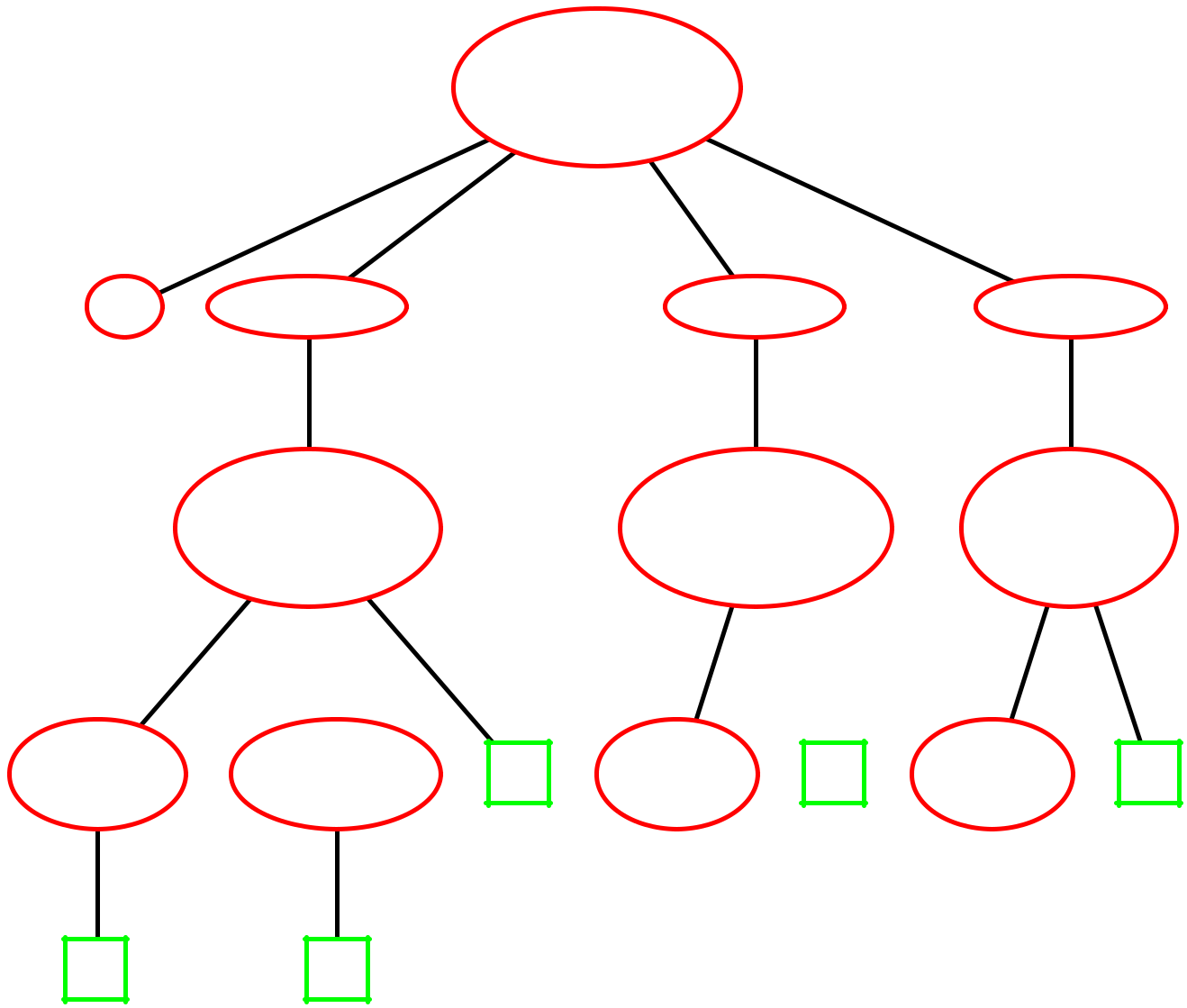
|  |  |  |
| --- | --- | --- |
| 导航 |  | 飞行计划 |
| 参数 | 5 | 参数 |
| 都被修改了 |  | 都被修改了 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 恶意软件感染 | | 恶意软件感染 | |  |
| 通过 UART/USB | 6 | 通过 UART/USB | 6 |  |
| 端口 | 端口 |  |
|  |  |  |
| 软件更新 | | 软件更新 | |  |

|  |  |
| --- | --- |
| 7; 8 | 7; 8 |

图 c. 5:1- 完整性故障的攻击树-第1部分

|  |  |
| --- | --- |
| C. 4攻击树 | 145 |



从

预先确定的

弹道

|  |  |  |  |
| --- | --- | --- | --- |
| 哦 | 射频模块 | 指南针 | 晴雨表 |

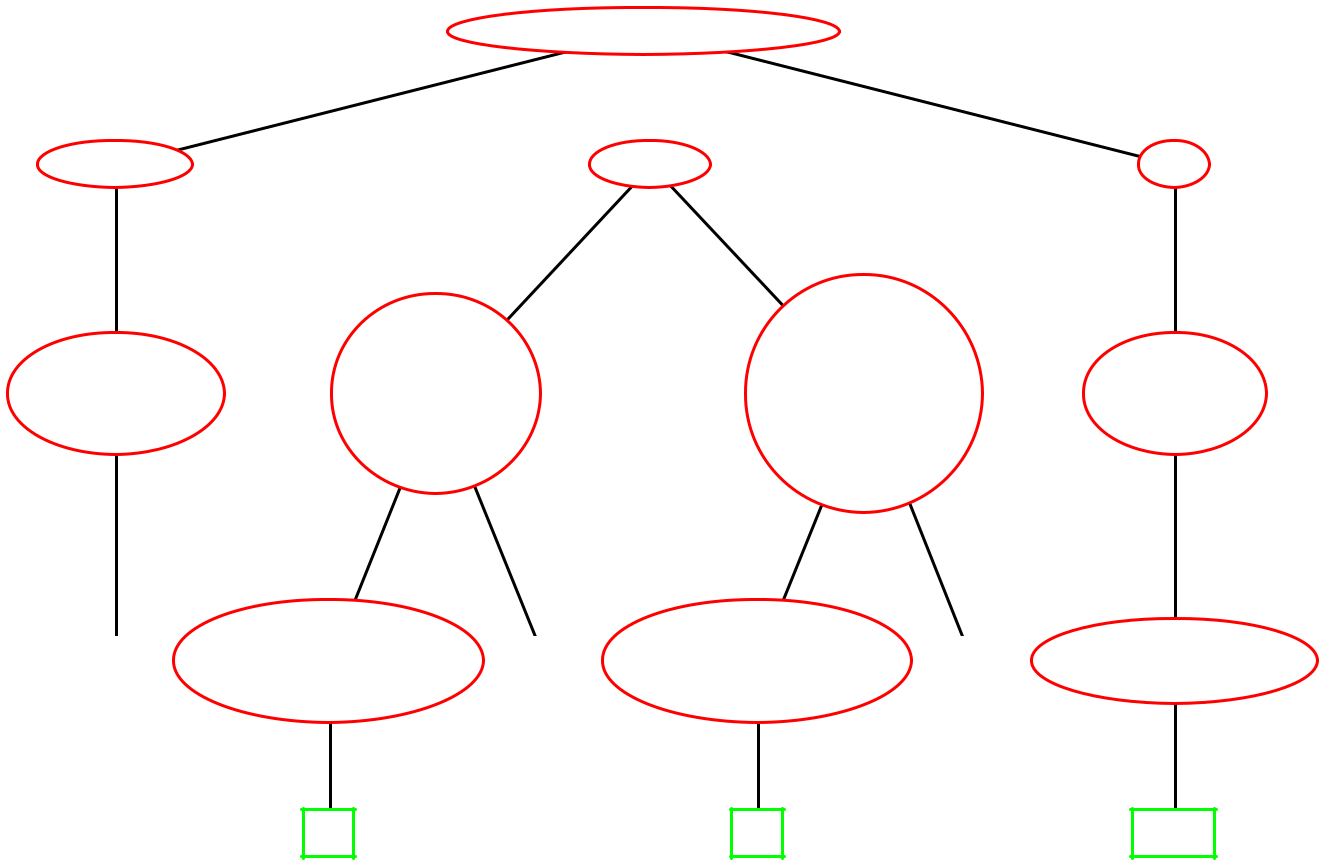
|  |  |  |
| --- | --- | --- |
| 提供 | 提供 | 提供假货 |
| 假的“回家” | 不正确/伪造 | 空气压力 |
| 命令 | 定位数据 | 资料 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 伪造数据 | 重播数据 | 15 | 信号 | 12 | 信号 | 10 |  |
| 注射 | 进攻 | 注射。 | 注射。 |  |
|  |  |  |  |

1414

图 c. 6:1- 完整性故障的攻击树-第2部分

146附录 c 风险管理结果



泄露航班资料

射频模块自动驾驶仪 GCS

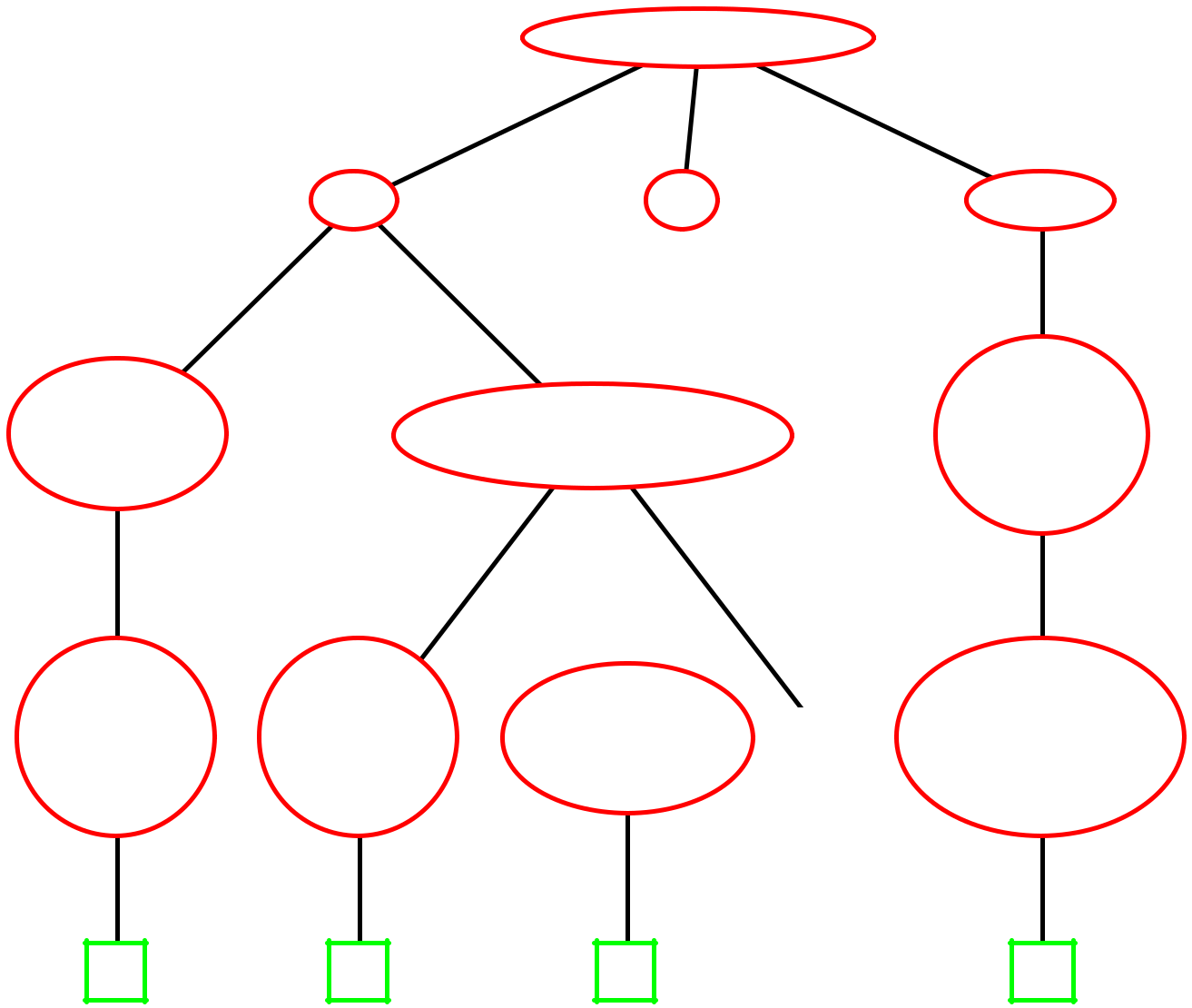
|  |  |  |  |
| --- | --- | --- | --- |
|  | 提供飞行 | 提供飞行 |  |
|  | 的资料 |  |
| 资料披露 | 资料 |  |
| 披露 |  |
| 期间 | 未经授权 | 未经授权 |  |
| 存储的数据 |  |
| 传送 | 派对结束 | 派对结束 |  |
| 格拉斯哥 |  |
|  | 未使用的端口 | 连接 |  |
|  | 对着镜头 |  |
|  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 恶意软件感染 |  | 恶意软件感染 |  | 未授权访问 |  |
| 14 | 18 | 18 |  |
| 通过 UART/USB 端口 | 通过 UART/USB 端口 |  |
| 到 GCS |  |
|  | 在软件更新期间 |  | 在软件更新期间 |  |  |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| 7; 8 | 7; 8 | 16; 24 |

图 c. 7:2- 机密性故障的攻击树

|  |  |
| --- | --- |
| C. 4攻击树 | 147 |



视频不可用

格拉斯哥昏迷指数

不能

显示影片

致营办商

|  |  |
| --- | --- |
| 恶意软件 | 恶意软件 |
| 感染 | 感染 |
| 通过未使用 | 通过未使用 |
| 港口 | 港口 |

2424

自动驾驶仪

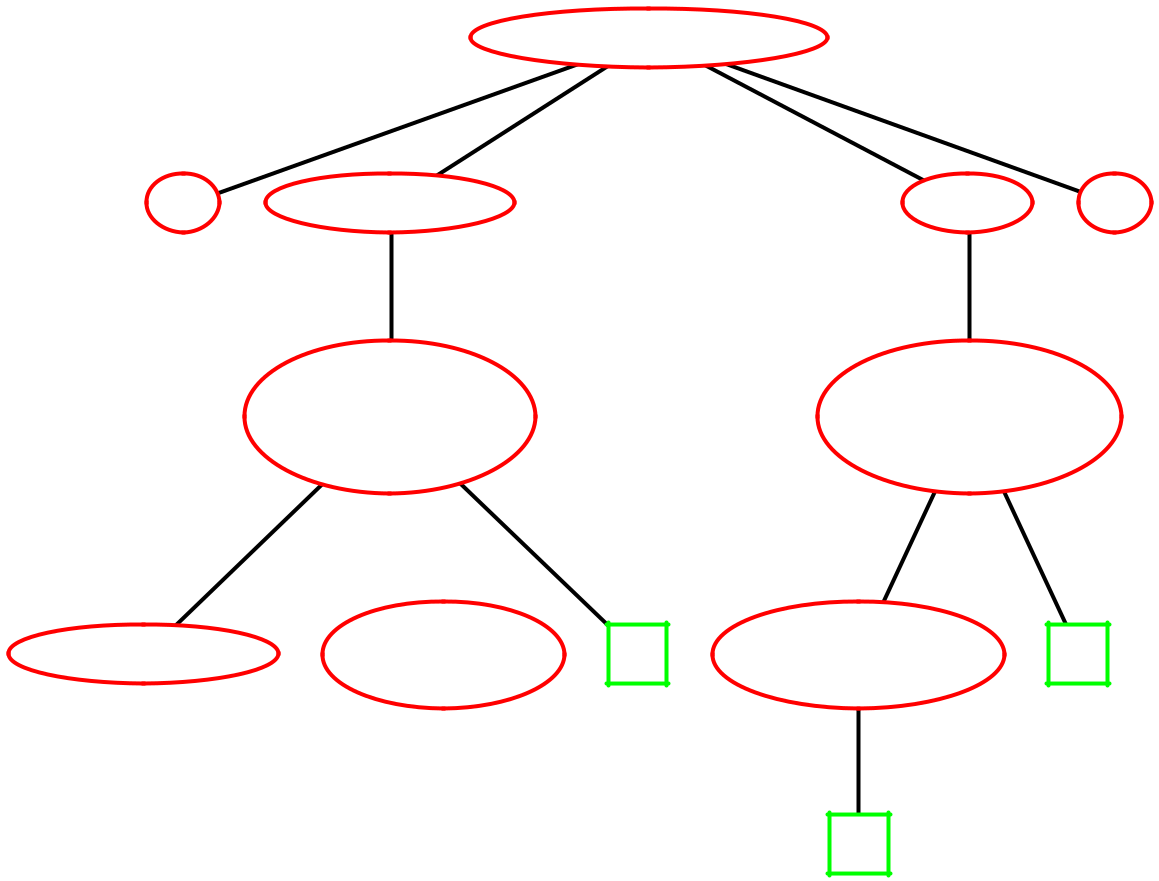
|  |  |
| --- | --- |
|  | 发送假/ |
| 提供假的/不正确的 | 不正确 |
| 命令呼叫射频模块 | 命令 |
|  | 万向节 |

|  |  |  |  |
| --- | --- | --- | --- |
| 未授权 |  | 恶意软件感染 |  |
|  | 通过 UART/USB |  |
| 14 |  |
| 进入昏迷控制系统 |  |
| 端口 |  |
| 电脑 |  |  |
|  | 软件更新 |  |
|  |  |  |

|  |  |
| --- | --- |
| 16 | 7; 8 |

图 c. 8:2-保密性故障的攻击树-第1部分

附录 c 风险管理结果



视频不可用

|  |  |  |  |
| --- | --- | --- | --- |
| 哦 | 3G/4G 模块 | Gimbal 万向节 | 哦 |

|  |  |
| --- | --- |
| 无法接近 | 不能用于 |
| 提供视频给 | 发号施令 |
| 格拉斯哥昏迷指数 | 发动机。 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 信号干扰 | DOS 攻击开始 | 23 | 恶意软件感染 | 22 |  |
| 基础设施 | 通过 USB 接口 |  |
|  |  |  |  |

21

图 c. 9:2-机密性故障的攻击树-第2部分

|  |  |
| --- | --- |
| C. 4攻击树 | 149 |



资料披露

期间

传送

经3G/4G

互联网

视频数据的披露

3G/4G 模块 GCS

|  |  |  |  |
| --- | --- | --- | --- |
| 3G/4G 模块 | | 披露 |  |
| 转发视频数据 |  |  |
| 23 |  |
| 数据储存在 |  |
| 外部 |  |
|  | GCS 计算机 |  |
| 当事人 | |  |
|  |  |

未授权

未授权

进入

恶意软件感染访问 GCS GCS

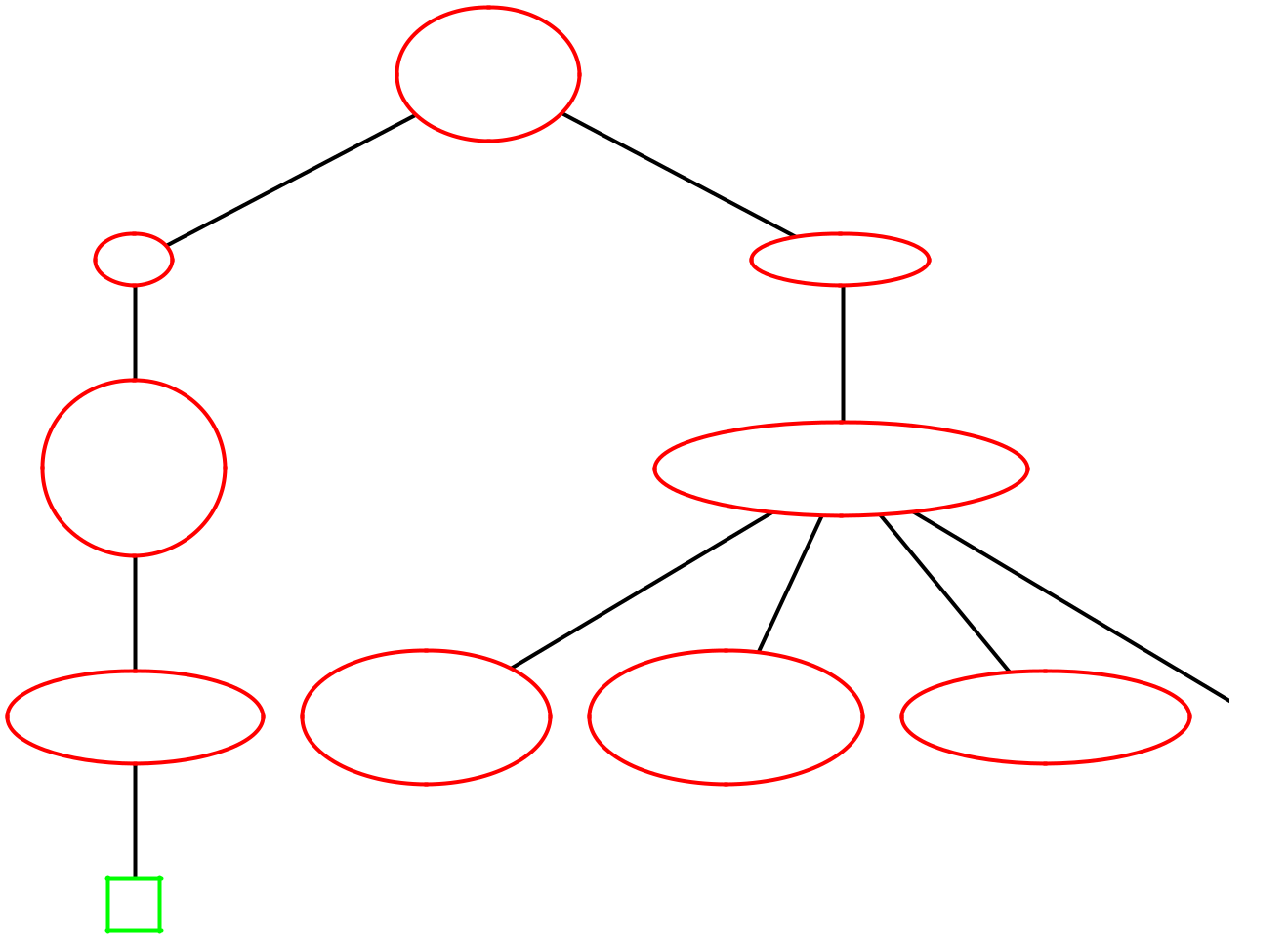
电脑

互联网

2416

图 c. 10:3保密故障的攻击树

150附录 c 风险管理结果



提供假货

视频传送至

接线员

GCS Com 3G/4G

|  |  |
| --- | --- |
| GCS. |  |
| 显示假的 | 通讯频道。 |
| 视频传送至 | 向 GCS 提供假视频 |
| 接线员。 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据注入 | 重放攻击 | 恶意软件感染 |  |  |
| 恶意软件感染 | 交流方面 | 23 |  |
| 通讯 |  |  |
| 通过未使用的端口 |  | 3G/4G 模块 |  |  |
| 链接 | 频道 |  |  |  |

24

图 c. 11:3-完整性故障的攻击树

附录 d

GPS 欺骗与对策

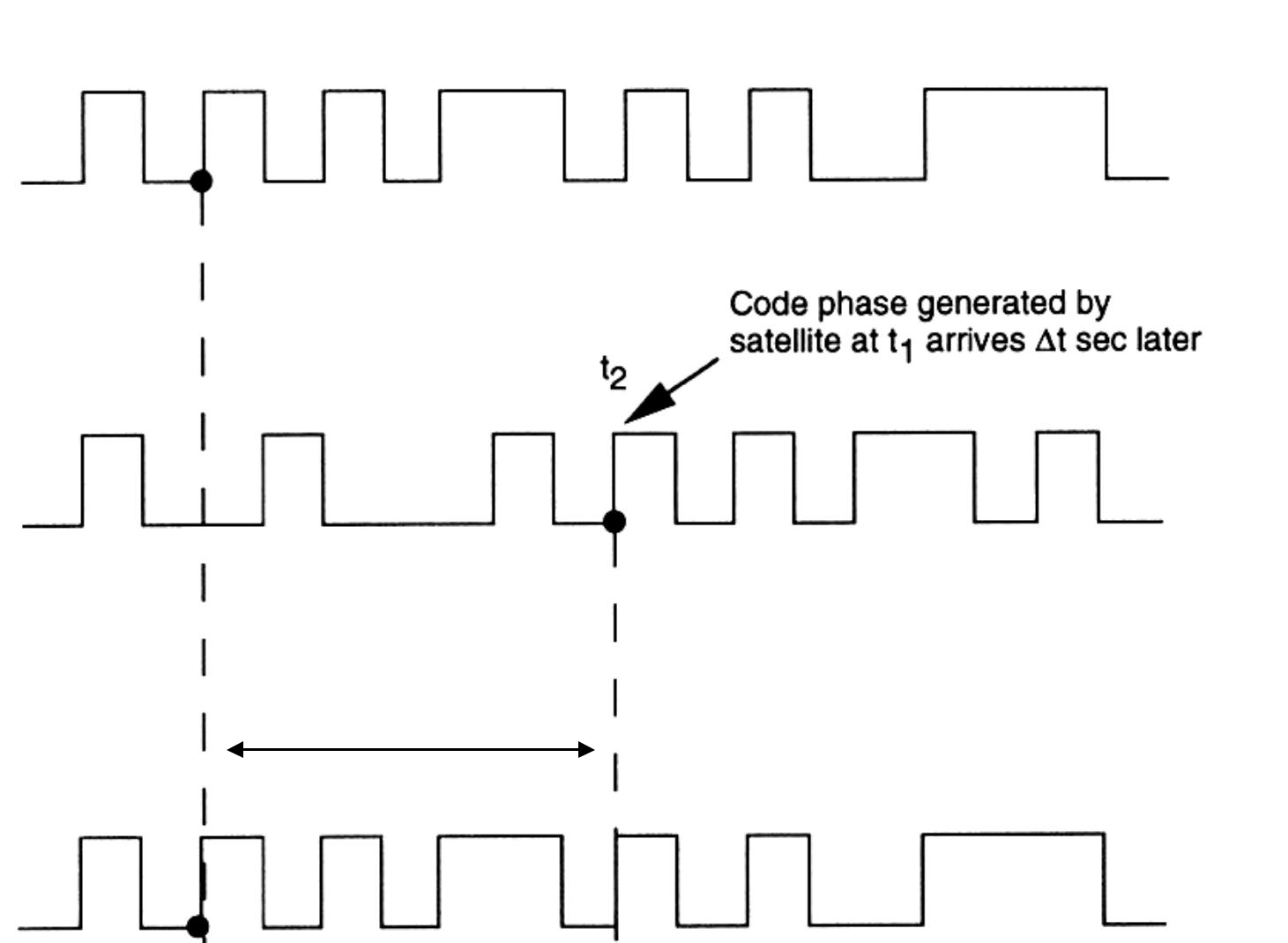
151

附录 d. GPS 欺骗与对策

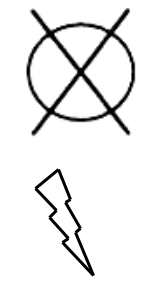
D. 1 GPS 基础

全球定位系统(GPS)是一个全球导航卫星系统(GNSS) ，自1973年以来一直由美国陆军开发和维护[209]。全球定位系统(GPS)卫星提供参考点，地球上的全球定位系统(GPS)接收器可以估计它们的位置。位置估计基于对卫星发射的信号的观测。每颗 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。信号采用两种伪乱数噪音编码: c/a (Coarse/Acquisition)和 p (Precision)进行调制。而 c/a 代码是为民用应用开放的，对每颗卫星都是唯一的，而 p 代码是加密的，用于军用应用。

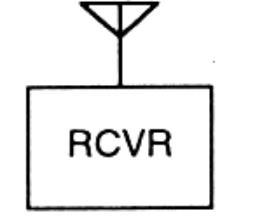
卫星生成



代码 t1



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 代码到达 |  |  | 卫星生成的代码 |  |
| T2 |  | 在 t1到达稍后 |  |
| 来自卫星 |  |  |
|  |  |  |  |



接收器

生成 TOA

副本代码

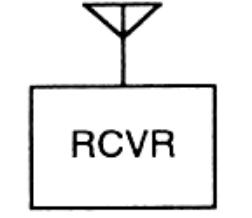


图 d. 1: 到达时间测量[210]

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算出来。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察卫星信号的到达时间(TOA)得到的。如前所述，GPS 卫星不断生成和传输经 PRN 码调制的信号。与此同时，在地球上，GPS 接收机也会产生 PRN 码调制的信号。当接收到来自卫星的信号时，接收器将接收到的代码与自身产生的代码进行比较，以确定 TOA (参见图 d. 1)。然后通过将 TOA 乘以无线电传播速度来计算卫星与接收机之间的距离。然而，在现实中，所给出的计算并没有给出从卫星到接收器的实际距离，而只是伪距离。原因是接收机的时钟通常与卫星的时钟不严格同步。这就导致了 TOA 估计和距离估计的偏差。接收机位置与伪距之间的关系如方程 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. GPS 基础 | 153 |

为了确定接收机的位置，需要知道四颗卫星而不是三颗卫星的伪距。

p

= 2(xs xr)2 + (ys yr)2 + ((zs zr)2) + c t (d

在哪里:

是从卫星到接收器的伪距离

(xs; ys; zs)是卫星的位置

(xr; yr; zr)是接收器的位置

C 是无线电传播速度

T 是接收机时钟偏差

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。生成假 GPS 信号的策略可以采用以下方法之一: GPS 信号发生器、基于中间接收器的欺骗器和基于复杂接收器的欺骗器[211]。

GPS 信号发生器是攻击者使用 GPS 模拟器产生假 GPS 信号的最直接的方法。这种技术产生的信号通常与真正的 GPS 信号不同步。因此，假信号可以通过不同的反欺骗技术来检测，如振幅监测，不同测量之间的一致性检查[212]

基于接收器的欺骗器是一种更先进的方法，其中欺骗器由 GPS 接收器和信号发射器组成。欺骗器首先与真实的 GPS 信号同步并提取导航信息。然后欺骗器用提取的信息生成假信号给目标接收者。这种攻击很难被发现，而且比第一类攻击更加复杂。这种方法的主要挑战是将欺骗信号投射到具有正确信号延迟和强度的目标接收器[212]。

复杂的基于接收机的欺骗是最复杂和有效的技术。它的目的是在接收器位置产生与真实信号相似的载波相位、信号功率和噪声。为此，欺骗器必须能够精确地跟踪接收器的位置和移动。与以前的攻击相比，这种攻击更复杂，更具挑战性，但也难以检测[212]。

附录 d. GPS 欺骗和对策

D. 2反措施的最新技术

文献中有许多著作提出了不同的对策来应对 GPS 欺骗攻击。这一部分提供了一个关注 GPS 欺骗检测的欺骗对策的回顾。主要有三种方法: (1)信号处理，(2)空间处理，(3)数据处理。

信号处理: GPS 欺骗的原理是用假信号欺骗 GPS 接收机。因此，检测未攻击的一种方法是信号监测。信号特征(如载波幅度、载波相位、信号强度、信号功率)的突然不合理跳变可能揭示一次攻击[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，以区分假信号。Shepard [215]提出了另一种基于信号功率监测的技术。由于欺骗器和目标接收器之间的距离，很难用适当的功率水平来调整假信号，这个功率水平足以欺骗接收器，但是低于真实信号的通常强度水平。Jovanovic 等[216]没有监测奇异特征，而是提出了一种算法来监测许多信号特征的统计特性并检查不一致性。

空间处理: 在正常情况下，GPS 接收机将接收不同卫星发送的信号。因此，信号会从不同的方向到达接收器。在攻击的情况下，攻击者可以生成不同卫星信号的多个假版本，并使用单一的天线进行传输。这就导致了假信号的空间相关性。这个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[218]部署了一个多天线接收机，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[219]不使用多天线接收器，而是使用带有单个天线的移动接收器来形成合成天线阵列结构，如图 d. 2所示。

数据处理: GPS 欺骗的主要目的是使 GPS 接收机提供错误的位置数据。因此，我们可以自然而然地想到，我们可以通过查找接收器输出数据的异常来检测 GPS 欺骗攻击。大多数 GPS 接收机采用接收机自主完好性监测(RAIM)算法来检测和拒绝异常测量。RAIM 算法寻找五个或更多伪距的不一致集合来检测异常测量。Psiaki 等[213]认为，这种技术可以提供一种基本的防御手段，以抵御那些只能在接收者接收到的真实信号中传输一到两个假信号的不成熟的欺骗软件。对于 Humphreys [49]实现的更复杂的攻击，这种技术是不切实际的。为了解决这个复杂的问题，一些研究人员通过寻找 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。Qiao 等[220]提出了一种利用 IMU 和单目相机实现无人机 GPS 欺骗的解决方案。数据融合应用于

|  |  |
| --- | --- |
| D. 2反制措施的最新进展 | 155 |

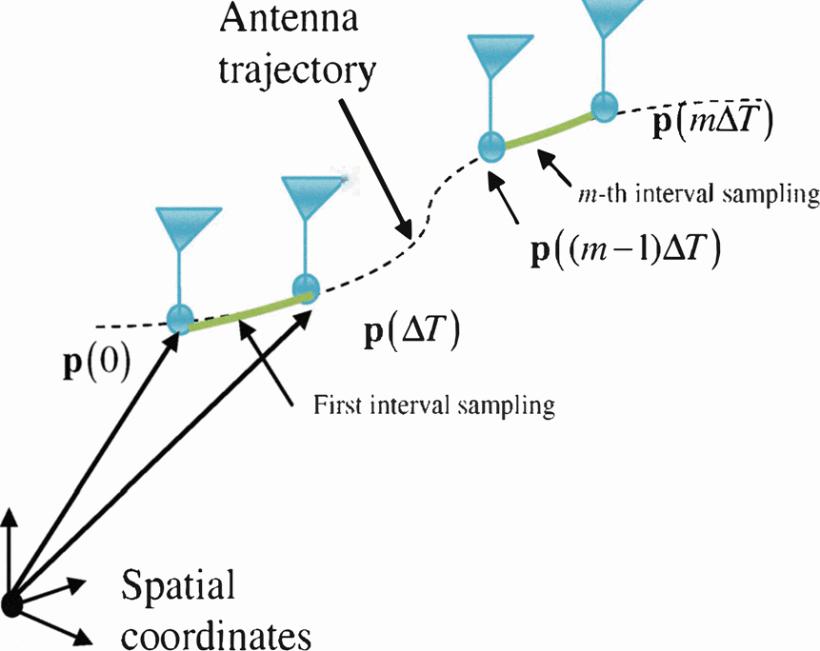


图 d. 2: 合成天线阵列结构[219]

IMU 数据和摄像机数据允许确定无人机的速度。然后，将这个值与从 GPS 数据中获得的值进行比较。当无人机接近地面飞行时，这个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这个解决方案的有效性。Panice 等[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。这个解决方案只需要 GPS 和 IMU 的数据。从 GPS 数据获得的位置信息和从 IMU 数据获得的位置信息进行比较，以寻找不一致之处。为了估计 IMU 测量的位置，它需要随着时间的推移积分加速度。在这个操作中，误差，不管多小，都会随着时间累积。这就导致了 IMU 数据位置估计的漂移效应。Panice 等人提出的这种解决方案对长时间攻击(超过30秒)不具有鲁棒性。Feng 等[222]提出了基于 IMU/GPS 数据分析的另一种解决方案。该解决方案集中于从 IMU 数据和 GPS 数据获得的加速度值，而不是无人机的位置。这样可以避免误差累积效应，使得结果更加稳健。然而，这个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。

摘要: 在这一节中，我们提供了一个 GPS 欺骗检测的简短回顾

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,

空间处理和(3)数据处理。前两种方法需要开发特定的 GPS 接收器(包括硬件和软件)。同时，大多数与第三种方法相关的解决方案可以在市场上现有的产品中实现。其中一些只需要修改自动驾驶软件。

附录 e

原有 SORA 方法中的操作安全目标

157

**无人驾驶系统规则制定联合当局**

**JARUS 关于 SORA 的指导方针**

**附件 e**

**诚信及保证水平**

**操作安全目标**

**文件标识符: jar-del-wg6-d. 04**

|  |  |  |
| --- | --- | --- |
| 版本号 | **:** | **1.0** |
| 版本日期 | **:** | 二零一九年一月二十五日 |
| 状况 | **:** | 最终/公开发布 |
| 预期目标 | **:** | 出版物 |
| 目录 | **:** | 指引 |
| 工作组 | **:** | **6** |
|  |  |  |

**未经 JARUS 允许，不得复制**

*保留所有权利。除非另有规定，本文档中的信息可以使用，但未经 JARUS 许可不允许复制粘贴。*

**目录**

**附件 e:**

**操作安全目标的完整性和保证水平**

*1. 如何使用 SORA 附件 e3*

*2. 无人机的技术问题*

OSO # 01-确保操作员有能力和/或经过验证

OSO # 02-由主管和/或经证明的实体5制造的无人机

OSO # 03-无人机由合格和/或经过验证的实体维护6

OSO # 04-UAS 开发到授权认可的设计标准7

OSO # 05-UAS 的设计考虑了系统的安全性和可靠性

OSO # 06-C3链路的特性(例如性能、频谱使用)适用于操作9

OSO # 07-无人机检验(产品检验) ，以确保与操作规程11的一致性

*3. 与业务程序有关的 OSOs 12*

*OSO # 08-操作程序的定义，验证和遵守(解决与无人机的技术问题)12*

*OSO # 11- 已有程序处理支持无人机操作的外部系统的恶化情况*

*OSO # 14-操作程序被定义，验证和遵守(解决人为错误)12*

*OSO # 21-操作程序的定义、验证和遵守(解决不良操作条件)12*

*4. 与远程船员培训有关的 OSOs 14*

*OSO # 09- 远程操作人员受过培训，能够及时控制异常和紧急情况(即技术问题)*

*无人机)14*

*OSO # 15-远程机组人员受过培训，目前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，以识别关键的环境条件，并避免他们*

*5. 与外管局设计有关的 OSOs 15*

*OSO # 10-安全回收技术问题15*

*OSO # 12- 无人机系统旨在管理支持无人机操作的外部系统的恶化情况*

*支持无人机操作的外部系统恶化16*

OSO # 13-支援无人机运作的外部服务足以应付运作16

*人为错误17*

OSO # 16-多人协调17

OSO # 17-Remote crew is fit to operate 19

OSO # 18-自动保护飞行信封免受人为错误20

OSO # 19-从人为错误中安全恢复21

OSO # 20-一个人的因素评估已经执行，人机界面(HMI)发现适合

任务23

*8. 恶劣的操作条件24*

OSO # 23-安全操作的环境条件

OSO # 24-针对恶劣环境条件设计并符合资格的无人机(例如足够的传感器、 DO-160资格)25

*技术 OSO 的保证级别标准26*

附件 e

版本: 1.0最终/公开发布第2页

***1. 如何使用 SORA 附件 e***

下表列出使用 SORA 附件 e 时需要考虑的基本原则。

|  |  |  |
| --- | --- | --- |
|  | 原理描述 | 附加信息 |
| # 1 | 附件 e 提供评审准则 | 操作安全目标的确定 |
|  | 完整性(即安全收益)和保证(即。 | 一个给定的行动，是责任的 |
|  | 证明手术安全的方法) | 申请人。 |
|  | 申请人建议的目标。 |  |
| # 2 | 附件 e 不包括 | 一些 JARUS 组织(例如 WG-7)可能会提供 |
|  | 主管当局的参与(LoI)。 | 参与程度的标准，以供 |
|  | Lol 基于主管当局 | 主管当局。 |
|  | 评估申请人的能力 |  |
|  | 执行给定的操作。 |  |
| 第三步 | 达到某一水平 |  |
|  | 正直/自信，当超过一个 |  |
|  | 这个水平是有标准的 |  |
|  | 诚信/保证，所有适用的标准 |  |
|  | 需要被满足。 |  |
| # 4 | 在 SORA 主体中定义的“可选”案例 | 操作的所有健壮性级别都是可接受的 |
|  | 表8不需要按照 | 安全目标的“可选”级别 |
|  | 附件 e 中的诚信和保证水平。 | 表6中定义了稳健性 |
|  |  | 营运安全目标」 |
|  |  | 主体。 |
| # 5 | 评估诚信水平的标准 |  |
|  | 或保证操作安全 |  |
|  | 目标依赖于“标准”尚未实现 |  |
|  | 由于 OSO 是可用的，因此需要在 |  |
|  | 能够被主管部门所接受 |  |
|  | 权威。 |  |
| 第六名 | 附件 e 故意使用非规定性的 |  |
|  | 条款(例如适当的、合理可行的) |  |
|  | 为申请人及申请人提供弹性 |  |
|  | 主管当局。这并不 |  |
|  | 限制申请人提出 |  |
|  | 缓解措施，亦无须向主管当局申请 |  |
|  | 逐案评估需要什么 |  |
|  | 基础。 |  |
| 第七名 | 本附录全文亦适用于 |  |
|  | 个人组织。 |  |

附件 e

版本: 1.0最终/公开发布第3页

***UAS 的技术问题***

**OSO # 01- 确保操作员是合格的和/或经过验证的**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | |  |  |  |  | 诚信水平 | |  |  |  |  |
|  |  | 无人机 | |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  | 相等于低。此外，申请人 |  |  |  |  |  |
|  |  |  |  |  | 申请人了解 |  |  | 有一个适合的组织 |  |  |  |  |  |
|  |  |  |  |  | 正在使用的无人机，至少 |  |  | 目的操作。申请人亦 |  |  |  |  |  |
|  | OSO # 01 |  | 标准 |  | 下列相关的运作 |  |  | 有方法识别、评估和 |  |  | 和中号一样。 |  |  |
|  |  |  | 程序: 清单、维护、, |  |  | 减少与飞行有关的风险 |  |  |  |  |
|  | 确保 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 培训、责任和 |  |  | 业务。这些应保持一致 |  |  |  |  |  |
|  | 接线员是 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 相关职责。 |  |  | 的性质和范围 |  |  |  |  |  |
|  | 称职的 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 指定的操作。 |  |  |  |  |  |
|  | 及/或 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 证明 |  |  |  |  |  | 1就本评估而言 | | |  |  |  |  |
|  |  |  |  |  |  |  | 适当的解释应该是 | | |  |  |  |  |
|  |  |  | 评论 | | 不认识 | | 与... 相称/相称 | | |  | 不认识 | |  |
|  |  |  |  |  |  |  | 组织的规模和 | | |  |  |  |  |
|  |  |  |  |  |  |  | 操作的复杂性。 | | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | |  |  |  |  | 保证水平 | |  |  |  |  |
|  |  | 无人机 | |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 申请人持有 |  |  |
|  | OSO # 01 |  |  |  |  |  |  | 在第一次操作之前，一名合格的 |  |  | 操作证书或有 |  |  |
|  |  |  |  | 级中描绘的元素 |  |  |  |  | 认可的飞行试验机构。 |  |  |
|  | 确保 |  |  |  |  |  |  |  |  |  |
|  |  | 标准 |  |  |  | 第三方进行审计 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 接线员是 |  |  | 完整性问题在 ConOps 中得到了解决。 |  |  |  |  | 此外，一个合格的第三方 |  |  |
|  |  |  |  |  |  | 组织 |  |  |  |  |
|  | 称职的 |  |  |  |  |  |  |  |  | 定期验证操作员 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | 及/或 |  |  |  |  |  |  |  |  |  | 胜任能力。 |  |  |
|  | 证明 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 评论 | | 不认识 | |  | 不认识 | |  | 不认识 | |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第4页

**OSO # 02-UAS 由合格和/或经过验证的实体制造**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | | |  |  |  |  |  |  | 诚信水平 |  |  |  |  |  |
|  | 无人机 | | |  |  |  | 很低 |  |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  | 和低价一样，另外, | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 制造程序亦包括: | |  |  |  |  |  |
|  |  |  |  |  |  | 至少是制造业 | |  |  |  | 配置控制, |  | 与媒介相同。此外, | |  |  |
|  |  |  |  |  |  | 程序包括: | |  |  |  | 来料验证 |  |  |  |
|  |  |  |  |  |  |  |  |  | 制造程序包括 | |  |  |
|  |  |  |  |  |  |  | 材料规格 |  |  |  | 产品、零部件、材料和 |  |  |
|  | OSO # 02 |  |  |  |  |  |  |  |  | 最少: |  |  |  |
|  |  |  |  |  |  | 适用性和耐久性 |  |  |  | 设备、, |  |  |  |  |  |
|  | 无人机 |  |  |  |  |  |  |  |  |  | 制造过程, |  |  |
|  |  |  | 标准 |  |  | 使用的材料, |  |  | 识别性和可追溯性, |  |  |  |
|  | 人造的 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 人事能力及 |  |  |
|  |  |  |  |  | 的必要程序 | |  |  |  | 正在进行中的，最终的 |  |  |  |
|  | 由胜任的 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 资格, |  |  |
|  |  |  |  |  |  | 的可重复性 |  |  |  | 检验及测试, |  |  |  |  |
|  | 及/或 |  |  |  |  |  |  |  |  |  |  | 供应商控制。 |  |  |
|  |  |  |  |  |  | 制造和整合 |  |  | 工具的控制和校准, | |  |  |  |
|  | 已证实的实体 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 在可接受的允许范围内。 |  |  |  | 处理及贮存, |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 不合格品控制。 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 评论 | | 不认识 |  |  |  | 不认识 |  |  | 不认识 |  |  |  |
|  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 技术问题 | | | |  |  |  |  |  |  | 保证水平 |  |  |  |  |  |
|  | 无人机 | | |  |  |  | 很低 |  |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  | 申报的制造业 | |  |  |  |  |  | 和中号一样，另外: | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 程序被发展成一个 | |  |  | 和低价一样，另外，证据是 | |  | 生产程序, |  |  |
|  |  |  |  |  |  | 认为足够的标准 | |  |  |  | 无人机系统是否符合其 | |  |  |
|  |  |  |  |  |  |  |  | 无人机系统已经可以使用 | |  |  |  |
|  |  |  |  | 标准 |  | 主管当局及/或 | |  |  |  |  | 设计及规格 |  |  |
|  |  |  |  |  |  |  | 制造，以符合其 | |  |  |  |  |
|  | OSO # 02 |  |  |  |  | 按照... 的方法 | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 设计。 | |  | 通过以下途径反复验证 | |  |  |
|  | 无人机 |  |  |  |  | 可接受的 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 程序或产品审核 | |  |  |
|  | 人造的 |  |  |  |  | 权威。 | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 有资格的第三者。 | |  |  |
|  | 作者: |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 称职的 |  |  |  |  | 国家航空局(NAAs) | | |  |  |  |  |  |  |  |  |
|  | 及/或 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 标准及/或 | | |  |  |  |  |  |  |  |  |
|  | 已证实的实体 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 他们认为符合规定的手段 | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 评论 | | 附件 e | | |  | 不认识 |  |  | 不认识 |  |  |  |
|  |  |  |  |  |  | 在稍后的时间更新 | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 的适当标准清单 | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | NAAs 提供的反馈意见。 | | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第5页

**OSO # 03-由有能力和/或经过验证的实体维护的 UAS**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | |  |  |  |  |  |  | 诚信水平 | | | | |  |  |  |  |  |  |
|  |  | 无人机 | |  |  | 很低 |  |  |  | 中等 | | | |  |  |  | 很高 | |  |  |
|  |  |  |  |  |  |  |  |  | 和 Low 一样，另外: | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  | 无人机维护说明 | |  |  | 定期维修保养 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 无人机系统是有组织的 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  | 定义，并在适用时 | |  |  |  |  | 与媒介相同。此外, | | |  |  |
|  | OSO # 03 |  |  |  | 覆盖无人机设计师 | |  |  | 按照 | | | 维修 |  |  |  | 维修人员按照 | | |  |  |
|  | 无人机 |  |  |  | 指示及要求。 | |  |  |  | 纲领。 |  | | |  |  | 还有维修程序手册 | | |  |  |
|  |  |  |  |  |  | 维修工作完成后, | | | | |  |  |  |
|  | 保持 |  |  |  | 维修人员 | |  |  |  |  |  |  |  |  |  |
|  |  | 标准 |  |  |  |  |  | 提供信息和 | | |  |  |
|  | 作者: |  |  |  |  | 日志系统用于记录所有 | | | | |  |  |  |  |
|  |  |  | 合资格，并已收到 | |  |  |  |  | 相关的程序 | | |  |  |
|  | 称职的 |  |  |  |  |  | 进行的维修保养工作 | | | | |  |  |  |  |
|  |  |  |  | 进行无人机系统的授权 | |  |  |  |  | 维修设施、记录、, | | |  |  |
|  | 及/或 |  |  |  |  |  | 无人机系统包括发行版 | | | | |  |  |  |  |
|  |  |  |  | 维修。 | |  |  |  |  | 维修指示、释放、, | | |  |  |
|  | 证明 |  |  |  |  |  | 维护释放只能是 | | | | |  |  |  |  |
|  |  |  |  | 维修人员使用 | |  |  |  | 工具、材料、部件、缺陷 | | |  |  |
|  | 实体(例如。 |  |  |  |  |  | 由职员完成 | | | | |  |  |  |  |
|  | 工业 |  |  |  | UAS 维护说明 | |  |  | 收到赡养费的人 | | | | |  |  | 延期。 | | |  |  |
|  | 标准) |  |  |  | 在进行维修工作时。 | |  |  | 放行授权书 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 特定无人机型号/系列。 | | | | |  |  |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 | | | 不认识 | | | | | | |  | 不认识 | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | |  |  |  |  |  | 保证水平 | | | | |  |  |  |  |  |  |
|  |  | 无人机 | |  | 很低 |  |  |  |  | 中等 | | |  |  | 很高 | | |  |  |
|  |  |  |  |  | 维修说明如下 |  |  | 和 Low 一样，另外: | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 维修保养计划是 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  | : 记录在案。 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 按照 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  | 进行的维修工程 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 认为适当的标准 | | | | |  |  | 与媒介相同。此外, | | |  |  |
|  |  |  |  |  | UAS 记录在一个维护中 |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 主管当局及/或 | | | | |  |  |  |  |
|  |  |  | 准则 # 1 |  |  |  |  |  | 维修保养计划及 | | |  |  |
|  |  |  |  | 日志系统1/2。 |  |  |  |  |  |  |
|  |  |  |  |  |  | 按照... 的方法 | | | | |  |  |  |
|  |  |  | (程序) |  |  |  |  |  | 维修程序手册 | | |  |  |
|  |  |  |  | 维修人员名单 |  |  | 可接受的 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 由有资格的第三方确认。 | | |  |  |
|  |  |  |  |  | 授权进行 |  |  | 权威3。 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 建立维修保养系统，并 |  |  | 维修人员名单 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  | 最新的。 |  |  | 维修放行授权书 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 建立并保持最新。 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 1目标是记录所有 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | OSO # 03 |  |  |  | 在飞机上进行的维修, | | 3国家航空局(NAAs) | | | | | | |  |  |  |  |  |  |
|  |  |  |  | 以及执行的原因(缺陷或 | | 标准及/或 | | | | | | |  |  |  |  |  |  |
|  | 无人机 |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 故障纠正，修改, | | 他们认为符合规定的手段 | | | | | | |  |  |  |  |  |  |
|  | 保持 |  |  |  |  |  |  |  |  |  |
|  |  | 评论 | | 定期维修等) | | 附件 e | | | | | | |  | 不认识 | | | |  |
|  | 作者: |  |  |  |
|  |  |  |  | 2维护日志可能是 | | 在稍后的时间更新 | | | | | | |  |  |  |  |  |  |
|  | 称职的 |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 署长要求进行的检查/审核 | | 适当标准的清单 | | | | | | |  |  |  |  |  |  |
|  | 及/或 |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 批准当局或获授权的 | | 提供的反馈意见。 | | | | | | |  |  |  |  |  |  |
|  | 证明 |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 代表。 | |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 实体(例如。 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 工业 |  |  |  |  |  |  | 和 Low 一样，另外: | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 初步培训大纲和培训 | | | | |  |  |  |  |  |  |  |
|  | 标准) |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 标准，包括 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 理论/实践要素, | | | | |  |  | 和中号一样，另外: | | |  |  |
|  |  |  |  |  |  |  |  | 定义了持续时间等 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 经常性培训计划 | | |  |  |
|  |  |  |  |  | 所有相关资历的记录; |  |  | 的规定 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 持有赡养费的员工的 | | |  |  |
|  |  |  | 标准 # 2 |  | 经验及/或已完成的训练 |  |  | 持有的授权 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  | 释放授权书 | | |  |  |
|  |  |  | (训练) |  | 由维修人员负责 |  |  | 维修人员。 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  | 编制; 及 | | |  |  |
|  |  |  |  |  | 并及时更新。 |  |  | 持有维修保养费的员工 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 这个计划是由一个 | | |  |  |
|  |  |  |  |  |  |  |  | 释放授权，最初的 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 有资格的第三者。 | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 培训是专门针对那个特定的 | | | | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 无人机型号/系列。 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 所有维修人员都拥有 | | | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 经过初步训练。 | | | | |  |  |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 | | 不认识 | | | | | | |  | 不认识 | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第6页

**OSO # 04-UAS 开发为权威认可的设计标准**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | |  |  |  |  |  |  | 诚信水平 | | | |  |  |  |  |  |  |
|  |  | 无人机 | |  |  | 很低 | |  |  |  | 中等 | |  |  |  | 很高 | |  |  |
|  |  |  |  |  | 无人机是按照标准设计的 | | |  |  | 无人机是按照标准设计的 | | |  |  | 无人机是按照标准设计的 | | |  |  |
|  |  |  |  |  |  |  | 认为足够的主管 | | |  |  | 认为足够的主管 | | |  |  |
|  |  |  |  |  | 认为足够的主管 | | |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 授权及/或按照 | | |  |  | 授权及/或按照 | | |  |  |
|  | OSO # 04 |  |  |  | 授权及/或按照 | | |  |  |  |  |  |  |
|  | 无人机 |  | 标准 |  | 可接受的符合规定方法 | | |  |  | 可接受的符合规定方法 | | |  |  | 可接受的符合规定方法 | | |  |  |
|  | 发展 |  |  | 标准及/或 | | |  |  | 标准及/或 | | |  |  | 标准及/或 | | |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 授权书 |  |  |  | 遵守规定的方法 | | |  |  | 遵守规定的方法 | | |  |  | 遵守规定的方法 | | |  |  |
|  | 认出来了 |  |  |  | 适用于诚信程度低的人 | | |  |  |  |  |  |  |
|  |  |  |  |  |  | 适用于中等程度的 | | |  |  | 适用于高度正直的人 | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 设计 |  |  |  | 以及预期的行动。 | | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 诚信和预期的操作。 | | |  |  | 以及预期的行动。 | | |  |  |
|  | 标准 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 国家航空局(NAAs)可以定义他们认为适当的标准和/或遵守手段。 | | | | | | | | | | | | | |  |
|  |  |  |  |  |  |
|  |  |  | 评论 | | SORA 附件 e 将在稍后时间更新，并根据所提供的反馈意见列出适当的标准清单 | | | | | | | | | | | | | |  |
|  |  |  |  |  | 国家航空航天局。 | | | |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | | |  |  |  | 保证水平 |  |  |
|  | 无人机 | | |  |  | 很低 |  | 中等 | 很高 |  |
|  | OSO # 04 |  |  | 标准 |  | 考虑第9节中定义的标准 |  |  |  |  |
|  | 无人机 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 发展成 |  |  |  |  |  |  |  |  |  |
|  | 权威 |  |  |  |  |  |  |  |  |  |
|  | 认出来了 |  |  | 评论 | | 不认识 | 不认识 |  | 不认识 |  |
|  | 设计 |  |  |  |  |  |  |  |  |  |
|  | 标准 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第7页

**OSO # 05-UAS 的设计考虑了系统的安全性和可靠性**

(a)本职业安全主任办公室补充:

在主体中定义的容器的安全要求

OSO # 10和 OSO # 12，仅针对在人口稠密地区或人群聚集地开展业务时发生死亡的风险。

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | |  |  |  | 诚信水平 | |  |  |  |  |
|  |  | 无人机 | | 很低 | |  | 中等 | |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  | 和中号一样，另外: |  |  |
|  |  |  |  |  |  |  |  |  |  | 主要故障情况不是 |  |  |
|  |  |  |  |  |  |  |  |  |  | 比 Remote3更频繁; |  |  |
|  |  |  |  |  |  |  |  |  |  | 危险故障情况如下 |  |  |
|  |  |  |  |  |  |  |  |  |  | 不比极端频繁 |  |  |
|  |  |  |  |  |  |  |  |  |  | Remote3; |  |  |
|  |  |  |  |  |  |  | 与 Low 相同。此外，战略 | |  | 灾难性的故障情况是 |  |  |
|  |  |  |  | 设备、系统和 | |  |  | 不比极端频繁 |  |  |
|  |  |  |  |  | 的检测、警报和管理 | |  |  |  |
|  |  |  |  | 装置的设计是为了尽量减少 | |  |  | Improbable3; |  |  |
|  |  |  | 标准 |  | 任何故障、故障或 | |  |  |
|  |  |  | 在可能发生的情况下 | |  |  | 软件(SW)和机载 |  |  |
|  |  |  |  | 两者的结合，将导致 | |  |  |  |
|  |  |  |  | 无人机的故障或失败。 | |  |  |  |  |
|  |  |  |  |  | 危险是可利用的。 | |  | 电子硬件(AEH) |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 发展错误可能导致或 |  |  |
|  | OSO # 05 |  |  |  |  |  |  |  |  | 造成危险或 |  |  |
|  | 无人机才是 |  |  |  |  |  |  |  |  | 灾难性的故障情况是 |  |  |
|  | 设计 |  |  |  |  |  |  |  |  | 发展成行业标准 |  |  |
|  | 考虑到 |  |  |  |  |  |  |  |  | 或考虑的方法 |  |  |
|  | 系统 |  |  |  |  |  |  |  |  | 由合资格人士提供足够的 |  |  |
|  | 安全及 |  |  |  |  |  |  |  |  | 授权及/或按照 |  |  |
|  | 可靠性 |  |  |  |  |  |  |  |  | 可接受的符合规定方法 |  |  |
|  |  |  |  |  |  |  |  |  |  | 授权4。 |  |  |
|  |  |  |  | 1就本评估而言, | |  |  |  |  | 3安全目标可能来源于 | |  |
|  |  |  |  | ”危险”一词应予以解释 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | JARUS AMC RPAS. 1309 Issue 2 Table JARUS AMC RPAS. 1309第二期 | |  |
|  |  |  |  | 作为一种故障情况，与 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 3取决于 UAS 类或 | |  |
|  |  |  |  | 主要的、危险的或 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 等效的基于风险的方法 | |  |
|  |  |  |  | 灾难性的。 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 为主管当局所接受。 | |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 评论 | 2就本评估而言, | | 不认识 | | |  | 4发展保证水平 | |  |
|  |  |  |  | 术语“可能”应该是 | |  |  |  |  | SW/AEH 的 DALs 可以派生出来 | |  |
|  |  |  |  | 以定性的方式解释为, | |  |  |  |  | 来自 JARUS AMC RPAS. 1309 Issue 2 | |  |
|  |  |  |  | 预期会发生一次或多次 | |  |  |  |  | 表3取决于 UAS 类或 | |  |
|  |  |  |  | 在整个系统/运作期间 | |  |  |  |  | 等效的基于风险的方法 | |  |
|  |  |  |  | 无人机系统」。 | |  |  |  |  | 为主管当局所接受。 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 技术问题 | | |  |  |  | 保证水平 | |  |  |  |  |
|  |  | 无人机 | | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  | 和 Low 一样，另外: | |  |  |  |  |  |
|  |  |  |  |  |  | 安全分析是在 | |  |  |  |  |  |
|  |  |  |  | 功能性危害评估1和 |  |  | 符合考虑的标准 |  | 和中号一样，另外，安全性 | |  |  |
|  |  |  |  |  |  | 由合资格人士提供足够的 |  |  |  |
|  |  |  |  | 设计和安装鉴定 |  |  |  | 分析及发展保证 | |  |  |
|  |  |  | 标准 |  |  | 授权及/或按照 |  |  |  |
|  | OSO # 05 |  | 显示危害最小化 |  |  |  | 活动由合资格的 | |  |  |
|  |  |  |  | 可接受的合规手段 |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  | 有空。 |  |  |  | 第三方。 | |  |  |
|  | 无人机才是 |  |  |  |  | 权威机构。 |  |  |  |
|  | 设计 |  |  |  |  | 一个策略，用于检测单 | |  |  |  |  |  |
|  | 考虑到 |  |  |  |  |  | 关注的失败包括 |  |  |  |  |  |
|  | 系统 |  |  |  |  |  | 飞行检查。 |  |  |  |  |  |
|  | 安全及 |  |  |  | |  |  |  |  |  |  |  |
|  |  |  | 1故障情况的严重程度(No | |  |  |  |  |  |  |  |
|  | 可靠性 |  |  |  |  |  |  |  |  |  |
|  |  |  | 安全效应，轻微，重大，危险 | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 评论 | 和灾难性的) | | 不认识 | | | 不认识 | | |  |
|  |  |  | 根据定义确定的 | |  |
|  |  |  |  |  |  |  |
|  |  |  |  | JARUS AMC RPAS. 1309 | |  |  |  |  |  |  |  |
|  |  |  |  | 第二期。 | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第8页

**OSO # 06-C3链路特性(例如性能、频谱使用)适用于操作**

就《职业介绍所管理条例》和本《职业介绍所管理条例》而言，“ C3联系”一词包括:

Command and Control (C2) link，以及

为了飞行安全所需要的任何通讯联系。

要正确评估该职业安全主任的完整性，申请人应确定:

C3将预期操作所需的性能要求联系起来。

所有 C3链路，连同它们的实际性能和射频(RF)频谱使用。

注意: C2链路的性能和射频频谱规范通常由 UAS 设计人员在 UAS 手册中记录。

注意: 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

(例如用于与 ATC 通信的 RCP)包括，但不限于以下内容:

可用性 o 连续性 o 完整性

有关定义，请参阅国际民航组织的参考文献。

预期操作的射频频谱使用要求(包括需要授权的情况下)。

注: 通常，各国公布适用于其领土的射频频谱波段的分配。这种分配主要来源于国际电信联盟(ITU)的无线电规则。然而，申请者应核对当地的要求，并在需要时请求批准，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(例如 AM (r) s、 AMS (r) s 5030-5091MHz)已获分配，可用于国际民用航空组织范围内的无人机作业，用于分类为目录的无人机作业。C (“认证”) ，但它们的使用可能被授权用于特定类别下的操作。预计其他持牌频带(例如分配给流动网络的频带)的使用也可能在特定类别下获得授权。某些未获发牌照的乐队(例如 ISM (Industrial，Scientific，Medical)或 SRD (Short Range Devices))在特定类别下也可接受，例如操作完整性要求较低的乐队。

可能影响 C3链路性能的环境条件。

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | |  |  |  |  |  | 诚信水平 |  |  |  |  |
|  | 无人机 | |  |  | 很低 |  |  | 中等 |  | 很高 |  |  |
|  |  |  |  |  | 申请人认为 |  |  |  |  |  |  |  |
|  |  |  |  |  | 性能，射频频谱使用1 |  |  |  |  |  |  |  |
|  |  |  |  |  | 以及环境条件 |  |  |  |  |  |  |  |
|  |  |  |  |  | C3连接足以保证安全 |  |  |  |  | 同样低。此外，使用 |  |  |
|  |  |  |  |  | 进行预期的操作。 |  |  |  |  |  |  |
|  |  | 标准 |  |  |  |  | 与 Low3相同。 |  | 用于 C2连接的持牌4频带 |  |  |
|  |  |  |  | 无人机远程驾驶员有 |  |  |  |  |
|  |  |  |  |  |  |  |  | 是必须的。 |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 持续监察环境监察及审核手 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | C3的性能，并确保 |  |  |  |  |  |  |  |
|  |  |  |  |  | 性能继续满足 |  |  |  |  |  |  |  |
|  |  |  |  |  | 运作规定2。 |  |  |  |  |  |  |  |
|  |  |  |  | 1对于诚信水平低的，未经许可 | | |  |  |  |  |  |  |
|  |  |  |  | 频带可能是可以接受的 | | |  |  |  |  |  |  |
|  |  |  |  | 在某些情况下，例如: | | |  |  |  |  |  |  |
|  | OSO # 06 |  |  | 申请人证明 | | |  |  |  |  |  |  |
|  | C3链接 |  |  |  | 与其他射频的一致性 | |  |  |  |  |  |  |
|  | 特征 |  |  |  | 频谱使用要求 | |  |  |  |  |  |  |
|  | (例如:。 |  |  |  | (例如欧盟: 指令2014/53/EU, | |  |  |  |  |  |  |
|  | 表演, |  |  |  | 美国: CFR 第47编第15部分 | |  |  |  | 4这确保了最低水平的 | |  |
|  | 频谱使用) |  |  |  | 联邦通讯局 | |  |  |  |  |
|  | **are** |  |  |  | 委员会(FCC)规则) | |  |  |  | 业绩，并不限于 | |  |
|  | 适当的 |  |  |  | 显示无人机设备是 | |  | 根据不同的操作方法，使用 |  | 持航空牌照的频带 | |  |
|  | 表示 |  |  |  | 符合这些要求 | |  | 持牌频带的数目可能会 |  | (例如手提电话的持牌波段 | |  |
|  | 行动 |  |  |  | (例如 FCC 标记) ，以及 | |  | 在某些情况下，使用 |  | 网络)。然而，有些 | |  |
|  |  | 评论 | | 保护机制的使用 | | |  | 非航空乐队(例如持牌乐队) |  | 操作可能需要使用 | |  |
|  |  |  |  |  | 防止干扰(例如, | |  | 的波段) |  | 分配给航空界的波段 | |  |
|  |  |  |  |  | 频率去冲突 | |  | 可以接受。 |  | 使用 C2连结的流动服务 | |  |
|  |  |  |  |  | 程序)。 | |  |  |  | (例如5030-5091 MHz)。 | |  |
|  |  |  |  | 2远程飞行员有持续的和 | | |  |  |  | 在任何情况下，许可证的使用 | |  |
|  |  |  |  | 及时查阅相关的 C3 | | |  |  |  | 频带需要授权。 | |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 可能影响安全的信息 | | |  |  |  |  |  |  |
|  |  |  |  | 对于只要求执行任务的 | | |  |  |  |  |  |  |
|  |  |  |  | 这个职业操守办公室的诚信水平低, | | |  |  |  |  |  |  |
|  |  |  |  | 这可以通过监控 | | |  |  |  |  |  |  |
|  |  |  |  | C2链路信号强度和 | | |  |  |  |  |  |  |
|  |  |  |  | 接收来自 UAS HMI 的警报，如果 | | |  |  |  |  |  |  |
|  |  |  |  | 信号变得太低。 | | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0

最终版/

**公开发布**

第9页

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | | |  |  |  |  | 保证水平 | |  |  |  |  |
|  | 无人机 | | |  |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  | C3链接的演示 |  |  |  |  |  |
|  | OSO # 06 |  |  |  |  |  |  |  | 性能符合 |  |  | 与中等水平相同。此外, |  |  |
|  |  |  |  |  | 考虑已定义的保证标准 |  |  | 认为适当的标准 |  |  |  |
|  | C3链接 |  |  | 标准 |  |  |  |  |  | 证据由合格的 |  |  |
|  |  |  |  | 在第9节(低保证水平) |  |  | 主管当局及/或 |  |  |  |
|  | 特征 |  |  |  |  |  |  |  | 第三方。 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 按照符合规定的方法 |  |  |  |
|  | (例如:。 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 获该当局接纳。 |  |  |  |  |  |
|  | 表演, |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 国家航空局(NAAs) | |  |  |  |  |
|  | 频谱使用) |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 标准及/或 | |  |  |  |  |
|  | **are** |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 他们认为符合规定的手段 | |  |  |  |  |
|  | 适当的 |  |  | 评论 |  |  |  |  |  |  |  |  |
|  |  |  | 不认识 | | |  | 附件 e | |  | 不认识 | |  |
|  | 表示 |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 在稍后的时间更新 | |  |  |  |  |
|  | 行动 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 的适当标准清单 | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | NAAs 提供的反馈意见。 | |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第10页

**OSO # 07-无人机检验(产品检验) ，以确保与操作规程的一致性**

该 OSO 的目的是确保用于操作的无人机符合用于支持操作的批准/授权的无人机数据。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | |  |  | 诚信水平 |  |  |
|  |  | 无人机 | |  | 很低 | 中等 | 很高 |  |
|  | OSO # 07 |  |  |  |  |  |  |  |
|  | 检查 |  | 标准 |  | 远程机组人员确保无人机处于安全运行状态，并符合批准的运行概念 | | |  |
|  | 无人机 |  |  |  |
|  | (产品 |  |  |  |  |  |  |  |
|  | 检查) |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | 以确保 |  |  |  | 1该准则的低、中和高稳健性之间的区别是通过 | | |  |
|  | 一致性 |  | 评论 | |  |
|  |  | 保证(见下表)。 |  |  |  |
|  | 对象 |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  | : ConOps |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 技术问题 | | |  |  |  |  | 保证水平 | |  |  |  |  |
|  |  | 无人机 | |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  | 准则 # 1 |  | 产品检验是有文件记录的 |  |  | 和低价一样。另外，产品 |  |  | 与媒介相同。此外, |  |  |
|  |  |  |  |  |  | 检验文件使用 |  |  |  |  |
|  |  |  |  | 制造商的帐目 |  |  |  |  | 产品检验通过 |  |  |
|  |  |  | (程序) |  |  |  | 清单。 |  |  |  |  |
|  | OSO # 07 |  |  | 建议(如适用)。 |  |  |  |  | 有资格的第三者。 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 检查 |  | 评论 | | 不认识 | | 不认识 | | |  | 不认识 | |  |
|  | 无人机 |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | (产品 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 培训大纲，包括 |  |  |  |  |  |
|  | 检查) |  |  |  |  |  |  |  |  | 有能力的第三方: |  |  |
|  | 以确保 |  |  |  | 远程机组人员接受了执行任务的训练 |  |  | 产品检验程序是 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | 一致性 |  | 标准 # 2 |  | 产品检验和培训 |  |  | 有空。 |  |  | 验证培训大纲。 |  |  |
|  |  | (训练) |  | 自行申报(附有证据) |  |  | 营办商提供 |  |  |  |
|  | 对象 |  |  |  |  |  |  | 验证远程机组人员 |  |  |
|  |  |  |  | 可用)。 |  |  | 基于能力的、理论上的和 |  |  |  |
|  | : ConOps |  |  |  |  |  |  |  | 能力。 |  |  |
|  |  |  |  |  |  |  | 实际训练。 |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  | |  |  |  |  |  | |  |
|  |  |  | 评论 | | 不认识 | | 不认识 | | |  | 不认识 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

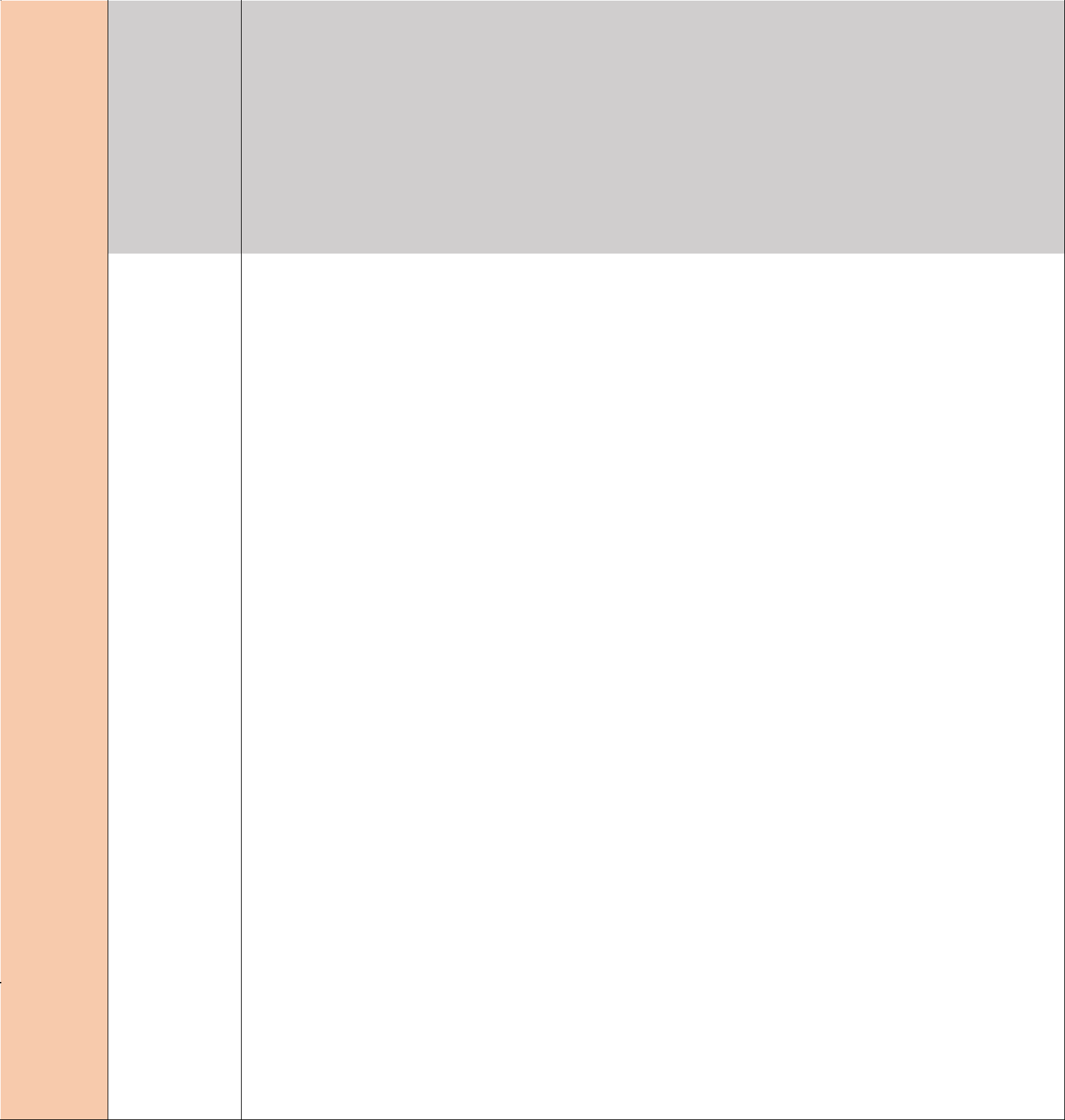
版本: 1.0最终/公开发布第11页

***3. 与业务程序有关的 OSOs***

*OSO # 08-制定、验证和遵守操作程序(以解决无人机的技术问题) OSO # 11-制定程序以处理支持无人机操作的外部系统的恶化情况 OSO # 14-制定、验证和遵守操作程序(以解决人为错误)*

*OSO # 21-操作程序的定义、验证和遵守(以解决不利的操作条件)*

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 操作程序 |  |  |  |  |  | 诚信水平 |  |  |  |  |
|  |  |  | 很低 |  |  | 中等 |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |



**OSO # 08 OSO # 11 OSO # 14和 OSO # 21**

适用于拟议操作的操作程序1被定义为最低限度包括以下要素:

飞行计划,

飞行前和飞行后检查,

在执行任务前和执行任务期间评估环境状况的程序(即实时评估) ,

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | o | 应对意外不利操作条件的程序(例如，当遇到冰 | | |  |  |
|  | 准则 # 1 |  |  |  |
|  |  |  |  | 不允许在结冰条件下进行操作) | | |  |  |
|  | (程序 |  |  |  |  |  |
|  |  |  | o | 正常程序, | | |  |  |
|  | 定义) |  |  |  |  |
|  |  |  | O 应急程序(应对异常情况) , | | | |  |  |
|  |  |  |  |  |  |
|  |  |  |  | O 紧急程序(以应付紧急情况) ，以及 | | | |  |  |
|  |  |  |  | o | 事故报告程序。 | | |  |  |
|  |  |  | 正常程序、应急程序和紧急程序编制在操作手册中。 | | | | |  |  |
|  |  |  |  | | |  |  |  |  |
|  |  |  | 支持 UAS 操作2的外部系统的局限性在操作手册中定义。 | | | | |  |  |
|  |  | 操作程序涵盖无人机本身及支援无人机操作的任何外部系统的损坏情况。 | | | | | | |  |
|  |  | 2在本评估范围内，支持无人机操作的外部系统被定义为尚未成为无人机系统一部分的系统 | | | | | | |  |
|  |  | 无人机系统，但习惯于: | | | | | | |  |
|  |  | *•* | | 发射/起飞无人机, | | | | |  |
|  |  | *•* | | 进行飞行前检查, | | | | |  |
|  |  | *•* | | 将 UA 保持在其运作容量内(例如全球导航卫星系统、卫星系统、航空交通管理、 UTM)。 | | | | |  |
|  | 评论 | 在失去操作控制后激活/使用的外部系统被排除在本定义之外。 | | | | | | |  |
|  |  |  |  |  |  |  |  |  |

*3为妥善处理操作所需的外部系统恶化问题，建议:*

*识别这些“外部系统”,*

*确定导致操作失控的”外部系统”恶化模式(例如全球导航卫星系统完全失效、全球导航卫星系统漂移、延迟问题等) ，说明如何检测外部系统/设施的这些恶化模式,*

*描述检测到故障时使用的程序(例如启动紧急恢复能力，切换到手动控制...)。*

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | 操作程序很复杂 |  |  |  |  |  |  |  |
|  | 标准 # 2 |  |  |  | 而且可能会危及 |  |  | 应急/紧急程序 |  |  |  |  |
|  |  |  |  | 船员的反应能力，提高 |  |  | 需要用遥控器手动控制 |  |  |  |  |
|  | (程序 |  |  |  |  |  |  | 操作程序很简单。 |  |  |
|  |  |  |  | 远程船员的工作量及/或 |  |  | 当无人机系统通常是 |  |  |  |
|  | 复杂性) |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 与其他实体的相互作用(例如。 |  |  | 自动控制。 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 自动取款机。 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 2. 这个问题仍在讨论之中 |  |  |  |  |
|  |  |  |  |  |  |  |  | 所有无人机都有一个模式，在这个模式下，飞行员 |  |  |  |  |
|  | 评论 | |  | 不认识 | | |  | 可以直接控制表面; |  | 不认识 | |  |
|  |  |  | 此外，有些人声称 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 需要相当高的技能才能做到 |  |  |  |  |
|  |  |  |  |  |  |  |  | 更糟糕的事。 |  |  |  |  |
|  |  |  |  |  | | |  |  |  |  |  |  |
|  |  |  |  |  | 至少，操作程序 |  |  |  |  |  |  |  |
|  |  |  |  |  | 提供: |  |  |  |  |  |  |  |
|  | 准则 # 3 |  |  |  | 明确的分配和 |  |  |  |  | 与媒介相同。此外, |  |  |
|  | (考虑 |  |  |  |  | 操作程序需要人力 |  | 远程船员3接收船员 |  |  |
|  |  |  |  | 任务分配 |  |  |  |  |  |
|  | 潜在的人类 |  |  |  |  |  | 考虑错误。 |  | 资源管理(CRM)4 |  |  |
|  |  |  |  | 内部核对表，以确保 |  |  |  |  |  |
|  | 错误) |  |  |  |  |  |  |  | 训练。 |  |  |
|  |  |  |  | 员工是否足够 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 执行指派的任务。 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 3在 SORA 的范围内，术语 | |  |
|  |  |  |  |  |  |  |  |  |  | “ Remote crew”指的是任何人 | |  |
|  |  |  |  |  |  |  |  |  |  | 参与了这次任务。 | |  |
|  | 评论 | |  | 不认识 | | |  | 不认识 |  | 4客户关系管理培训的重点是有效的 | |  |
|  |  |  |  | 使用所有远程机组人员以确保安全 | |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 和高效率的操作，减少错误, | |  |
|  |  |  |  |  |  |  |  |  |  | 避免压力和增加 | |  |
|  |  |  |  |  |  |  |  |  |  | 效率。 | |  |

附件 e

版本: 1.0最终/公开发布第12页

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 操作程序 | | | |  |  |  |  |  | 保证水平 | |  |  |  |  |  |
|  |  |  |  |  |  | 很低 |  |  |  | 中等 |  |  | 很高 |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 操作程序如下 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 标准的验证 |  |  |  |  |  |  |
|  |  |  |  |  |  | 操作程序没有 |  |  |  | 认为足够的 |  |  | 和中号一样，另外: |  |  |  |
|  |  |  |  |  |  |  |  |  | 主管当局及/或 |  |  |  |  |  |
|  |  |  |  |  |  | 需要根据 |  |  |  | 按照... 的方法 |  |  | 进行飞行测试以验证 |  |  |  |
|  |  |  |  |  |  | 标准或合规手段 |  |  |  | 可接受的 |  |  |  |  |  |
|  |  |  |  |  |  | 认为足够的 |  |  |  | 权威1。 |  |  | 程序及清单 |  |  |  |
|  |  |  |  |  |  | 主管当局。 |  |  |  |  |  |  | 覆盖整个飞行信封 |  |  |  |
|  | OSO # 08, |  |  | 标准 |  |  |  |  |  |  |  |  |
|  |  |  |  | 运作的充分性 |  |  |  | 应变及应变措施的充分性 |  |  | 或被证明是保守的。 |  |  |  |
|  | OSO # 11, |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 程序，但 |  |  |  | 紧急程序已被证实 |  |  | 程序，清单，航班 |  |  |  |
|  | OSO # 14职业操作系统 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 紧急程序 |  |  |  | 通过: |  |  | 测试和模拟验证 |  |  |  |
|  | 和 OSO |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 经过测试。 |  |  |  | O 专门的飞行测试，或 |  |  | 由合格的第三方提供。 |  |  |  |
|  | 第21位 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | o 模拟提供 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 模拟被证明是有效的 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 为了预期的目的 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 产生积极的结果。 |  |  |  |  |  |  |

*国家航空当局(NAAs)可界定标准及/或*

|  |  |  |  |
| --- | --- | --- | --- |
| 评论 | 不认识 | 他们认为足够的合规手段。《津贴管理条例》附件 e 将 |  |
| 在稍后时间更新了一份基于《基本法》的适当标准清单 |  |
|  |  |  |
|  |  | 提供的反馈意见。 |  |

附件 e

版本: 1.0最终/公开发布第13页

***4. OSOs 与 Remote crew training 相关***

*OSO # 09- 远程机组人员经过培训，能够及时控制异常和紧急情况(即无人机的技术问题)*

*远程机组人员受过培训，目前能够控制异常和紧急情况(即人为错误)*

申请人须提供以能力为本的理论及实务训练:

适合于批准的操作，以及

包括能力要求和培训经常性。

全体远程机组人员(即任何参与行动的人员)应接受与其职责相关的能力为本、理论和实践训练(例如飞行前视察、地面设备处理、气象条件评估等)。

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 远程摄制组 | | |  |  |  |  | 诚信水平 |  |  |
|  | 胜任能力 | | |  |  | 很低 |  | 中等 | 很高 |  |
|  |  |  |  |  | 以能力为本的理论和实践培训确保了以下方面的知识: | | | |  |  |
|  |  |  |  |  | A) | 无人机规例 | |  |  |  |
|  |  |  |  |  | B) | 无人机空域操作原则 | |  |  |  |
|  |  |  |  |  | C) | 航空技术和航空安全 | |  |  |  |
|  | OSO # 09，OSO |  | 标准 |  | D) | 人类的性能限制 | |  |  |  |
|  |  |  | E) | 气象学 | |  |  |  |
|  |  |  |  |  |  |  |
|  | # 15和 OSO |  |  |  |  |  |  |
|  |  |  |  | F) | 导航/图表 | |  |  |  |
|  | 第22名 |  |  |  |  |  |  |
|  |  |  |  |  | G) | UA 知识 | |  |  |  |
|  |  |  |  |  | H) | 操作程序 | |  |  |  |
|  |  |  |  |  | 足以进行手术 | | |  |  |  |
|  |  |  |  |  | 1上述不同科目所涵盖范围的详情将由 JARUS WG1在2019年提供。 | | | | |  |
|  |  |  | 评论 | | 2区分该准则的低、中和高三个稳健性水平是通过 | | | | |  |
|  |  |  |  |  | 保证(见下表)。 | | |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 远程机组人员的能力 | | |  |  |  |  | 保证水平 | |  |  |  |  |
|  |  |  |  |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  | 培训课程大纲可供参考。 |  |  | 有能力的第三方: |  |  |
|  | OSO # 09，OSO |  | 标准 |  | 训练是自我声明的(有证据的) |  |  | 营办商提供 |  |  | 验证培训大纲。 |  |  |
|  | # 15和 OSO |  |  | 可用)。 |  |  | 基于能力的，理论上的 |  |  |  |
|  |  |  |  |  |  |  | 验证远程机组人员 |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 和实际训练。 |  |  |  |
|  | 第22名 |  |  |  |  |  |  |  |  | 能力。 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 | |  | 不认识 | |  | 不认识 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第14页

***5. 与 Safe 设计相关的 OSOs***

*OSO # 10-从技术问题中恢复安全*

*OSO # 12-UAS 旨在管理支持 UAS 运行的外部系统的恶化*

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操作时发生死亡的风险来补充技术安全性要求。

在本评估范围内，支持无人机操作的外部系统被定义为尚未成为无人机系统一部分的系统，但用于:

发射/起飞无人机,

进行飞行前检查,

将 UA 保持在其运作容量内(例如全球导航卫星系统、卫星系统、航空交通管理、 UTM)。

在失去操作控制后激活/使用的外部系统被排除在本定义之外。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  | 诚信水平 | | |  |  |  |  |
|  |  |  |  |  | 很低 | | |  |  | 中等 | |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  | 在人口稠密地区或 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 人群聚集: | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 可以合理地预期 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 致命事件不会发生在任何 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 无人机的单次故障或任何其他故障 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 在人口稠密地区或 | | |  | 外部系统支持 | | |  |  |  |  |  |
|  |  |  |  |  | 人的集会，可以是 | | |  | 行动。 | | |  |  |  |  |  |
|  |  |  | 标准 |  | 有理由相信死亡会 | | |  | 软件(SW)和航空电子 | | |  |  | 和中号一样 |  |  |
|  |  |  |  | 不会发生在任何 | 可能1失败2 | 的 |  | 硬件(AEH)的开发 | | |  |  |  |  |
|  |  |  |  |  | 无人机或任何外部系统 | | |  | 错误可能直接导致故障 | | |  |  |  |  |  |
|  |  |  |  |  | 支持操作。 | | |  | 以这种方式影响操作 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 以致可以合理地预期 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 将会发生的死亡发展成为 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 认为足够的标准 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 主管当局及/或 | | |  |  |  |  |  |
|  | OSO # 10 OSO # 10 |  |  |  |  |  |  |  | 按照符合规定的方法 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 该当局可接受的。 | | |  |  |  |  |  |
|  | & OSO # 12 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 3某些结构或机械 | | | | |  |  |  |  |
|  |  |  |  |  | 1就本评估而言, | | | 不合格者可被排除在否 | | | | |  |  |  |  |
|  |  |  |  |  | 单一破坏准则，如果可以显示 | | | | |  |  |  |  |
|  |  |  |  |  | 术语“可能”应该是 | | |  |  |  |  |
|  |  |  |  |  | 这些机械部件 | | | | |  |  |  |  |
|  |  |  |  |  | 以定性的方式解释为, | | |  |  |  |  |
|  |  |  |  |  | 设计得符合标准 | | | | |  |  |  |  |
|  |  |  |  |  | 预期会发生一次或多次 | | |  |  |  |  |
|  |  |  |  |  | 足够的主管当局 | | | | |  |  |  |  |
|  |  |  |  |  | 在整个系统/运作期间 | | |  |  |  |  |
|  |  |  |  |  | 及/或按照 | | | | |  |  |  |  |
|  |  |  |  |  | 无人机系统」。 | | |  |  |  |  |
|  |  |  |  |  | 该当局可接受的遵守情况 | | | | |  |  |  |  |
|  |  |  | 评论 | |  |  |  |  |  |  |  |
|  |  |  | 2某些结构或机械 | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 4国家航空局(NAAs) | | | | |  |  |  |  |
|  |  |  |  |  | 故障可能被排除在 | | |  |  |  |  |
|  |  |  |  |  | 标准及/或 | | | | |  |  |  |  |
|  |  |  |  |  | 标准是否可以证明这些 | | |  |  |  |  |
|  |  |  |  |  | 他们认为符合规定的手段 | | | | |  |  |  |  |
|  |  |  |  |  | 机械零件被设计成 | | |  |  |  |  |
|  |  |  |  |  | 附件 e | | | | |  |  |  |  |
|  |  |  |  |  | 航空业最佳做法。 | | |  |  |  |  |
|  |  |  |  |  | 在稍后的时间更新 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  | 适当标准的清单 | | | | |  |  |  |  |
|  |  |  |  |  |  |  |  | 提供的反馈意见。 | | | | |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | 保证水平 | |  |  |  |  |
|  |  |  |  |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  | 设计和安装鉴定是 |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 特别是，这个评估 |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 显示: |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 设计和安装特点 |  |  | 与低水平相同。此外, |  |  |  |  |  |
|  |  |  |  |  | (独立、分离和 |  |  |  |  | 与中等水平相同。此外, |  |  |
|  |  |  |  |  |  |  | 声称的完整性是由 |  |  |  |  |
|  |  |  | 标准 |  | 冗余) ，以满足低 |  |  |  |  | 有能力的第三方验证水平 |  |  |
|  | OSO # 10 OSO # 10 |  |  |  |  | 分析及/或测试数据 |  |  |  |  |
|  |  |  | 完整性标准; |  |  |  |  | 正直的声明。 |  |  |
|  | & OSO # 12 |  |  |  |  |  | 支持证据。 |  |  |  |  |
|  |  |  |  | 相关的特定风险 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 冰雹(例如冰雹、冰、雪、, |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 电磁干扰...) |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 不得侵犯独立 |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 如果有的话。 |  |  |  |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 | |  | 不认识 | | 不认识 | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第15页

***6. 支持无人机操作的外部系统恶化***

OSO # 13-支持无人机操作的外部服务足以满足操作要求

就《空中交通管理条例》及本《空中交通管理条例》而言，「支援无人机运作的外部服务」一词，包括航班安全所需的任何服务提供者，例如:。

通信服务提供商(CSP),

UTM 服务提供商，..。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 环境恶化 | | | |  |  |  |  |  | 诚信水平 | |  |  |  |  |  |
|  | 外部系统 | | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 支持 UAS | | | |  | 很低 |  |  |  | 中等 |  |  | 很高 |  |  |  |
|  | 行动超越 | | | |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 无人机的控制 | | | |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 职业安全办公室 # 13 |  |  |  |  | 申请人确保为保障航班安全而提供的任何外部服务的表现水平 | | | | | | | |  |  |  |
|  |  |  |  |  | 是否足以进行预期的操作。 | |  |  |  |  |  |  |  |  |  |
|  | 外部 |  |  | 标准 |  |  |  |  |  |  |  |  |  |  |
|  | 服务 |  |  |  | 如果外部提供的服务需要经营者和服务提供者之间进行沟通，申请者应确保 | | | | | | | |  |  |  |
|  |  |  |  |  |  |  |  |
|  | 支援 |  |  |  |  | 有有效的沟通来支持服务的提供。 | | | | | |  |  |  |  |  |
|  | 无人机 |  |  |  |  | 定义了申请者和外部服务提供者之间的角色和职责。 | | | | | | | |  |  |  |
|  | 操作 |  |  |  |  |  |  |  |  |  |  | 订约承办服务的要求 | | |  |  |
|  | **are** |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 服务供应商可以派生 | | |  |  |
|  | 足以 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 | | 不认识 | | | | 国际民用航空组织标准及 | | |  |  |
|  | 是的 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 推荐做法-SARPS | | |  |  |
|  | 行动 |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | (目前正在发展中)。 | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | |  |  | |  |  |  |  |  | |  |  |  |  |  |
|  | 环境恶化 | | | | |  |  |  |  | 保证水平 | |  |  |  |  |  |
|  | 外部系统 | | | | |  |  |  |  |  |  |  |  |  |  |  |
|  | 支持 UAS | | | | | 很低 | |  |  | 中等 | |  | 很高 | |  |  |
|  | 行动超越 | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | 无人机的控制 | | | | |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 申请人有证明文件 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 所要求的表现水平 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 任何外部提供的服务 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 为了飞行的安全需要 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 的全部时间内都可以达到 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 任务。 | |  |  |  |  |  |
|  | 职业安全办公室 # 13 | |  |  |  |  |  |  |  | 这可以采取服务的形式 | |  | 和中号一样，另外: | |  |  |
|  |  |  |  | 申请人声明 | |  |  |  | 外部证据 | |  |  |
|  |  |  |  |  |  | 水平协议(SLA)或任何官员 | |  |  |  |
|  | 外部 | |  |  |  |  |  |  |  |  |
|  |  |  |  | 要求的任何性能水平 | |  |  |  | 提供的服务表现 | |  |  |
|  |  |  |  |  |  | 承诺之间的承诺 | |  |  |  |
|  | 服务 | |  |  |  |  |  |  |  |  |
|  |  |  |  | 外部提供的必要服务 | |  |  |  | 是通过 | |  |  |
|  |  | 标准 | |  |  | 服务供应商及申请人 | |  |  |  |
|  | 支援 | |  |  |  |  |  |  |
|  |  | ，以确保飞行安全 | |  |  |  | 示威游行。 | |  |  |
|  |  |  |  | 服务的相关方面 | |  |  |  |
|  | 无人机 | |  |  |  |  |  |  |  |  |
|  |  |  |  | (没有必要的证据 | |  |  |  | 有能力的第三方 | |  |  |
|  |  |  |  |  |  | (包括质量、可用性、, | |  |  |  |
|  | 行动是 | |  |  |  |  |  |  |  |  |
|  |  |  |  | 可用)。 | |  |  | 职责)。 | |  | 证实所声称的水平 | |  |  |
|  | 足以 | |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 申请人有办法监察 | |  | 正直。 | |  |  |
|  | 行动 | |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 对外提供的服务 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 影响飞行关键系统，并采取 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 适当的行动，如果实时 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 表现可能导致损失 | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 控制整个行动。 | |  |  |  |  |  |
|  |  |  |  |  | |  | |  |  |  | |  |  | |  |  |
|  |  |  |  | 评论 | | 不认识 | |  |  | 不认识 | |  | 不认识 | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第16页

***7. 人为错误***

OSO # 16-多人协调

(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 |  |  |  |  |
|  |  | 很低 |  |  |  |  | 中等 |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 确保船员之间协调的程序和健全有效的沟通渠道是(是) | | | | | | | |  |  |
|  |  |  | 准则 # 1 |  | 可用且最低覆盖率: | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | (程序) |  | 分配给船员的任务, | | |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 建立循序渐进的沟通机制 | | | | | |  |  |  |  |
|  |  |  | 评论 | | 1该准则的低、中和高稳健性之间的区别是通过 | | | | | | | | |  |
|  |  |  | 保证(见下表)。 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 标准 # 2 |  | Remote Crew training covers multi 远程船员培训涵盖多个 | |  |  | 和 Low 一样，另外，遥控器 | |  |  |  |  |
|  |  |  |  |  |  | Crew2接收 Crew 资源 | |  | 和中号一样。 |  |  |
|  |  |  | (训练) |  | 船员协调 |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 管理(CRM)3培训。 | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 2在 SORA 的背景下，术语 | |  |  |  |  |
|  |  |  |  |  |  |  |  |  | “ Remote crew”指的是任何人 | |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 参与了这次任务。 | |  |  |  |  |
|  |  |  | 评论 | | 不认识 |  |  |  | 3客户关系管理培训的重点是有效的 | |  | 不认识 | |  |
|  | OSO # 16 Multi |  |  |  |  |  |  |  | 使用所有远程机组人员以确保安全 | |  |  |  |  |
|  |  |  | |  |  |  |  | 和高效率的操作，减少错误, | |  |  |  |  |
|  | 全体船员 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  | 避免压力和增加 | |  |  |  |  |
|  | 协调 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  | 效率。 | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 通讯设备符合 | |  | 通讯设备是多余的 |  |  |
|  |  |  | 准则 # 3 |  |  |  |  |  | 认为适当的标准 | |  | 并符合所考虑的标准 |  |  |
|  |  |  |  |  |  |  |  | 主管当局及/或 | |  | 足够的主管当局 |  |  |
|  |  |  | (通讯 |  | 不认识 |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 按照... 的方法 | |  | 及/或按照 |  |  |
|  |  |  | 设备) |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 可接受的 | |  | 可接受的 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 权威4。 | |  | 权威6。 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | 这意味着提供额外的 | |  |
|  |  |  |  |  |  |  |  |  | 4国家航空局(NAAs) | |  | 处理故障情况的装置 | |  |
|  |  |  |  |  |  |  |  |  | 标准及/或 | |  | 第一个装置。 | |  |
|  |  |  |  |  |  |  |  |  | 他们认为符合规定的手段 | |  | 6个国家航空局 | |  |
|  |  |  | 评论 | | 不认识 |  |  |  | 附件 e | |  | 标准及/或 | |  |
|  |  |  |  |  |  | 在稍后的时间更新 | |  | 他们认为符合规定的手段 | |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 适当标准的清单 | |  | 附件 e | |  |
|  |  |  |  |  |  |  |  |  | 提供的反馈意见。 | |  | 在稍后的时间更新 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  | 适当标准的清单 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  | 提供的反馈意见。 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 人为错误 | | | |  |  |  |  |  | 保证水平 |  |  |  |  |
|  | 很低 |  |  |  |  | 中等 |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 程序根据 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 认为适当的标准 |  |  |  |  |
|  |  |  |  |  | 程序不需要 |  |  |  |  | 主管当局及/或 |  | 和中号一样，另外: |  |  |
|  |  |  |  |  |  |  |  |  | 按照 |  |  |  |
|  |  |  |  |  | 标准的验证 | | |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 可接受的 |  | 进行飞行测试以验证 |  |  |
|  |  |  |  |  | 或者是一种服从的方式 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 权威1。 |  |  |  |
|  |  |  | 准则 # 1 | | 认为足够的 | | |  |  |  | 程序涵盖全部 |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  | 主管当局。 |  |  |  |  | 程序的充分性 |  | 飞行信封或被证明是 |  |  |
|  |  |  | (程序) | |  |  |  |  |  |  |  |
|  |  |  | 程序的充分性 | | |  |  |  | 保守。 |  |  |
|  |  |  |  |  |  |  | 通过以下证明: |  |  |  |
|  |  |  |  |  | 并声明检查表。 |  |  |  |  |  | 程序、飞行测试及 |  |  |
|  |  |  |  |  |  |  |  |  | O 专门的飞行测试，或 |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 模拟是由一个验证 |  |  |
|  |  |  |  |  |  |  |  |  |  | O 模拟，提供 |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 有资格的第三者。 |  |  |
|  |  |  |  |  |  |  |  |  |  | 模拟被证明有效 |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 的预期目的 |  |  |  |  |
|  | OSO # 16 Multi |  |  |  |  |  |  |  |  | 正面结果。 |  |  |  |  |
|  | 全体船员 |  |  |  |  |  |  |  |  | 1个国家航空局 |  |  |  |  |
|  | 协调 |  |  |  |  |  |  |  |  | 标准及/或 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 他们认为符合规定的手段 |  |  |  |  |
|  |  |  | 评论 | | 不认识 |  |  |  |  | 附件 e |  | 不认识 | |  |
|  |  |  |  |  |  |  |  |  |  | 在稍后的时间更新 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 的适当标准清单 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | NAAs 提供的反馈意见。 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 培训课程大纲可供参考。 |  | 有能力的第三方: |  |  |
|  |  |  | 标准 # 2 | | 训练是自我声明的(有证据的) | | |  |  | 营办商提供 |  | 验证培训大纲。 |  |  |
|  |  |  | (训练) | | ) |  |  |  |  | 基于能力的、理论上的和 |  |  |
|  |  |  |  |  |  |  |  | 验证远程机组人员 |  |  |
|  |  |  |  |  |  |  |  |  |  | 实际训练。 |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 能力。 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 |  |  |  |  | 不认识 |  | 不认识 | |  |
|  |  |  |  | |  |  |  |  |  |  |  |  |  |  |
|  | 附件 e | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 版本: 1.0 | | | 最终/公开发布 | | | | |  | 第17页 | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 人为错误 | |  |  |  |  | 保证水平 | |  |  |  |  |
|  |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 准则 # 3 |  |  |  |  |  |  |  |  |  |  |
|  |  | (通讯 |  | 考虑第9节中定义的标准 | |  |  |  |  |  |  |  |
|  |  | 设备) |  |  |  |  |  |  |  |  |  |  |
|  |  | 评论 | | 不认识 | | 不认识 |  |  |  | 不认识 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第18页

**OSO # 17- 远程工作人员适合操作**

为了这次评估的目的，“适合操作”这个表达应该被解释为身体和精神上适合执行任务和安全履行责任。

疲劳和压力是导致人为错误的因素。因此，为了确保警惕性保持在令人满意的安全水平，可以考虑以下几点:

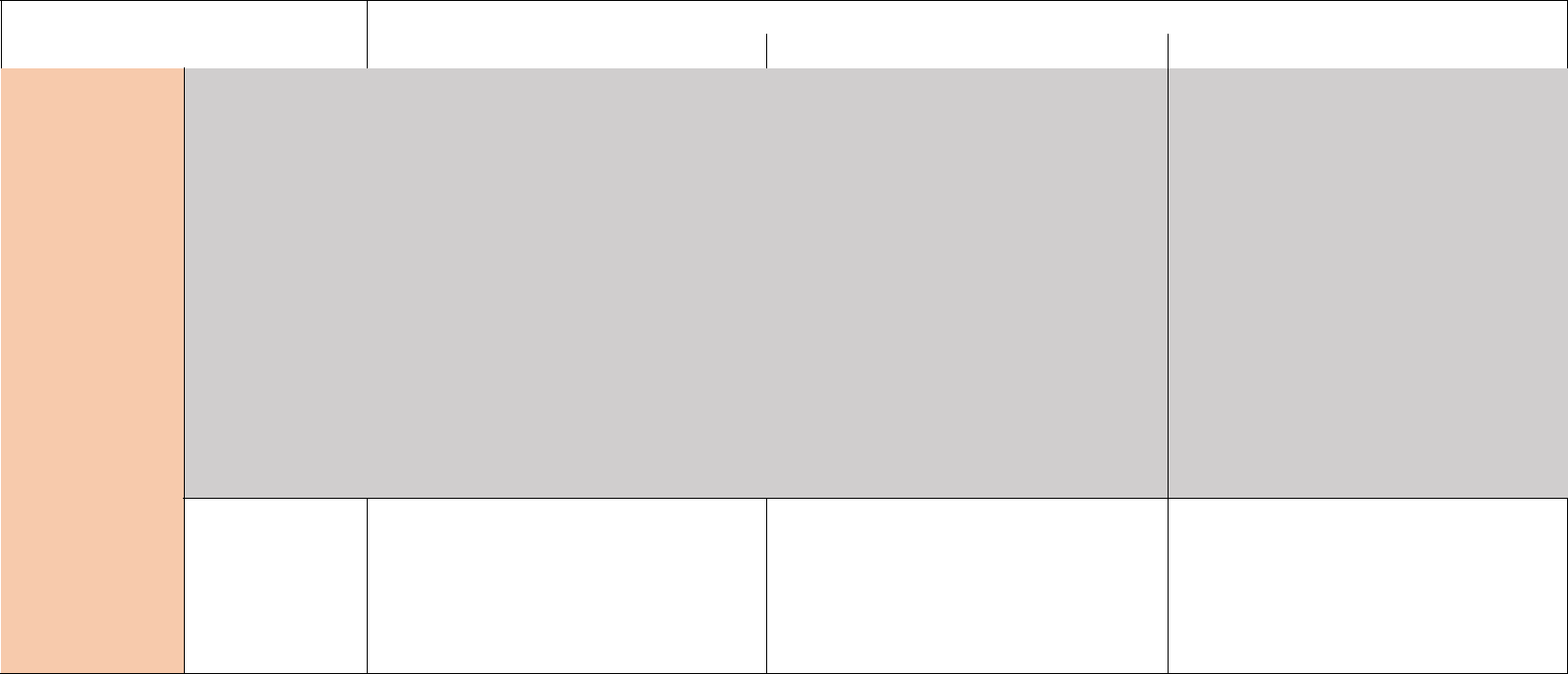
远程船员值班时间;

定期休息;

休息时间;

移交/接管程序。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 人为错误 | | |  |  |  |  | 诚信水平 | |  |  |  |  |
|  |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 和 Low 一样，另外: |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 职责，飞行职责和休息 |  |  | 和中号一样，另外: |  |  |
|  |  |  |  |  | 申请人有一个政策，定义如何 |  |  | 远程摄制组的时间是 |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 远程机组人员身体健康, |  |  |
|  |  |  |  |  |  |  | 由申请人定义，并 |  |  |  |  |
|  |  |  |  |  | 远程船员可以声明 |  |  |  |  |
|  |  |  | 标准 |  |  |  |  |  | 疲劳风险管理。 |  |  |
|  | OSO # 17 |  |  |  |  | 足以进行手术。 |  |  |  |  |
|  |  |  | 他们以前就适合做手术了 |  |  |  |  | 系统(FRMS)已经就位 |  |  |
|  | 远程摄制组才是 |  |  |  |  |  | 操作员定义 |  |  |  |  |
|  |  |  |  | 进行任何行动。 |  |  |  |  | 管理任何升级 |  |  |
|  | 适合做手术 |  |  |  |  |  | 的适当要求 |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 当值/飞行当值时间。 |  |  |
|  |  |  |  |  |  |  |  | 远程机组人员操作 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 无人机。 |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 | | 不认识 | | | 不认识 | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 人为错误 | | |  |  |  |  |  |  |  | 保证水平 | | |  |  |  |  |  |
|  |  |  |  | 很低 |  |  |  |  | 中等 |  |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 和 Low 一样，另外: | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 遥控机组职责、飞行职责和 | |  |  |  |  | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | 和中号一样，另外: |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 休息时间政策是 | |  |  |  | 考虑到医疗标准 |  |  |
|  |  |  |  |  |  |  |  |  |  |  | : 记录在案。 | |  |  |  | 由合资格人士提供足够的 |  |  |
|  |  |  |  |  |  |  | 政策如何定义 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 远程机组人员工作周期是 | |  |  |  | 的权限和/或手段 |  |  |
|  |  |  |  |  |  |  | 远程机组人员宣布 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 登录，并至少覆盖: | |  |  |  | 可接受的 |  |  |
|  |  |  |  |  |  |  | 适合操作(在操作前) |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | o | 当远程摄制组 |  |  |  | 权威机构1建立和一个 |  |  |
|  |  |  |  |  |  |  | 都有记录。 |  |  |  |  |  |  |  |  |
|  |  |  | 标准 |  |  |  |  |  |  |  | 会员当值日 |  |  |  | 有能力的第三方核实 |  |  |
|  |  |  |  |  | 远程机组人员合格声明 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 开始, |  |  |  | 远程机组人员身体状况良好。 |  |  |
|  |  |  |  |  |  |  | 操作(在操作之前) |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | o | 当远程摄制组 |  |  |  | 有能力的第三方确认 |  |  |
|  | OSO # 17 |  |  |  |  |  | 定的政策 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 会员免受 |  |  |  | 当值/飞行当值时间。 |  |  |
|  | 远程摄制组才是 |  |  |  |  |  | 申请人。 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 职责, |  |  |  | 如果使用 FRMS，它将被验证 |  |  |
|  | 适合做手术 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 的休息时间 | |  |  |  | 并由一名合资格的 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  | 职责周期。 | |  |  | 第三方。 | |  |

有证据表明远程机组人员适合操作无人机。

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | 1个国家航空局 |
|  |  |  | 标准及/或 |
|  |  |  | 他们认为符合规定的手段 |
| 评论 | 不认识 | 不认识 | 附件 e |
|  |  |  | 在稍后的时间更新 |
|  |  |  | 的适当标准清单 |
|  |  |  | NAAs 提供的反馈意见。 |

附件 e

版本: 1.0最终/公开发布第19页

**OSO # 18- 自动保护飞行包线不受人为错误的影响**

无人驾驶飞机(UA)设计了一个飞行包线，描述了其最低和最高操作速度以及操作结构强度方面的安全性能极限。

飞行包线的自动保护是为了防止远程飞行员在飞行包线外操作 UA。如果申请人证明远程飞行员不在环路中，则此 OSO 不适用。

实施这种自动保护功能的无人机系统将确保无人机在可接受的飞行包线范围内运行，即使在远程驾驶员控制输入不正确(人为错误)的情况下也是如此。

没有自动保护功能的无人机容易受到不正确的远程驾驶员控制输入(人为错误)的影响，如果超过设计的飞机性能限制，可能导致失去 UA。

飞行包线保护的失败或开发错误在 OSOs # 5，# 10和 # 12中得到解决。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 人为错误 | | |  |  |  |  |  |  |  |  |  | 诚信水平 | |  |  |  |  |  |
|  |  |  | 很低 | | | |  |  |  | 中等 |  |  | 很高 | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 无人机飞行控制系统 | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 包括自动保护 | | | | |  |  |  |  |  |  |  |  |  |  |
|  | OSO # 18 |  |  |  | 飞行信封，防止遥控器 | | | | |  |  | UAS 飞行控制系统包含了飞行的自动保护功能 | | | | | |  |  |
|  |  |  |  | 飞行员不做任何单一的输入 | | | | |  |  | 信封，以确保无人机保持在飞行信封内，或确保及时 | | | | | |  |  |
|  | 自动的 |  | 标准 |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 在正常操作条件下 | | | | |  |  | 返回到设计的操作飞行包线后，远程飞行员 | | | | | |  |  |
|  | 保障 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 错误1 | | |  |  |  |  |  |
|  |  |  |  | 会导致无人机超速飞行 | | | | |  |  |  |  |  |  |  |
|  | 航班 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 信封或防止其恢复 | | | | |  |  |  |  |  |  |  |  |  |  |
|  | 的信封 |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 及时赶到。 | | | | |  |  |  |  |  |  |  |  |  |  |
|  | 人为错误 |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  | |  |
|  |  |  | 评论 | | 不认识 | | | | | |  | 1这个标准的中等和高度健壮性之间的区别 | | | | | | |  |
|  |  |  |  | 是通过保证水平实现的(见下表)。 | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 人为错误 | | |  |  |  |  | 保证水平 | |  |  |  |  |
|  |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 飞行的自动保护 |  |  |  |  |  |
|  |  |  |  |  | 飞行的自动保护 |  |  | 信封已经发展到 |  |  |  |  |  |
|  |  |  |  |  | 信封是在 |  |  | 认为适当的标准 |  |  | 和中号一样，另外还有证据 |  |  |
|  |  |  | 标准 |  | 房子或盒子外面(例如使用 |  |  | 主管当局及/或 |  |  |  |  |
|  | OSO # 18 |  |  | 从架子上取下的元素), |  |  | 按照... 的方法 |  |  | 由有能力的第三方验证。 |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 自动的 |  |  |  | 没有遵循特定的标准。 |  |  | 可接受的 |  |  |  |  |  |
|  | 保障 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 权威。 |  |  |  |  |  |
|  | 航班 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 信封 |  |  |  |  |  | 国家航空局(NAAs) | | |  |  |  |  |
|  | 来自人类 |  |  |  |  |  | 标准及/或 | | |  |  |  |  |
|  | 错误 |  |  |  |  |  | 他们认为符合规定的手段 | | |  |  |  |  |
|  |  |  | 评论 | | 不认识 | | 附件 e | | | 不认识 | | |  |
|  |  |  |  |  | 在稍后的时间更新 | | |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 的适当标准清单 | | |  |  |  |  |
|  |  |  |  |  |  |  | NAAs 提供的反馈意见。 | | |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第20页

**OSO # 19-从人为错误中安全恢复**

本办公室处理人为错误的风险，如不及时预防、检测和恢复，可能会影响操作的安全。

错误可能来自任何参与操作的人员

一个例子可能是人为错误，导致有效负载加载不正确，在操作过程中有从 UA 脱落的风险。

另一个例子可能是没有延长天线杆的人为错误，减少了 C2链路覆盖。

注意: 航班信封保护不包括在这个 OSO 中，因为它是 OSO # 18特别涵盖的。

这个 OSO 包括:

程序及名单,

培训及

无人机系统设计，即系统探测及/或修复人为错误(例如安全别针、使用确认功能、燃油或能源消耗监察功能等)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 人为错误 | | |  |  |  |  |  | 诚信水平 | | |  |  |  |  |  |
|  |  | 很低 |  |  |  |  | 中等 |  |  | 很高 | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 减少任何参与特派团人员可能出现人为错误的风险的程序和清单如下: | | | | | | | | | |  |  |
|  |  |  | 准则 # 1 |  | 定义和使用。 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | (程序及 |  | 程序至少规定: | | | |  |  |  |  |  |  |  |  |
|  |  |  | 检查清单) |  |  |  |  |  |  |  |  |  |
|  |  |  |  | 明确的任务分配和分配, | | | | | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 内部清单，以确保员工充分执行分配的任务。 | | | | | | |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 |  |  |  | 不认识 | | |  | 不认识 | | |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  | |  | | |  | |  | |  |  |  |  |  |
|  |  |  | 标准 # 2 |  | Remote crew 1受过程序和清单方面的训练。 | | | | | | |  |  |  |  |  |
|  |  |  | (训练) |  | Remote Crew 1接受 Crew Resource Management (CRM)2的培训 | | | | | | |  |  |  |  |  |
|  |  |  |  |  | 1在 SORA 的范围内,”远程机组人员”一词是指参与任务的任何人员。 | | | | | | | | | | |  |
|  |  |  |  |  | 客户关系管理培训的重点是有效使用所有远程机组人员，以确保安全和有效的操作，减少错误, | | | | | | | | | | |  |
|  | 职业安全办公室 # 19 |  | 评论 | | 避免压力，提高效率。 | | | |  |  |  |  |  |  |  |  |
|  |  |  |  | 3该准则的低、中和高鲁棒性之间的区别是通过 | | | | | | | | | | |  |
|  | 安全恢复 |  |  |  |  |
|  |  |  |  | 保证(见下表)。 |  |  |  |  |  |  |  |  |  |  |  |
|  | 来自 Human |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 错误 |  |  |  |  |  |  |  | 系统检测和/或恢复 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 从人为错误发展到 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 准则 # 3 |  | 系统检测和/或恢复 | |  |  | 认为适当的标准 | |  |  |  |  |  |  |
|  |  |  |  |  |  | 主管当局及/或 | |  |  |  |  |  |  |
|  |  |  |  | 从人为错误发展到 | |  |  |  |  | 与媒介相同。 | |  |  |
|  |  |  | (UAS 设计) |  |  |  |  |  |  |  |
|  |  |  |  |  |  | 按照... 的方法 | |  |  |  |  |
|  |  |  |  | 行业最佳做法。 |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | 可接受的 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 权威。 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 国家航空局(NAAs) | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 标准及/或 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 他们认为符合规定的手段 | | |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 |  |  |  | 附件 e | | |  | 不认识 | | |  |
|  |  |  |  |  |  | 在稍后的时间更新 | | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 适当标准的清单 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 提供的反馈意见。 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |
|  | 人为错误 | | |  |  |  |  |  | 保证水平 | | |  |  |  |  |  |
|  |  | 很低 |  |  |  |  | 中等 |  |  | 很高 | |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 程序及清单如下: | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 标准的验证 | |  |  |  |  |  |  |
|  |  |  |  |  | 程序和检查表没有 | |  |  | 认为足够的 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 主管当局及/或 | |  |  | 和中号一样，另外: | |  |  |
|  |  |  |  |  | 需要根据 | |  |  | 按照... 的方法 | |  |  | 进行飞行测试以验证 | |  |  |
|  |  |  |  |  | 标准或合规手段 | |  |  | 可接受的 | |  |  |  |  |
|  |  |  | 准则 # 1 |  | 认为足够的 |  |  |  | 权威1。 | |  |  | 程序及清单 | |  |  |
|  |  |  | (程序及 |  | 主管当局。 |  |  |  |  |  |  |  | 覆盖整个飞行信封 | |  |  |
|  |  |  | 检查清单) |  | 程序的充分性 | |  |  | 程序的充分性及 | |  |  | 或被证明是保守的。 | |  |  |
|  |  |  |  |  | 并声明检查表。 |  |  |  | 清单是通过以下方式来证明的: | |  |  | 程序，清单，航班 | |  |  |
|  | 职业安全办公室 # 19 |  |  |  |  |  |  |  | O 专门的飞行测试，或 | |  |  | 测试和模拟验证 | |  |  |
|  | 安全恢复 |  |  |  |  |  |  |  | o 模拟提供 | |  |  | 由合格的第三方提供。 | |  |  |
|  | 来自 Human |  |  |  |  |  |  |  |  | 模拟被证明是有效的 |  |  |  |  |  |  |
|  | 错误 |  |  |  |  |  |  |  |  | 为了预期的目的 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 产生积极的结果。 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 1个国家航空局 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 标准及/或 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 他们认为符合规定的手段 | | |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 |  |  |  | 附件 e | | |  | 不认识 | | |  |
|  |  |  |  |  |  |  |  |  | 在稍后的时间更新 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 适当标准的清单 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  | 提供的反馈意见。 | | |  |  |  |  |  |
|  |  |  | 标准 # 2 |  | 考虑为通用远程机组人员培训 OSO (即 OSO # 09，OSO # 15和 | | | | | | | | |  |  |  |
|  |  |  | (训练) |  | OSO # 22)对应于操作的 SAIL | | | | |  | |  |  |  |  |  |
|  | 附件 e | |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 版本: 1.0 | | | 最终/公开发布 | | | | | |  | 第21页 | | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 人为错误 | |  |  |  |  | 保证水平 | |  |  |  |  |
|  |  | 很低 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | 评论 | | 不认识 | | 不认识 |  |  |  | 不认识 | |  |
|  |  |  | |  |  |  |  |  |  |  |  |  |
|  |  | 准则 # 3 |  | 考虑第9节中定义的标准 | |  |  |  |  |  |  |  |
|  |  | (UAS 设计) |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  | 评论 | | 不认识 | | 不认识 |  |  |  | 不认识 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第22页

**OSO # 20——已经对人的因素进行了评估，发现人机界面(HMI)适合这次任务**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 人为错误 | | | | |  |  | 诚信水平 |  |  |  |  |  |
|  | 很低 |  | 中等 |  | 很高 | |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | OSO # 20 |  |  | 标准 | | 无人机系统的信息和控制界面清晰简洁，不混淆，不合理 | | | | | |  |  |
|  | 一个人 |  |  | 疲劳，或有助于远程机组人员错误，可能对操作安全产生不利影响。 | | | | | |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | 如果一个电子手段被用来支持潜在的可视观察者在他们的角色，以保持对位置的意识 | | | | | | |  |
|  | 影响因素 |  |  |  |  |  |
|  | 的评估 |  |  |  |  | 无人驾驶飞机，其人机界面: |  |  |  |  |  |  |  |
|  | **been** |  |  |  |  | 足以让视觉观察者在操作期间确定 UA 的位置; | | | | | | |  |
|  | 进行和 |  |  | 评论 | |  |
|  |  |  | 不会降低视觉观察者的能力: | | |  |  |  |  |  |
|  | 人机界面发现 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 适合 |  |  |  |  | O 视觉扫描无人驾驶飞机正在操作的空域，以防有任何潜在的碰撞危险; 以及 | | | | | | |  |
|  | 任务 |  |  |  |  | 始终保持与远程驾驶员的有效沟通。 | | |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | 人为错误 | | | |  |  |  | 保证水平 |  |  |  |  |  |
|  |  |  |  |  |  | 很低 |  | 中等 |  | 很高 |  |  |  |
|  | OSO # 20 | |  |  |  | 申请人表现出人为因素 |  |  |  |  |  |  |  |
|  | 一个人 | |  |  |  | 对无人机进行评估，以确定是否 |  | 与低相同，但人力资源指数评估是 |  | 与中等水平相同。此外, |  |  |  |
|  | 影响因素 | |  | 标准 |  | 人力资源管理是适合这项任务的 |  | 基于示范或 |  | 有资格的第三者见证 |  |  |  |
|  | 的评估 | |  |  |  | 人力资源管理体系评价是基于检查或 |  | 模拟 |  | 人力资源管理评估。 |  |  |  |
|  | **been** | |  |  |  | 分析。 |  |  |  |  |  |  |  |
|  | 进行和 | |  |  |  |  |  | 1仿真实验结果表明，该方法的有效性 |  |  |  |  |  |
|  | 人机界面发现 | |  | 评论 | |  |  |  |  |  |  |  |
|  |  | 不认识 |  | 所使用的目标环境 |  | 不认识 | |  |  |
|  | 适合 | |  |  |  |  |  |
|  |  |  |  |  |  | 这个模拟需要被证实。 |  |  |  |  |  |
|  | 任务 | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第23页

***8. 不良运作情况***

**OSO # 23-确定、可测量和遵守的安全操作环境条件**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 逆向操作 | | |  |  | 诚信水平 |  |  |  |
|  | 条件 | | |  | 很低 | 中等 | 很高 |  |  |
|  |  |  | 准则 # 1 |  | 安全作业的环境条件在飞行手册或同等文件中得到界定和反映 | | |  |  |
|  |  |  | (定义) |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | OSO # 23 |  |  |  |  |  |  |  |  |
|  |  |  |  | 1这个标准的低、中和高鲁棒性之间的区别是通过 | | | |  |
|  | 环境许可证 |  | 评论 | |  |
|  |  | 保证(见下表)。 |  |  |  |  |
|  | 条件 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  | 安全 |  | 标准 # 2 |  | 在执行任务前和执行任务期间评估环境状况的程序(即实时评估)是可用的，并且 | | |  |  |
|  | 操作 |  | (程序) |  | 包括用简单的记录系统评估气象条件(METAR，TAFOR 等) | | |  |  |
|  | 定义, |  | 评论 | | 2该准则的低、中和高鲁棒性之间的区别是通过 | | | |  |
|  | 可衡量的 |  |  |
|  |  | 保证(见下表)。 |  |  |  |  |
|  | 并坚持 |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | 准则 # 3 |  | 培训涵盖气象条件的评估 | |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | (训练) |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  | 评论 | | 3该准则的低、中和高鲁棒性之间的区别是通过 | | | |  |
|  |  |  | 保证(见下表)。 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 逆向操作 | | |  |  |  |  | 保证水平 |  |  |  |  |
|  | 条件 | | |  | 很低 | |  | 中等 |  | 很高 |  |  |
|  |  |  | 准则 # 1 |  | 考虑第9节中定义的标准 | |  |  |  |  |  |  |
|  |  |  | (定义) |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | |  |  |  |  |
|  |  |  |  |  |  |  | 程序根据 | |  |  |  |  |
|  |  |  |  |  |  |  |  | 认为适当的标准 |  |  |  |  |
|  |  |  |  |  |  |  |  | 主管当局及/或 |  | 和中号一样，另外: |  |  |
|  |  |  |  |  | 程序不需要 |  |  | 按照... 的方法 |  | 进行飞行测试以验证 |  |  |
|  |  |  |  |  |  |  | 可接受的 |  |  |  |
|  |  |  |  |  | 标准的验证 |  |  |  |  |  |
|  |  |  |  |  |  |  | 权威。 |  | 程序涵盖全部 |  |  |
|  | OSO # 23 |  | 标准 # 2 |  | 或者是一种服从的方式 |  |  |  |  |  |
|  |  |  |  |  |  |  | 飞行信封或被证明是 |  |  |
|  |  |  | 认为足够的 |  |  |  |  |  |  |
|  | 环境许可证 |  | (程序) |  |  | 程序的充分性如下: | |  | 保守。 |  |  |
|  |  |  | 主管当局。 |  |  |  |  |
|  | 条件 |  |  |  |  |  | 通过以下证明: |  | 程序、飞行测试及 |  |  |
|  |  |  |  | 程序的充分性 |  |  |  |  |  |
|  | 安全操作 |  |  |  |  |  | O 专门的飞行测试，或 |  | 模拟是由一个验证 |  |  |
|  |  |  |  | 并声明检查表。 |  |  |  |  |  |
|  | 定义, |  |  |  |  |  | o 模拟提供 |  | 有资格的第三者。 |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 可衡量的 |  |  |  |  |  |  | 模拟被证明是有效的 |  |  |  |  |
|  | 并坚持 |  |  |  |  |  |  | 为了预期的目的 |  |  |  |  |
|  |  |  |  |  |  |  |  | 产生积极的结果。 |  |  |  |  |
|  |  |  | 评论 | | 不认识 | | 不认识 | |  | 不认识 | |  |
|  |  |  |  |  |  |  |  | |  |  | |  |
|  |  |  |  |  |  |  | 培训课程大纲可供参考。 | |  | 有能力的第三方: |  |  |
|  |  |  | 准则 # 3 |  | 训练是自我声明的(有证据的) |  | 经营者提供能力 - | |  | 验证培训大纲。 |  |  |
|  |  |  | (训练) |  | 可用)。 |  |  | 理论和实践的基础 |  |  |
|  |  |  |  |  |  |  | 验证远程机组人员 |  |  |
|  |  |  |  |  |  |  |  | 训练。 |  |  |  |
|  |  |  |  |  |  |  |  |  | 能力。 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 评论 | | 不认识 | | 不认识 | |  | 不认识 | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第24页

**OSO # 24-针对恶劣环境条件(例如充足的传感器、 DO-160认证)设计并合格的无人机**

为了评估该 OSO 的完整性，申请人确定:

设备环境资格测试/声明可否获得认可，例如回答下列问题:

*申请人是否可以获得一份设计和性能声明书(DDP) ，说明设备经测试达到的环境资格水平？*

*环境资格测试是否符合主管当局认为足够的标准(例如 DO-160) ？*

*环境资格测试是否适当且足以涵盖与 ConOps 相关的所有环境条件？*

*如果测试没有按照认可标准进行，测试是否由具有资格或具有进行 DO-160类似测试经验的机构/实体进行？*

设备对预期/预期无人机环境条件的适用性能否根据在役经验或相关测试结果来确定？

影响设备适用于预期/预期无人机环境条件的任何限制。

对于无人机设备只有部分环境合格和/或部分相似性证明和/或部分没有任何合格证明的情况，应考虑最低完整性水平。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 逆向操作 | | |  |  |  |  | 诚信水平 | |  |  |  |  |
|  | 条件 | | |  | 不认识 |  |  | 中等 |  |  | 很高 |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 无人机系统的设计使用 |  |  |
|  |  |  |  |  |  |  |  |  |  |  | 考虑环境标准 |  |  |
|  |  |  | 标准 |  | 不认识 |  |  | 无人机的设计就是为了限制这种影响 |  |  | 足够的主管当局 |  |  |
|  | OSO # 24 |  |  |  |  | 环境状况。 |  |  | 及/或按照 |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 可接受的 |  |  |
|  | 无人机设计 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  | 权威。 |  |  |
|  | 和合格的 |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | |  |  |  |  |  |  |  |  |  |
|  | 不良反应 |  |  |  |  |  |  |  |  |  | 国家航空局(NAAs) | |  |
|  | 环境影响 |  |  |  |  |  |  |  |  |  | 标准及/或 | |  |
|  | 条件 |  |  |  |  |  |  |  |  |  | 他们认为符合规定的手段 | |  |
|  |  |  | 评论 | | 不认识 | |  | 不认识 | |  | 附件 e | |  |
|  |  |  |  |  |  |  |  |  |  |  | 在稍后的时间更新 | |  |
|  |  |  |  |  |  |  |  |  |  |  | 适当标准的清单 | |  |
|  |  |  |  |  |  |  |  |  |  |  | 提供的反馈意见。 | |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 逆向操作 | | |  |  |  |  | 保证水平 |  |  |
|  | 条件 | | |  | 不认识 |  |  | 中等 | 很高 |  |
|  | OSO # 24 |  | 标准 |  | 不认识 |  |  | 考虑第9节中定义的标准 |  |  |
|  | 无人机设计 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 和合格的 |  |  |  |  |  |  |  |  |  |
|  | 不良反应 |  | 评论 | | 不认识 | |  | 不认识 |  |  |
|  | 环境影响 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  | 条件 |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第25页

***9. 技术 OSO 的保证级别标准***

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | 保证水平 | |  |  |  |
|  |  |  |  |  |  | 很低 |  | 中等 |  |  | 很高 |  |
|  |  |  |  |  | 申请人声明 | |  | 申请人有证明文件 |  |  | 有能力的第三方验证 |  |
|  |  |  |  |  | 诚信水平已经达到1。 | |  | 所需的诚信水平是 |  |  | 声称的诚实程度。 |  |
|  |  |  | 标准 |  |  |  |  | 这通常是由 |  |  |  |  |
|  | 技术 |  |  |  |  |  | 测试，分析，模拟, |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 检查、设计评审或通过 |  |  |  |  |
|  | OSO |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  | 运作经验。 |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  | *1* | 支持证据可能是，也可能不是 |  | 2当使用模拟时，有效性 | |  |  |  |
|  |  |  | 评论 | |  | 所使用的目标环境 | |  | 不认识 |  |
|  |  |  | 可用 | |  |  |  |
|  |  |  |  |  |  | 这个模拟需要被证实。 | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

附件 e

版本: 1.0最终/公开发布第26页

参考书目

普华永道称，2020年世界无人机市场接近1270亿美元。第1,9,10页)。

“自主和无人驾驶飞行器的网络安全研究”，《国防建模与模拟杂志》 ，第12卷，第4期，第369-381页，2015(cit)。第1,15,75页)。

“无人驾驶飞行器的网络安全漏洞评论”，2017年 IEEE 安全、安全和救援机器人国际研讨会，IEEE，2017，第194-199页。第1,75页)。

“智能城市的无人机: 网络安全、隐私和公共安全问题”，2016年国际无线通信和移动计算会议，IEEE，2016年9月，216-221页。第1,4,16,75页)。

在2017年无人机系统国际会议上，“基于 ekf 导航控制的虚假数据注入”,

1608-1617(参见第1页)。

《国际民用航空组织无人机系统》 ，2011年第4,7页。

Zolich，T.a。 Johansen，k。 Cisek，and k。 Klausen，“海上任务的无人驾驶航空系统架构。《设计与硬件描述》 ，“2015年无人驾驶航空系统研究、教育和开发工作坊”，IEEE，2015，第342-350页。第4,5,7,8页)。

S. g. Gupta，d. Ghonge，p. m. Jawandhiya，et al。 ，“无人机系统评论”，《国际计算机工程与技术高级研究杂志》2013年第2卷。第4,5页)。

鲁道尔，“通过使用成像传感器提高无人驾驶飞机系统的自主性”，博士论文，林雪平大学电子出版社，2011(cit。译注:

4).

Nonami，f。 Kendoul，s。 Suzuki，w。 Wang 和 d。 Nakazawa，自主飞行机器人: 无人驾驶飞行器和微型飞行器。Springer Science & Business Media，2010(cit.第5页)。

刘振民，d. 泰利奥尔，l. Yang，He，and j. Han，“基于多模型自适应方法的倾转旋翼无人航空载具的过渡控制”，载于2017年国际无人机系统会议，2017，第560-566页。第5页)。

李伯平，朴正群，金志扬，安志强，《无人机混合电力推进系统的动力管理》 ，《机械科学与技术杂志》 ，2012年第26卷，第8期，第2291-2299页。第5页)。

一百八十五

186参考书目

“燃料电池动力飞机的开发和实验特性”，《动力源杂志》 ，第171卷，第2期，第793-801页，2007年(角色塑造)。第5页)。

“燃料电池混合动力系统在模拟小型无人飞行任务中的性能”，《国际氢能杂志》 ，第41卷，第26期，第11418-11426页，2016年(cit)。第5页)。

H González-Jorge，m Bueno，j Martínez-Sánchez，and p aria，“低空长航时太阳能无人驾驶飞机用于森林防火: 在 Serra do Xures (西班牙)自然公园的应用”，《国际摄影测量、遥感和空间信息科学档案》 ，第42卷，第135页，2017年。第5页)。

2016年 IEEE 航空航天会议，IEEE，2016，第1-8页。第5页)。

2016年 IEEE/AIAA 第35届数字航空电子系统会议(DASC) ，IEEE，2016，第1-7页(cit。第6页)。

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》 ，Springer，2015，第433-460页。第6页)。

无人驾驶飞行器手册，2015年，第385-399页。第6页)。

Grewal，l。 well，and a。安德鲁斯，全球定位系统，惯性导航，和整合。约翰威立父子公司，2007(cit。第6页)。

D. Dusha 和 l. Mejias，“单眼 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”，《国际机器人研究杂志》 ，第31卷，第6期，第714-737页，2012(cit。第6页)。

J.R.g. Braga，H.f. de Campos Velho，e. h. Shiguemori，“激光雷达和无人机自主导航的非扩展粒子滤波器”，载于《工程应用新兴技术中的计算智能》 ，Springer，2020，第227-238页。第6页)。

哈勒曼和莫根塔尔，“从航拍摄影到桥梁的三维检查”，在 IABSE 会议记录，2016年，第8-11页(cit。第7页)。

I. Colomina and p. Molina，“用于摄影测量和遥感的无人驾驶航空系统: 评论”，ISPRS 摄影测量和遥感杂志，第92卷,

79-97,2014(见第7页)。

“人类在建筑和基础设施环境中的无人机操作表现”，《工程管理杂志》 ，第35卷，第6期,

04019026,2019(见第7页)。

|  |  |
| --- | --- |
| 参考书目 | 187 |

“ Sloam: 用于森林调查的语义激光雷达里程测量和绘图”，IEEE 机器人与自动化通讯，第5卷，第2号，第612-619页，2020(cit。第7页)。

郭燕，基于激光雷达的测绘方法、设备和系统，美国专利10,578,742,2020年3月(参见第7页)。

“21世纪害虫管理创新方法”中的“用于喷洒杀虫剂的无人驾驶航空系统技术”，Springer，2020，第47-60页。第7页)。

Y. a. Pederi 和 h. s. Cheporniuk，“无人驾驶飞行器和精细农业中监测和作物保护的新技术方法”，2015年 IEEE 国际会议无人驾驶飞行器发展的实际问题，2015，第298-301页(cit)。第7页)。

《无人驾驶飞机系统数据链路和通信系统的操作要求》 ，《计算机网络先进杂志》 ，第4卷，第1期，2016年第28-32页。第8页)。

国际摄影测量、遥感和空间信息科学档案，第41卷，第885页，2016(cit)。第8页)。

欧洲无人机前景研究: 为欧洲释放价值，单一欧洲天空 Atm 研究合资公司(SESAR) ，2016年11月。第8,10页)。

“从玩具到工具: 无人机行业技术和企业发展的共同进化”，《商业地平线》 ，第60卷，第6期,

875-884,2017(参见第9,10页)。

Thibault 和 g。 Aoude，“公司正在把无人机变成一种竞争优势,”《哈佛商业评论》 ，2016年。第9页)。

“农业中无人机的兴起”，欧共体农业，第2卷，第2号,

2015年第325-327页(参见第9页)。

Kulbacki，j. Segen，w. knie，r. Klempous，k. Kluwak，j. Nikodem，j. Kulbacka，and a. Serester，“从种植到收获的农业自动化无人机调查”，2018年 IEEE 第22届智能工程系统国际会议，IEEE，2018，第000353-000358页。第9页)。

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(参见第9页)。

《能源工业中的无人机》 ，《无人机工业洞察》 ，2018年12月(参见第9页)。

无人机市场规模和2019-2024年预测，无人机工业洞察，2019年3月

10).

无人机市场研究报告——2028年预测，未来市场研究，2018年7月(引自第10页)。

2022年的商用无人机，Interact 分析(参见第10页)。

188参考书目

胡图宁先生，“ u 空间概念”，转载自《航空航天法》 ，第44卷，第1期,

69-89,2019(cit. on pp. 10,11,14).

巴斯卡亚，“使用机器学习的无人机故障检测和诊断”，博士论文，ENAC-国家民用航空学院，2019(cit。第11页)。

2017-05年度建议修订公告: 引入无人机操作规管架构，欧洲联盟航空安全局，2017年5月(cit。

11).

J Kamienski 和 j Semanek，“ ATC 对受控空域中无人机集成的观点”，Procedia Manufacturing，第3卷，第1046-1051页，2015(cit。第11页)。

2015-10年拟议修正案通知: 引入无人机运营监管框架，欧洲联盟航空安全局，2015年10月(cit。

11).

U 空间: 蓝图，SESAR 合资公司，2017年(引自第13,14页)。

A. Jafarnia-Jahromi，s. Daneshmand 和 g. Lachapelle,”全球导航卫星系统接收机的欺骗对策——当前和未来研究趋势的回顾”，欧洲航天局，第4卷，第6页，2013(cit。第15页)。

美国德克萨斯州大学奥斯汀分校，“关于民用无人驾驶飞行器和其他系统对民用 GPS 欺骗的脆弱性的声明”,

2012年1月16日(参考文献第15,75,154页)。

S-h.Seo，B.-H.李先生。Im 和 g-i。“利用伪造的 GPS 信号对无人驾驶飞行器进行欺骗的效果”，《定位、导航和计时杂志》 ，第4卷，第2期，第57-65页，2015(cit。第15,75页)。

在第24届 USENIX 安全研讨会(USENIX Security 15)上，K.Dongkwan，p. Youngseok，n. Juhwan，c. Kibum，c. Jung-woo，and k. Yongdae，“在陀螺传感器上故意发出声音噪音的摇摆无人机”，华盛顿特区: USENIX 协会，2015，第881-896页。第15,75页)。

C.-Y.陆炳豪。冯爱仪。Yang，j-y.小王，还有 c-y。邢，“一种基于短时傅立叶变换家族中的关系来控制 MEMS 陀螺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，IEEE，2019，第1-4页。第15,75页)。

T.Trippel，o. Weisse，W.Xu，p. Honeyman，and k. Fu，“ WALNUT: Waging doubt O. the integrity O. MEMS accelerometer with acoustic injection attacks,”in 2017 IEEE European symposium O. security and privacy (EuroS & p) ，IEEE，2017，p. 3-18(cit。译注:

15,75).

杜飞飞，m. Eagon，d. Xu，和 x. Deng，“使用 compro-mised imu 进行小牛的飞行恢复”，arXiv 预印本 arXiv: 1812.00063,2018。第15页)。

“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,

2018年第2488页(引自第16页)。

|  |  |
| --- | --- |
| 参考书目 | 189 |

2017年第25届地中海控制与自动化会议(MED) ，IEEE，2017，第980-985页。第16页)。

G.Fournier，p. Audren De Kerdrel，p. Cotret，and v. Viet Triem Tong，“ drone jack: Kiss your drones goodbye!”2017年国家统计局信息和通信技术安全专题讨论会，法国雷恩，2017年6月，第1-8页。第16,75页)。

Mavlink 开发者指南，Online (参见第16页)。

马蒂，“指挥和控制无人飞机的 mavlink 协议的漏洞分析”，空军技术研究所。2013(cit.第16页)。

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年无人机系统国际会议，IEEE，2016，第830-839页。第16页)。

海格斯，贝弗，卡纳汉，“如何安全飞行测试一架无人机受到网络攻击,”乔治亚理工学院研究所，理工学院。2015年。第16,75页)。

《安全和安保的定义》 ，《埃塔海洋科学杂志》 ，第3卷，第2期，第53-54页，2015年。第20页)。

《论安全和保障的意义》 ，《计算机杂志》 ，第35卷，第1期，第3-15页，1992年。第20页)。

术语词汇，第1版，无人系统规则制定联合权威(JARUS) ，2017年6月(引自第20页)。

安全管理系统: 文献综述》 ，《安全科学》 ，第103卷，第94-123页，2018年。第20页)。

ISO/IEC 27032:2012- 信息技术ー安全技术ー网络安全准则，国际标准化组织，国际电子技术委员会，ISO/IEC 日内瓦，2012(cit。第20页)。

大卫 · 克莱德马赫，迈克 · 克莱德马赫和迈克 · 克莱德马赫，嵌入式系统安全，新闻，2012(参见第20页)。

可靠度工程与系统安全，第110卷，第110-126页，2013年。第20,24-26,40页)。

国际原子能机构原子能机构安全术语表: 术语

用于核安全和辐射防护。维也纳: 国际原子能机构，第227页，2007年。第20,22页)。

《 SEMA 参考框架: 避免在“安全”和“安全”这两个术语中出现歧义》 ，《国际关键基础设施保护杂志》 ，第3卷，第2期，第55-66页，2010年。第20页)。

“工业控制系统的安全性与安全性相结合的方法调查”，《可靠度工程与系统安全性》 ，第139卷，第156-178页，2015年。第20页)。

190参考书目

《系统与软件杂志》 ，第86卷，第4期，第1124-1151页，2013年。第20页)。

C.Schmittner，T.Gruber，p. Puschner，and e. Schoitsch，“失效模式和影响分析的安全应用”，E.，在计算机安全，可靠性和安全，a. Bondavalli 和 f. Di Giandomenico，eds. 卷8666，Springer International Publishing，2014，第310-325页。第20,41页)。

Steve Kremer Ludovic mé and v. Roca，“网络安全——当前的挑战和 INRIA 的研究方向”，INRIA，Tech。代表，2019(cit。第20页)。

民用航空器和系统发展指南 -ARP4754，SAE 国际集团(参见第22,26页)。

Ccps 过程安全术语，化学过程安全中心(参见第22页)。

Iso14971:2019医疗器械ー医疗器械风险管理的应用国际标准化组织及国际电工技术委员会。第22页)。

R Ask，r roisli，s Johnsen，m Line，a Ueland，b Hovland，l Groteide，b Birkeland，a Steinbakk，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)(cit.第22页)。

基塞尔，“关键信息安全术语词汇表”，恩，国家标准与技术研究所，技术。NIST IR 7298r2,2013年5月。第22页)。

ISO/iec27000词汇标准、国际标准化组织(ISO)和国际电工委员会(IEC)。

《互联网安全术语表，第2版》 ，RFC 4949,8月，技术代表，2007(引用第22页)。

惠特曼和马托德，《信息安全原理》 ，Cengage learning-ing，2011(参见第23页)。

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”，博士论文，格勒诺布尔阿尔卑斯大学，2017(cit。第23,25,28页)。

Stamatelatos，w。 Vesely，j。 Dugan，j。 Fragola，j。 Minarick，and j。 Railsback，Fault Tree Handbook with Aerospace Applications。美国宇航局华盛顿特区，2002(cit。第23页)。

ISO/guide 73:2009风险管理ー词汇，国际标准化组织(ISO)(参见第23页)。

“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。在第23,32页)。

P. Kobes,”工业数字系统网络安全国际标准 IEC 62443 Zoom”，in cybersecurity des installations industrials，Cé-paduès，2016(cit。第23,39页)。

|  |  |
| --- | --- |
| 参考书目 | 191 |

Mcdonald，n. Oualha，a. Puccetti，a. Hecker，and f. Planchon，“ EBIOS 在配电分站使用 ICT 的风险评估中的应用”，2013年 IEEE 格勒诺布尔会议，IEEE，2013，第1-6页。第25页)。

V. Agrawal，“ ISO 27005标准中的信息分类框架”，2017年 IEEE 第四届网络安全和云计算国际会议，IEEE，2017，第264-269页。第25页)。

“ ISO/IEC 27005在管理信息系统风险安全分析中的实施”，第6卷，第1-6页，2016年。第25,27页)。

《无人驾驶飞机系统的安全风险管理》 ，《无人驾驶飞行器手册》 ，2015年第2229-2275页。第25页)。

Jjalouneix，p. Cousinou，j. Couturier，and d. Winter，“核安全与核安全的比较方法”，Rapport Technique，第117卷，2009(引自《纽约时报》)。第25,26页)。

埃里克森等，系统安全的危害分析技术。约翰威立父子公司，2015(cit。25,32,34,36-38页)。

DO-326a/ED-202a: 适航安全过程规范，EUROCAE，2014年6月(参见第25页)。

《工业的风险: 复杂性、不确定性和决策: 一种跨学科的方法》 ，Tec & doc-Lavoisier，2006(参见第26页)。

美国 idaho 国家实验室(INL) ，理工学院“控制系统的补丁管理推荐实践”。代表，2008(cit。说

26).

安全服务参考手册，CLUSIF，30 rue Pierre Sémard，75009 Paris，France，2010(参见第26页)。

SORA 附件 e-操作安全目标(oso)的完整性和保证水平，无人系统规则制定联合当局(JARUS) ，2019年1月。第26、66、92、95页)。

米特尼克和西蒙，《欺骗的艺术: 控制安全的人为因素》。约翰威立父子，2003(cit。第26页)。

贝尔，“ iec61508入门”，ACM 国际会议进程系列，卷162,2006，第3-12页。第27页)。

功能安全对整体安全至关重要-功能安全和 IEC 61508系列介绍，国际电工委员会，2015。

27).

美国 ARP4761，“对机载系统和设备进行安全评估过程的指导方针和方法”，美国: 推进机动性工程学会，1996年。第27页)。

JARUS 特定操作风险评估指南(SORA) ，第1版，无人系统规则制定联合权威(JARUS) ，2017年6月。第27、62、64、66、67、69页)。

192参考书目

JARUS 特定操作风险评估指南(SORA) ，第2版，无人系统规则制定联合权威机构(JARUS) ，2019年10月。第27,62,66,86,87页)。

B. Leander，a. A. evi，and h. Hansson，“ IEC 62443标准在工业4.0/iot 中的适用性”，《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)。

适航安全过程规范 ed-202/do-326，EUROCAE，102 rue Eti-enne Dolet，92240 MALAKOFF，法国，2014年6月(cit。28页)。

J.p. Jouas，J.l. Roule，d. Buc，o. Corbier，m. gagné，m. Hazzan，g. Molines，c. Pineault，l. Poulin，p. Sasseville，c. Jolivet，and m. Touboul，MEHARI Overview，Club D. L. security O. L.information français (CLUSIF) ，2010年4月(引自 cit)。第28页)。

法国信息安全俱乐部(CLUSIF) ，摩加多尔大街11号，巴黎75009,2011年。第28页)。

E. Kelling，m. Friedewald，t. Leimbach，m. Menzel，p. Säger，h. seudié，and 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，Tech。2009年12月。第28页)。

罗兰，r。马提亚斯，b。亨利克，a。卢多维奇，p。雷诺，p。加布里埃尔，r。阿拉斯泰尔，w。大卫和 w。本杰明，“基于暗面情景的汽车车载网络安全要求”，EVITA，Tech。代表，2009(cit。第28页)。

培训指南: 危害与可操作性分析(HAZOP) ，产品质量研究所，2015年5月(参见第29页)。

Dunjó，v。 Fthenakis，j。 Vílchez，and j。 Arnaldos，“危害和可操作性(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(cit。第29页)。

诺兰，过程工业的安全和安全审查: HA-ZOP，PHA，what-if 和 SVA 审查的应用。William Andrew，2011(cit.第29页)。

萨拉克，c。西蒙和 j。“确定安全完整性等级的模糊概率方法”，《模糊系统上的 IEEE 事务》 ，第16卷，第1期，第239-248页，2008(cit。第29-32页)。

萨默斯，“分配目标安全完整性等级的技术”，ISA 交易，第37卷，第2期，第95-104页，1998年(cit。第30,31页)。

《利用故障树分析进行可靠性分析: 综述》 ，《国际化学工程与应用杂志》 ，第4卷，第3期，第169页，2013年。第32页)。

《容错计算机系统的动态故障树模型》 ，《 IEEE 可靠性交易》 ，第41卷，第3期，第363-377页，1992年。第33页)。

|  |  |
| --- | --- |
| 参考书目 | 193 |

H. Boudali，a. Nijmeijer 和 M.i. Stoelinga，“ Dftsim: 一个扩展动态故障树的模拟工具”，发表于2009年春季模拟多会议会议记录，Citeseer，2009，第1-8页。第33页)。

梅尔，j.m。鲁塞尔和 j。《基于结构函数的动态故障树的定量分析》 ，《质量与可靠度工程国际》 ，第30卷，第1期，第143-156页，2014年。第33页)。

G. Merle j. m.鲁塞尔。《基于结构函数与蒙特卡罗模拟耦合的动态故障树的定量分析》 ，《质量与可靠度工程国际》 ，第32卷，第1期，第7-18页，2016年(cit)。第33页)。

田中先生，范立凡，赖福林，和 k Toguchi，“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(cit。第33页)。

《过程工业中的损失预防》 ，第17卷，第5期，第339-345页，2004年。第33页)。

《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)。

M. Yazdi，f. Nikfar，m. Nasrabadi，“应用模糊故障树分析进行失效概率分析”，《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)。

J 安德鲁斯，“教程故障树分析”，在第16届国际系统安全会议的进程中，拉夫堡，1998年。第33页)。

安德鲁斯和丹尼特，“使用二进制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(cit。第34页)。

反应堆安全研究: 对美国商业核电站事故风险的评估，美国核管理委员会，1975。第34页)。

《领结方法: 评论》 ，《安全科学》 ，第88卷，2016年第211-218页。第35,36页)。

《安全壁垒: 定义、分类和性能》 ，《过程工业损失预防杂志》 ，第19卷，第5期，第494-506页，2006年。第35页)。

A. Badreddine，T.b. Romdhane，M.A.b. HajKacem，and n. b. Amor，“在领结图中实施预防性和保护性障碍的新的多目标方法”，《过程工业中的损失预防》 ，第32卷，第238-253页，2014年(cit。第36页)。

“领结分析中不确定信息的处理和更新”，《过程工业中的损失预防》 ，第25卷，第1期，2012年第8-19页。第36页)。

O. Salvi 和 b. Debray，“ ARAMIS 的全球观点，SEVESO II 指令框架内的工业风险评估方法”，《危险材料杂志》 ，第130卷，第3期，第187-199页，2006年(cit。第36页)。

194参考书目

C. Jacinto 和 c. Silva，“使用领结表征对职业风险进行半定量评估”，《安全科学》 ，第48卷，第8期，第973-979页，2010年(cit。第36页)。

N. Paltrinieri，f. Khan，p. Amyotte，and v. Cozzani,”风险管理的动态方法: 在 hoegaes 金属粉尘事故中的应用”，《工艺安全与环境保护》 ，第92卷，第6期，第669-679页，2014年。第36页)。

“使用蝴蝶结图分析不确定性下的系统安全和风险: 一种创新的方法”，《过程安全与环境保护》 ，第91卷，第1-2期，第1-18页，2013年(cit。第36页)。

《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)。

ISO 17776:2000石油和天然气工业ー海上生产设施ー国际标准化组织2000年危害辨识和风险评估工具和技术导则。第36页)。

《安全分析技术比较》 ，《可靠性工程与系统安全》 ，第75卷，第3期，第289-294页，2002年。第36,38页)。

Bouissou 先生和 j- 我。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，可靠度工程与系统安全，卷82，第2期，第149-163页，2003(cit)。第36页)。

H-c.《失效模式中的风险评估方法和影响分析: 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)。

David，v. Idasiak，and f. Kratz，“朝向设计和可靠性分析之间更好的相互作用: 源自 UML/SysML 模型的 FMEA,”，Proceedings of ESREL 2008 and 17th SRA-EUROPE annual conference，vol. 3，sep. 2008(cit。第37页)。

Kmenta 和 K.Ishii 在1998年 ASME 设计工程技术会议论文集中提出的“利用元行为建模进行产品和控件并行设计的先进 FMEA”。第38页)。

M Nicholson 和 j McDermid 在2003年第21届国际系统安全会议(ISSC)会议记录中“为复杂系统扩展 PSSA”。第39页)。

Kube 和 b Singer 在2008年第2届 SCADA 安全科学研讨会(S4)会议录中的“安全保证级别: SIL 安全方法”(cit。第39页)。

Gilsinn 和 R.Schierholz，“安全保证等级: 描述安全需求的向量方法”，NIST，2010(cit。第39页)。

温特，o.a。Johnsen 和 B.a. Gran，“使用 HAZOPs 对安全关键系统进行安全评估”，载于国际计算机安全、可靠性和安全会议，Springer，2001，第14-24页。第40页)。

|  |  |
| --- | --- |
| 参考书目 | 195 |

2015年第七届国际电子、计算机和人工智能会议(ECAI) ，IEEE，2015，SSS-1(cit) ，“基于 hazop 的嵌入式系统安全分析: 开放的案例研究”。第40页)。

克拉克和波拉克，“有效的安全需求分析: Hazop 和用例”，载于《国际信息安全会议》 ，Springer，2004，第416-427页。第40页)。

达鲁瓦拉，s。曼杜哈诺，N.k。曼吉普迪和 h。“使用 HazOP 对硬件和软件产品进行威胁分析”，载于《计算和信息科学国际会议记录》 ，2009年，第446-453页。

40).

施奈尔，“安全威胁建模”，Dobb 博士的期刊，1999(引用第40页)。

V. Nagaraju，l. Fiondella，and t. wanda ji，“网络风险管理的故障和攻击树建模与分析调查”，2017年 IEEE 国际国土安全技术研讨会，IEEE，2017，第1-6页。第40页)。

O. Henniger，l. Apvrille，a. Fuchs，y. Roudier，a. Ruddle，and b. Weyl，“汽车车载网络的安全要求”，2009年第9届智能运输系统电信国际会议，IEEE，2009，第641-646页。第40,75页)。

2016年 IEEE 系统会议(SysCon) ，2016，第1-7页(cit。第40页)。

Byres，m。 Franz 和 d。 Miller，“在评估 SCADA 系统中的脆弱性时使用攻击树”，发表于《国际基础设施生存性研讨会会刊》 ，citseer，2004，第3-10页。第40页)。

“利用攻击和保护树来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会议(HICSS’07) ，IEEE，2007,144b-144b (cit。第40页)。

“网络安全分析的企业架构模型”，2009年 IEEE/PES Power Systems Conference and Exposition，IEEE，2009,

1-6(参看第40页)。

B. Kordy，s. Mauw，m. Melissen，and p. Schweitzer，“攻击防御树和二人二进制零和广义形式博弈是等价的”，《安全决策与博弈论国际会议》 ，Springer，2010，第245-256页。译注:

40).

Jürgenson and j。 Willemson，“ Processing Multi-Parameter attack tree with es-estimated Parameter Values,”in International Workshop on Security，Springer，2007,

308-319(参看第40页)。

Yager，“ OWA 树及其在使用攻击树进行安全建模中的作用”，In-formation Sciences，第176卷，第20期，第2933-2959页，2006(cit。第40页)。

196参考书目

“利用博弈论和模糊逻辑的概念为 vanet 的风险和安全评估提供一个基于攻击树的综合框架”，《 Web 智能中的新兴技术杂志》 ，第6卷，第2期，第247-252页，2014(cit。第40页)。

A.Gran，D.Raptis，and k。 Stolen，“基于模型的风险评估以提高企业安全性”，刊于 Proceedings。第六版国际企业分布式对象计算，IEEE，2002，第51-62页。第41页)。

Gorbenko，v. Kharchenko，o. Tarasyuk，and a. Furmanov，“ f (i) web 服务分析和可靠性保证技术”，《复杂容错系统的严格开发》 ，Springer，2006，第153-167页。第41页)。

C. Schmittner，Z.Ma，P.Smith，“ FMVEA 智能和合作车辆的安全和安保分析”，载于国际计算机安全、可靠性和安全会议，Springer，2014，第282-288页。第41页)。

威胁效应分析: 将 FMEA 应用于计算机系统威胁建模，2008年度可靠性和可维护性研讨会，IEEE，2008，第463-468页。第41页)。

M.Rebekah，“评估工程环境中的网络风险: 一个建议的框架和方法,”SANS 研究所，技术。2016年(cit。第41页)。

“海洋运输系统中的网络风险”，载于《网络物理安全》 ，斯普林格出版社，2017年，第113-131页。第41页)。

哈里，“网络安全的领结(0x01) : 如何打一个网络领结,”PI 广场，科技。代表，2016(cit。第41页)。

Bernsmed，c。 Frøystad，P.h。 Meland，d。 Nesheim，and ø。Rødseth，“ Vi-sualizing cyber Security risks with bow-tie diagrams,”in International Workshop on graphic Models for Security，Springer，2017，pp. 38-56(cit。第41页)。

H. Abdo，“处理风险分析中的不确定性: 安全与安保相结合”，阿尔卑斯格勒诺布尔大学，2017年12月。第41,43页)。

《马尔可夫链模型在网络攻击检测中的稳健性》 ，《 IEEE 可靠性交易》 ，第53卷，第1期，第116-123页，2004年。第42页)。

“基于马尔可夫博弈论的网络信息系统风险评估模型”，2008年国际计算机科学与软件工程会议，IEEE，第3卷，2008年，第1057-1061页。第42页)。

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”，载于2019年 IEEE 信息通信、科学和技术国际科学实践会议问题，IEEE，2019，第497-501页。第42页)。

|  |  |
| --- | --- |
| 参考书目 | 197 |

Piètre-Cambacédès and m. Bouissou，“ Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP) ,”in 2010 European De-pendable Computing Conference，IEEE，2010，pp. 199-208(cit。第42页)。

Piètre-Cambacédès 和 m. Bouissou，“使用 BDMP 进行攻击和防御建模”，《计算机网络安全的数学方法、模型和体系结构国际会议》 ，Springer，2010，第86-101页。第42页)。

McDermott，“攻击网络渗透测试”，2000年新安全范式研讨会会刊，2001年，第15-21页。第42页)。

周美华，秦振锋，张振强，张晓强，陈华，刘强，“基于着色 petri 网的攻击建模”，参加国际粗糙集、模糊集、数据挖掘和粒度软计算研讨会，Springer，2003，第715-718页。第42页)。

Fu，j. Zhu，and s. Gao，“基于 Petri 网的 CPS 信息安全风险评估系统”，2017年 IEEE 第二届国际信息空间数据科学会议，IEEE，2017，第541-548页。第42页)。

周建国、张立国，“基于 petri 网的化学过程安全背景下的攻击时间分析”，《计算机与化学工程》 ，第130卷，第106546页，2019年。第42页)。

“安全和安保共同分析: 一个系统的文献综述”，IEEE 系统杂志，第13卷，第3期，第2189-2200页，2018(cit。在

43).

Reichenbach，J.Endresen，M.m. Chowdhury，and J.rossebø，“一个安全和安全风险综合分析的实用方法”，2012年 IEEE 第23届软件可靠度工程国际研讨会，IEEE，2012，第239-244页(cit。第43页)。

施密特纳和瓦尔加，“为工业协同自动化系统结合安全和安全分析”，载于国际计算机安全、可靠性和安全会议，Springer，2017，第187-198页。第43页)。

可靠度工程与系统安全，第94卷，第9期，第1394-1402页，2009(cit)。译注:

43).

普伊斯，M.l。Potet 和 A.Khaled，“针对工业系统的应用攻击场景的产生”，在国际安全基础与实践研讨会上，Springer，2017，第127-143页。第43页)。

Juras 关于 sora 的指导方针，附件 a: 关于为特定的无人机行动收集和呈现系统和操作信息的指导方针，《无人机系统规则制定联合当局，2017年》(cit。第47,98,101页)。

适航安全方法和考虑，EUROCAE，102 rue Etienne Dolet，92240 MALAKOFF，法国，2015年9月(引用于第53页)。

198参考书目

O. Gadyatskaya，r. Jhawar，p. Kordy，k. Lounis，s. Mauw，and r. Trujillo-Rasua，“用于实际安全评估的攻击树: 使用 ADTool 2.0对攻击场景进行排序”，载于《系统的定量评估》 ，g. Agha 和 b. Van Houdt，eds. ，Cham: Springer International Publishing，2016，第159-162页。第55页)。

Nikodem，a. Bierig，and J.s. Dittrich，“与普通民用航空风险评估相比，新的特定操作风险作为 UAS 监管的评估方法”，在 DLRK 2018,2018(cit。第62页)。

欧洲联盟航空安全局(EASA)2019/947委员会实施规例(eu)可接受的合规方式(AMC)及指引材料(GM) ，2019年10月(cit)。第62页)。

2015年12月，欧洲联盟航空安全局(EASA)介绍了无人驾驶飞机运营的监管框架。第62,67页)。

A-NPA 2015-10: 引入无人机操作的监管框架，欧盟航空安全局(EASA) ，2015年10月。第67页)。

C. Pauner，i. Kamara 和 j. Viguri,”雄蜂”。当前隐私和数据保护领域的挑战和标准化解决方案,”2015年国际电联万花筒: 信任信息社会(K-2015) ，2015，第1-7页(cit。第67,69,71页)。

《隐私与民用无人机的使用: 进一步规范的必要性》 ，《 IEEE 安全与隐私》 ，第16卷，第5期，第72-80页，2018年。译注:

67).

张永志，张振福，孙耀民，余振宇，“无人机的安全与隐私问题: 一个调查”，《移动网络与应用》 ，第95-101页，2019(cit。第69页)。

《欧洲数据保护中的七种隐私类型: 成年》 ，斯普林格出版社，2013年，第3-32页。第69页)。

2019年国际计算、网络和通信会议(ICNC) ，2019，第562-566页，“通过调节高度和有效载荷来实现无人机隐私”。第69页)。

来自上面的观察: 无人驾驶飞机系统和隐私，哈佛法律公共政策杂志，2013(cit。第69页)。

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,

1-7(参见第69,71页)。

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 国际会议和自动面部和手势识别研讨会，卷04,2015，第1-6页(cit)。第69,71,72页)。

2015年综合通信、导航和监视会议(ICNS) ，2015，第1-8页。第69页)。

|  |  |
| --- | --- |
| 参考书目 | 199 |

P. Blank，s. Kirrane，and s. Spiekermann，“无人驾驶航空系统的隐私感知限制区”，IEEE 安全隐私，第16卷，第2期，第70-79页，2018(cit。关于

70,72).

规划、设计、安装和操作闭路电视监控系统。《实务守则及相关指引》 ，英国安全行业协会，二零一四年七月(香港法例第2014章)。第71页)。

A. y. Javaid，w. Sun，v. k. Devabhaktuni，and m. Alam，“网络安全威胁分析和无人航空载具系统建模”，2012年 IEEE 国土安全技术会议，IEEE，2012，第585-590页(cit)。第75页)。

D. Davidson，H.Wu，r. Jellinek，v. Singh，and t. Ristenpart，“用传感器输入欺骗攻击来控制无人机”，在2016年第10届 fUSENIXg 攻击技术研讨会上(fWOOTg 16)。第75页)。

C. Capitán，j. Capitán，a. r. Castano，and a. Ollero，“基于 SORA 方法的无人机媒体生产应用风险评估”，2019年无人机系统国际会议，IEEE，2019，第451-459页。译注:

84,90).

可交付的 d2.1: 多重无人机媒体生产要求，多重无人机项目-布里斯托尔大学，2017年7月(引用于第84页)。

在2017年第33届年度计算机安全应用会议记录中，“基于协同处理器的行为监控: 应用于检测针对系统管理模式的攻击”,

399-411(引用于第106页)。

阮先生，《平台嵌入式安全技术》 ，斯普林格自然出版社，2014年(参见第106页)。

在没有内部非挥发性记忆体的设备中提供固件版本的防回滚保护的方法，美国专利9,910,659,2018(cit。第106页)。

《卫星遥感与地理信息系统在农业气象学中的应用》 ，第121页，2004年。第152页)。

Kaplan and c。 Hegarty，Understanding GPS: principles and applications。 Artech house，2005(引用于第152页)。

Ahmad，M.a. Farid，s. Ahmed，k. Saeed，M.Asharf，and u. Akhtar，“ GPS 欺骗的影响和探测以及防范欺骗的对策”，2019年第二届国际计算、数学和工程技术会议，IEEE，2019，第1-8页(cit。第153页)。

“ GPS 易受欺骗威胁和反欺骗技术回顾”，《国际导航与观测杂志》 ，2012年第二期。第153页)。

《全球导航卫星系统欺骗与检测》 ，《 IEEE 会刊》 ，第104卷，第6期，第1258-1270页，2016年。第154页)。

200参考书目

温家宝，P.y.r。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)。

德克萨斯州大学奥斯汀分校博士论文，2011(角色塑造)。第154页)。

A. Jovanovic c. Botteron 和 p.a。Fariné，“针对全球导航卫星系统接收机欺骗攻击的多测试检测和保护算法”，2014年 IEEE/ION 位置、定位和导航研讨会-plans 2014，IEEE，2014，第1258-1271页。译注:

154).

麦克道尔，使用数字空间零点的 GPS 欺骗和中继器缓解系统，美国专利7,250,903,2007(cit。第154页)。

P.y. 蒙哥马利，“接收机自主欺骗检测: 多天线接收机防御便携式民用 GPS 欺骗器的实验结果”，在无线电导航实验室会议记录，2011(cit。第154页)。

《全球导航卫星系统对单天线手持接收机的欺骗检测》 ，导航，第58卷，第4期，第335-344页，2011年。译注:

154,155).

在2017年第13届计算智能与安全国际会议(CIS)上，“一种基于视觉的小型无人机 gps 欺骗检测方法”，IEEE，2017，第312-316页。第154页)。

Panice，s. Luongo，g. Gigante，d. Pascarella，c. D. Benedetto，a. Vozella，and a. pescè，“一种基于支持向量机的 GPS 欺骗攻击检测方法”，2017年第23届国际自动化与计算会议，IEEE，2017，第1-11页。第155页)。

Z. Feng，n. Guan，M.Lv，w. Liu，q. Deng，x. Liu，and w. Yi，“利用机载运动传感器进行有效的无人机劫持检测”，载于《欧洲会展设计、自动化与测试》 ，2017，IEEE，2017，第1414-1419页。关于

155).