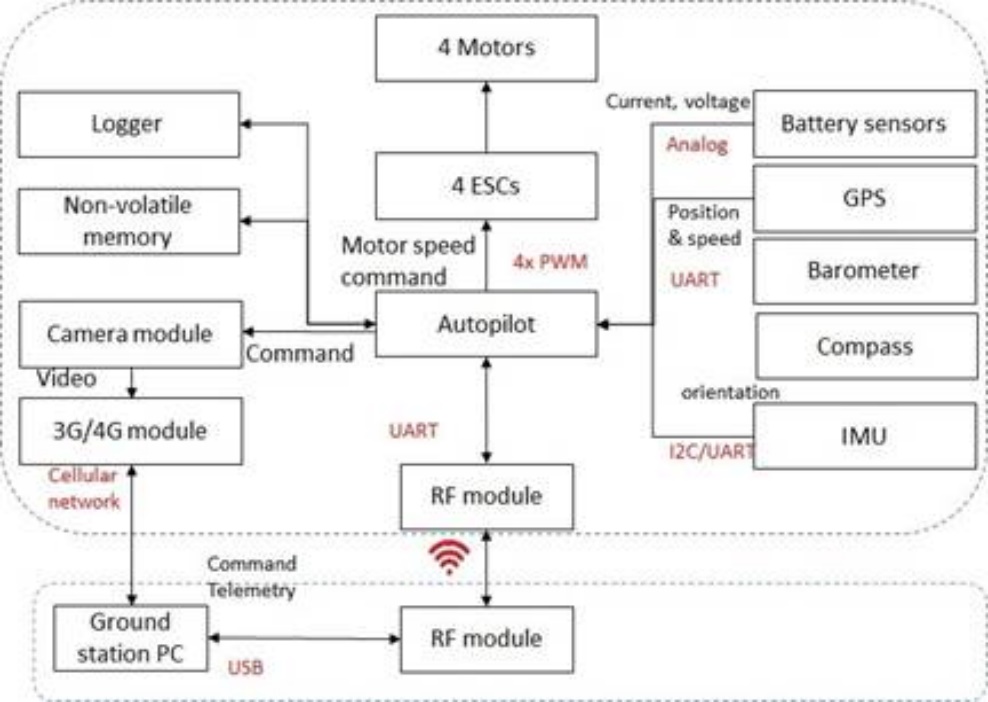
3.3 研究案例

本小节会运用上文所述的方法，来分析一个实际案例。本案例是SOGILIS公司推出的一套基于无人机的道路监测系统。在这套系统中，无人机主要的任务是在自动导航模式下，实时监测高速公路的地面情况。具体的操作过程是这样的：

无人机开始执行任务，会飞至指定的目标公路，然后对公路地面进行摄录，同时记录此刻自身的飞行数据，接着同步反馈信息给地面控制站（GCS）。地面控制站成功接收到消息后，操作员可以计算机中实时获取无人机拍摄的相关视频和飞行数据。

在无人执行任务时，无人机会沿着目标公路遵循任务预定轨迹飞行。整个任务执行过程中，无人机都会在操作员的超视距（BVLOS）观察下始终以自动模式飞行。地面操作员秩序执行三个基础任务：启动导航、结束导航、提前返航。

这套自动飞行系统（UAS）的架构图如下图所示。为了简化模型，假设该自动飞行系统的架构图是在没有任何网络安全威胁的情况下设计的，也就是说，，该架构面对潜在攻击所导致的故障，没有相应的应对措施。



自动飞行系统（UAS）的架构图

从自动飞行系统（UAS）的架构图中可以分析得出，无人机整体上有三个系统模块：

模块1：导航模块。无人机需要按照操作员预先录入的飞行轨迹进自动飞航。飞行轨迹中可以包含多个途经点。每个途经点都有相关坐标、海平面高度和地面高度等重要信息。

模块2：状态传输模块。无人机需要保存自身所有的状态信息，这包括了飞行姿态、飞行坐标、预定航迹、电量信息等状态信息。这些信息需要在无人机执行任务时，向地面控制站实时发送。

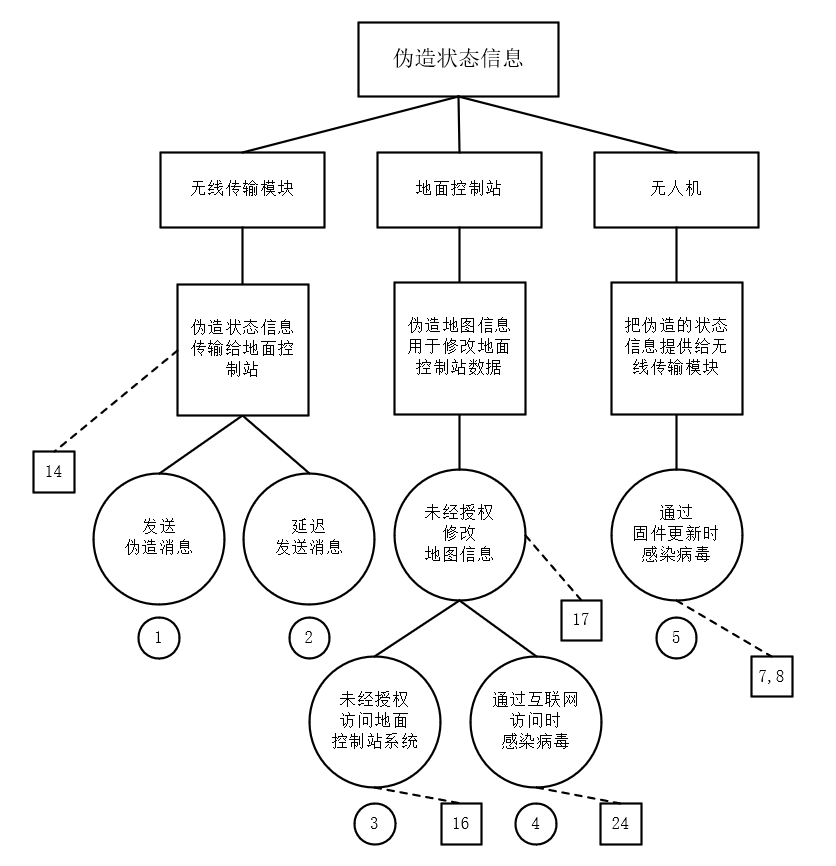
模块3：视频传输模块。无人机在执行任务期间，需要通过摄像机捕获地面目标信息，并实时的传输给地面控制站。

综上，无人机自动飞行系统有导航、状态传输、视频传输三个核心模块，因此我们需要对应设计三个安全决策系统。

在定义安全预防系统之前，需要先假设攻击者在攻击核心模块后会引发何种故障，之后根据故障表现再设计可以应对的安全决策。每个故障都与系统核心模块中的一个网络安全属性（完整性、可用性、机密性）的有关。故障列表如下所示。其中，一级故障为特别严重、二级故障为严重、三级故障为比较严重、四级故障为一般严重。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **故障模块** | **故障**  **属性** | **故障名称** | **故障状态** | **故障**  **等级** |
| 模  块  1 | 可用性 | 无人机  坠毁 | 受到攻击后，无人机失去可调整姿态，导致坠毁。对地点造成破坏。 | 一级 |
| 完整性 | 偏离  预定航道 | 受到攻击后，无人机偏离预定航道。攻击者可能劫持无人机，同时利用无人机对我方设施造成破坏。 | 一级 |
| 保密性 | 无 |  |  |
| 模  块  2 | 可用性 | 状态信息  损毁 | 受到攻击后，无人机飞行状态信息被损毁，无法恢复。地面控制站无法获取无人机状态，失去对目标的完全监控。 | 二级 |
| 完整性 | 状态信息  伪造 | 受到攻击后，攻击者会把伪造后的飞行状态信息发送至我方地面控制站。导致我方控制站可能会据此做出错误决策。 | 二级 |
| 保密性 | 状态信息  泄露 | 受到攻击后，攻击者可能获得保密的无人机飞行状态信息，这有助于攻击者发起潜在的其他攻击。 | 二级 |
| 模  块  3 | 可用性 | 视频信息  损毁 | 受到攻击后，地面控制站无法恢复视频信号。 | 四级 |
| 完整性 | 视频信息  伪造 | 受到攻击后，地面控制站接收伪造后的视频信息，获得假情报。无人机自身扔在的安全的可操作范围内。 | 四级 |
| 保密性 | 视频信息  泄露 | 受到攻击后，攻击者可以观察到视频内容，导致泄露被观察者隐私，暴露任务目标。 | 三级 |

接下来需要对每一个故障问题，建立一个对应的攻击树。本文通过 ADTool —— 一个开源软件来绘制具有相关需求的攻击树。



“状态信息伪造”攻击树

上图显示了与模块2-完整性的“状态信息伪造”攻击树。本章接下来会着重分析状态信息伪造攻击树。其他故障的攻击树分析在附录部分展示。

面对“状态信息伪造”故障，该攻击树模拟了五种可能的攻击场景：

场景1：攻击者通过射频通信信道攻击无人机。如果无人机的射频通信信道没有足够的保护措施，攻击者就可以把伪造的假状态信息发送到地面控制站，此时攻击者可以伪造无人机故障，欺骗地面控制站。因此，防御该类型攻击的有效措施是确保无人机通信的RF模块对每个接受到的数据包在时间、有效载荷和消息来源等方面进行核验，以确保信息的完整性。

场景2：该场景与第一个场景类似，攻击者同样会发送假状态信息给地面控制站。与场景1不同的是，攻击者不会编造假信息，而是把无人机传输回地面控制站的信息拦截后推迟发送。导致操作员接收到时间混乱的状态信息。在该场景下，攻击者无需知道消息的结构或加密方案。防御这种攻击的方式，主要是在RF模块中，对接收的消息包的时间间隔和先后顺序的进行验证，以检查消息的完整性。

场景3：在此场景中，攻击方通过地面军事系统攻击无人机。如果攻击覆盖面涵盖地面控制站，攻击方可以对地面控制站内的战术地图进行修改。则地面控制站保存的地图和无人机的预定轨道不一致，从而引发故障。对于此攻击场景，攻击者无需具备高科技技术，而需要有机会访问控制站的内部系统（如内部人员泄露）。面对这种攻击，有效的措施是对军事信息分等级的设置访问权限。

场景4：在此场景中，攻击方会通过互联网将我方地面控制站的计算机系统感染恶意病毒，该病毒可能会在我方计算机防火墙未检测到病毒入侵的前提下静默修改存储的地图信息。对于此攻击方式，攻击者必须具备攻击和破坏防火墙的后门程序，难度较高。攻击者需要了解我方地面控制站使用的计算机系统内部数据库和系统架构等基本信息，且我方地面控制站使用的内部网或互联网存在尚未被发现的致命漏洞。

场景5：在此场景中，攻击者在无人机系统更新固件时，置入后门程序。这样无人机在执行任务时会被后门程序篡改数据，把错误消息返回给地面控制站。对于此类攻击，攻击者需要了解无人机系统内部的系统架构等核心技术，同时可以在我方不被发现的情况下更新无人机固件。

下表评估了上述攻击场景的风险级别：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 类别 | 攻击难度（DOA） | | | | 严重  程度 | 风险  等级 |
| 攻击的  准备难度 | 攻击的  潜在时机 | 攻击的  实施难度 | 总计 |
| 场景1 | 2 | 1 | 6 | 9（一般） | 中等 | 中等 |
| 场景2 | 2 | 1 | 6 | 9（一般） | 中等 | 中等 |
| 场景3 | 6 | 6 | 10 | 22（高） | 中等 | 低 |
| 场景4 | 6 | 6 | 10 | 22（高） | 中等 | 低 |
| 场景5 | 6 | 6 | 10 | 22（高） | 中等 | 低 |

表xx 与模块2完整性相关的攻击场景的风险评估

3.3.1 结果分析

基于攻击树，本小节分析了49种可能的攻击场景，包括9中高风险场景、28种中风险场景和12中低风险场景，这些攻击场景涉及到了无人机的多个组件。下图显示了无人机各个组件受到攻击的可能….

