

Document Title: Requirements Specifications		
Document #: RS 01	Revision #: 03	Previous Doc/Rev #: N/A

#### CHANGE HISTORY

Rev.	Date	Detailed change description (include rationale for change)	Affected Documents	Supporting Documents
01	01/15/2022	Initial Release		<House of Quality Use Cases, Input-Output diagram, etc.>
02	9/29/2025	Applicable Information		<Project Request Form>
03	10/1	Target Specifications		<Requirements Matrix>

#### DOCUMENT REVIEW AND APPROVAL

Name	Title	Contributed Sections	Signature/Date
Isabella Burley	Project Lead	Change History Purpose Definitions Acronyms Customer Needs: Table System Requirements: Verification Type	
Will	Engineering	Customer Needs Ethical Considerations Use Case: Spoofing Use Case: Spoof Detection	
Carl Holmberg	Engineering	Problem Statement Key Stakeholders External Factors	
Drew Schineller	Engineering	Product Requirements System Requirements: Matrix Target Specifications Benchmarking Information	
Kush Pamar	Engineering	General Constraints – Societal System Requirements – Diagrams	

Sachel Jetly	Engineering		
Andrian Jordan, POC	Customer		
Isreal Jordan, POC	Customer		
Ryan Williams, SME	Subject Matter Expert		
Janice Burr, Mentor	Mentor		

## TABLE OF CONTENTS

Purpose .....	4
Definitions .....	4
Document Definitions .....	4
Table 01-1 Document Definitions.....	4
Document Acronyms.....	5
Table 01-2 Document Acronyms.....	5
Customer Needs .....	6
Problem Statement .....	6
Customer Needs Description .....	6
Key Stakeholders .....	8
General Constraints.....	8
External Factors - Global, Cultural, and Environmental .....	8
Social Factors - Public Health, Safety, and Welfare.....	9
Ethical Factors - Global, Societal, Economic, and Environmental .....	10
Use Case: LiDAR/GPS Spoofing .....	11
Use Case: Spoof Detection.....	12
Product Requirements .....	13
System Requirements.....	13
Target Specifications.....	16
Table 01-5 Target Specifications .....	16
Table 01-6 Standards and Statutory Requirements .....	18
Benchmarking Information .....	18
Table 01-7 Benchmarking Information .....	18

References..... 19

## Purpose

This document defines the customer needs and requirement specifications for the low-cost smart sensor spoofer on an unmanned air system (UAS) including the functional/engineering metrics such as two reliable spoofing techniques, UAV flight expectations, and neural network processing. It is intended to establish traceable requirements that guide system design and future validation as well as translation of those needs. This document will be used as entry criteria to the Architecture Phase of the project. This document outlines all plans are aligned with the sponsor's expectation, ethical considerations, and any relevant standards

## Definitions

### Document Definitions

Table 01-1 Document Definitions

Term	Definition
Design History File	A compilation of records containing the complete design history of a finished device or service
Verification	Confirmation by testing, analysis, demonstration, and/or inspection that specified requirements have been fulfilled
Validation	Establishing objective evidence that system specifications conform to user needs and intended uses in the operational environment
Component	One of the parts that make up a system. A component may be hardware or software and may be subdivided into components
Functional Testing	Testing that ignores the internal mechanism of a system or component and focuses on the outputs generated in response to selected inputs
Control System	The integrated set of hardware and software that manages the UAV's flight operations, sensor inputs, and spoof detection logic. It executes commands, maintains stability, and enforces failsafe behaviors.

Control Station	The ground-based interface (potentially a laptop or dedicated controller) used by the operator to monitor UAV status, receive sensor data, and issue flight or spoofing commands.
Operator	The individual responsible for commanding, supervising, and interpreting UAV operations through the control station, including initiating spoofing scenarios and responding to system alerts.
Sensor Data	The raw or pre-processed measurements (e.g., images, LiDAR point clouds, GPS coordinates) collected by onboard sensors and transmitted to the control system or neural network for analysis.
Neural Network	A computational model inspired by biological neural systems that processes sensor data, identifies patterns, and detects anomalies (such as spoofed versus real inputs) in real-time.
Spoofing	The intentional manipulation, alteration, or falsification of sensor data streams (e.g., camera frames, LiDAR points, or GPS signals) to mislead the UAV's perception and decision-making processes.
Real-time	The capability of the system to process sensor inputs, run neural network inference, and output detection results within strict time constraints such that responses occur without perceptible delay during flight.

## Document Acronyms

Table 01-2 Document Acronyms

Acronym	Description
DHF	Design History File
IEEE	Institute of Electrical and Electronics Engineers
CR	Customer Requirement
SR	System Requirement
UAV	Unmanned Air Vehicle

UAS	Unmanned Air System
COTS	Commercial off the Shelf
UI	User Interface
GPS	Global Positioning System
PNT	Position, Navigation, and Timing

## Customer Needs

### Problem Statement

Our customer requires data collection and analysis on sensor spoofing and spoof detection between two UAS platforms equipped with sensor and controlled emitter hardware. This project will aid in the research and development of small, inexpensive UAV spoofer platforms to be used by the US Navy and increase awareness of spoofing techniques and neural network applications. The final project will be completed within the next two semesters and will produce desired datasets (real and spoofed) and trained detection models through a physical UAV system.

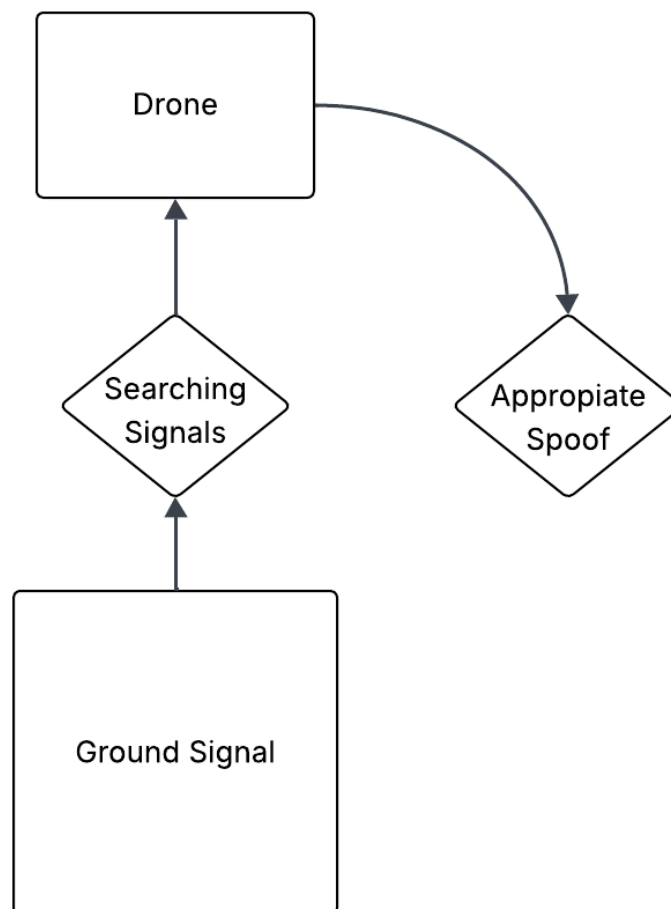
### Customer Needs Description

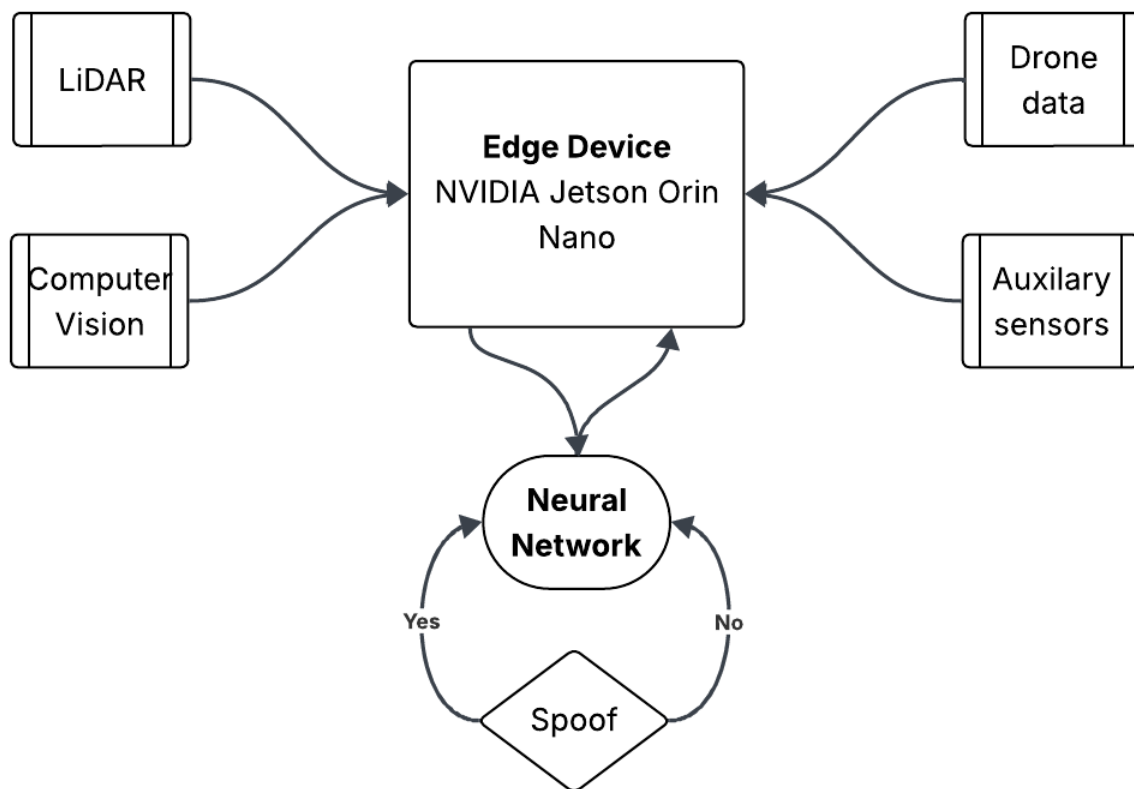
The customer requires a solution which entails a commercial off the shelf drone that must

Customer Needs	Requirements
Optical Camera	15-25 m detection range with a 360-degree field of view
Laser	Directional, able to spoof a LiDAR or optical sensor
Control System	Has a display with event-based sensor imagery
Ground Control	3 miles from “control station”, able to display sensor data to the operator
UAV (Control and Navigation)	Fly at a minimum of 40 feet above ground and 15mph while flying, log all data, differentiate actual/spoofed sensor data, maintain stable flight while spoofing, failsafe mode, incorporate a neural network processing unit to analyze data in real-time

Spoofing Capability (UAV)	Capable of spoofing sensor data to mimic environments/objects, spoof $\geq 2$ types of sensor data, dynamically adjust spoofing parameters, selective spoofing, use a user interface (UI), receive updated spoofing profiles, train data wirelessly, record spoofing activity to local storage
Neural Network Processing	Trainable and retrainable, support integration of multiple neural networks, power-efficient (flight endurance), implement methods for uncertainty, method to detect adversarial inputs

### Spoof Detection & Removal





## Key Stakeholders

- NAWCAD Pax River (Primary Stakeholder/Customer)
- US DoD (Research data for inexpensive spoofer UAS)
- Foreign Military Forces (Work may impact foreign allies/enemies, positively or negatively)
- VT AOE Department (Main UAV source)

## General Constraints

### External Factors - Global, Cultural, and Environmental

#### Global Effects:

The biggest global concern of our project is the impacts on public transportation and other civilian systems that rely on accurate LiDAR and GPS data to function properly. Many autonomous vehicles utilize LiDAR to reduce uncertainties in recognizing lane shapes, traffic light locations, and traffic signs [2], which are critical in ensuring safe self-driving. Spoofing these sensors could lead the victim off roads or make them ignore traffic lights [2], leading to

collisions and possible death of occupants in the vehicle. GPS devices are also critical in ensuring correct location of manned and unmanned air and ground systems, and if these systems are spoofed, they quickly become inaccurate and rendered useless. To ensure that we abide by FAA and FCC regulations, all spoofing systems that we design will be tested in an anechoic environment to ensure safety.

#### Cultural Effects:

Culturally, our project has significant impacts on the reliance of technology and the increased presence of cyber-attacks in military tactics. GPS Spoofing techniques are already widely used in the middle east by Israel to disrupt civilian and military GPS devices [3], causing overall distrust in GPS accuracy in the affected areas. LiDAR attacks are more targeted; however LiDAR is widely used in military UAV platforms, and any advancement in LiDAR spoofing technology would be met with subsequent advancements in foreign military forces as the technology is perceived as a threat.

#### Environmental Effects:

Our project has several environmental effects, including the sustainability of the materials we use to design our UAV payload and the energy sources we use to power the payload. The materials we use to design the payload container will be either machined or 3D printed, which are both recyclable options, and all the sensors and other components will be COTS and able to be reused in other systems. We also plan on powering our system on a single, rechargeable COTS battery assembly to reduce environmental impact.

We will minimize the impacts on the project lifecycle by selecting recyclable materials for the enclosure with components that can be reused. By choosing a reusable lithium-ion battery pack we reduce waste vs using disposable cells and simplify charging. We will follow the EPA guidance for safe handling of dead lithium-ion packs.

The operational choices that reduce environmental harm would be following the FAA rules and local approvals. This will determine how we test, and which sites are okay to be used. For any laser work we will follow the correct guidance to make sure we handle it correctly.

## Social Factors - Public Health, Safety, and Welfare

The primary social concern for this project is public safety rather than direct health and welfare due to the nature of the work in LiDAR and GNSS signal generation with UAVs. The potential consequences of this system extend beyond testing near public infrastructure and thus must be addressed. Uncontrolled contained signal experiments could degrade navigation for ground vehicles, commercial air vehicles, autonomous systems, and interfere with timing dependent services that could undermine public safety and confidence in said infrastructure thus undermining public confidence. For these reasons, protecting the public and critical infrastructure is the guiding principle for both our research questions and our experimental methods.

All testing will be restricted to simulations, shielded laboratory environments, or faraday cages. Live public space signal injection is explicitly prohibited and will not be executed in any situation

regardless of authority or use case. Lab safety practice include ensuring proper RF containment, pre test checklists for equipment, continuous monitoring, and comprehensive logging for all system outputs. Personnel will follow institutional safety procedures and maintain documented emergency procedures for tests that could affect the public safety of nearby and far areas.

From an engineering standards perspective, the design emphasizes fail safe behavior and constrained operating procedures the design emphasis fail safe behavior and constrained operational standards. Hardware limits on signal strength, output power, and hardware interlocks will allow unintended broadcasts to not bleed through and cause potential issues. We will map specific standards and guidelines (IEEE standards and similar) into the development and verification plan to ensure traceability of our project from requirements to verification and testing.

Customer and stakeholder requirements were directly influenced by this safety analysis: the product must include monitoring and automatic control capabilities which include air gapped software, documented safety procedures, and regulatory coordination before any field demonstration. These constraints are reflected in constraint tables that detail output metrics, mandatory enclosure usages, and required logging/data collection for all use cases.

## Ethical Factors - Global, Societal, Economic, and Environmental

The most relevant parts of the IEEE code of ethics that relate to our project are listed below [1]:

- *Section I. To uphold the highest standards of integrity, responsible behavior, and ethical conduct in professional activities.*
  - *Section I. 1) to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, to protect the privacy of others, and to disclose promptly factors that might endanger the public or the environment;*
  - *Section 1. 2) to improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems;*
  - *Section 1. 4) . to avoid unlawful conduct in professional activities, and to reject bribery in all its forms;*
- *Section III. To strive to ensure this code is upheld by colleagues and co-workers.*
  - *Section III. 1) to support colleagues and co-workers in following this code of ethics, to strive to ensure the code is upheld, and to not retaliate against individuals reporting a violation.*

The biggest ethical concern relating to our project involve proper use, testing, and implementation of the project to ensure that the safety of public is not compromised [Section I. 1.], that the intelligent system and emerging technology does not have negative implications in the desired use case [Section 1. 2.], and to avoid breaking the law during testing [Section 1.4.]. As with any project, not only is it important to follow all aspects of the IEEE code of ethics, but also to hold team members to the same standards [Section III.1.].

The various consequences related to our project particularly involve public safety. If testing of the spoofing and spoof detection is done carelessly, the general public may be put in danger, and nearby sensors may be damaged or inhibited. The primary intent of our project is to ensure that design, build, and test of the system is completed safely and successfully to support the customer and help them with the defense of the country. It is important to value both the relationship with the customer, the safety of the technology, and look to work with utmost character to complete this project.

The primary concern with design, development, and testing of our project is related to spoofing. Most types of spoofing are illegal, including LiDAR and GPS. We need to ensure our testing is performed in a private airspace, or an anechoic chamber where there are no potential implications for the safety of the general public. We must also ensure that we follow all government regulations and obtain the proper licenses before performing any flight tests or spoofing. Due to the sensitive nature of our project, it is important that we hold each other accountable while researching, designing, testing, and presenting. The fundamental aspect of the project involves creating a neural network, which is an intelligent system. We must ensure that the use of an intelligent system for spoofing purposes does not break the IEEE code of ethics for this use case. Since LiDAR spoofing is defensive, this does not seem to be a problem.

## Use Case: LiDAR/GPS Spoofing

### 1. Title

- LiDAR and GPS Spoofing of enemy UAVs

### 2. Primary Goal

- Detection of LiDAR probe signals and generation of either a spoofed LiDAR point cloud topography or a spoofed GPS signal.

### 3. Actors

- Primary Actors: Enemy UAV and LiDAR signal detector
- Supporting Actors: Ground station with neural network for spoofing, flight controller, communication station receiving data of spoofed topography/GPS signal, power station, laser pointer.

### 4. Preconditions

- Sensors polling, battery charged, or system powered, neural network trained, and laser or GPS spoofer available with preprogrammed topography.

### 5. Trigger

- Detection of enemy UAV (LiDAR or other signal detection).

### 6. Main Success Scenario (Normal Flow)

- Sensor system in a low power polling mode
- Ground station sensors detect enemy UAV
- Neural network adapts to UAV location to set up preprogrammed GPS and LiDAR topography spoofs for specific orientation
- Laser/GPS spoofer successfully injects signal into enemy UAV sensors until UAV is out of range
- Send data to communication station and return to sleep mode

### 7. Alternative Flows

- If the system does not initially detect enemy UAV, begin spoofing UAV once it is detected
  - Backup battery power if not receiving enough power in the ground station
  - Communication system can update topography to something simpler if the UAV is changing direction too quickly for the neural network to keep up with the spoof
  - Back up lasers in case of initial failure
- 8. Exception Flows (Error Conditions)**
- If things go wrong, the system returns to sleep mode until fixed
  - Ideally there should be redundant systems (ie. Multiple stations per spoof)
- 9. Postconditions (Outcomes)**
- The bad actor (enemy UAV) should have received improper data and go out of range
  - The ground station should transmit information about the encounter as well as the spoof accuracy to the communication station and then return to idle
- 10. Notes / Assumptions**
- The bad actor is trying to create a topographical LiDAR point cloud.
  - System is being used to spoof LiDAR and/or GPS data
  - Enemy UAV is within range of system

## Use Case: Spoof Detection

1. **Title**
  - LiDAR and GPS spoof detection and resilience for UAVs
2. **Primary Goal**
  - Detection of spoofed or anomalous signals based on known spoofing techniques to improve data accuracy
3. **Actors**
  - Primary Actors: Friendly UAV GPS/LiDAR systems and bad actor sending spoofed signal
  - Supporting Actors: Neural network trained with known spoofing techniques, code to eliminate spoofed signal and maintain data integrity if possible, and communication station receiving data from UAV
4. **Preconditions**
  - UAV is currently probing for LiDAR point cloud or relying on GPS data and the system has enough power to run the neural network
5. **Trigger**
  - The bad actor sends a spoofed signal or jam, and the neural network identifies it
6. **Main Success Scenario (Normal Flow)**
  - Friendly UAV with enough power to properly run the system is relying on GPS data for flight and/or creating a topographical LiDAR point cloud
  - Neural network on UAV detects input data from a spoofed signal
  - The system adapts to filter out the spoofed signal and maintain data integrity
  - Proper GPS data is identified and/or LiDAR topography is sent back to communication station and UAV returns to base
7. **Alternative Flows**
  - The system doesn't have enough power to interpret the LiDAR spoof and just has resiliency against GPS spoof to maintain location integrity and return to base
  - LiDAR spoof not properly correct so data is identified as corrupted and is flagged as unreliable

- Backup power systems in case of long flight time and longer than average neural network adjustment
8. **Exception Flows (Error Conditions)**
    - System doesn't have enough power for LiDAR or GPS spoof prevention, in which case it returns to base once spoof has been completed
    - Lack of power to return to base
  9. **Postconditions (Outcomes)**
    - Friendly UAV should be able to identify and remove the spoofed signal, resulting in correct data being sent back to the communication station
    - UAV returns to base undamaged
    - Enemy assumes spoof worked
  10. **Notes / Assumptions**
    - Friendly UAV is probing for LiDAR point cloud or is reliant on GPS for PNT

## Product Requirements

### System Requirements

Category	REQ-#	Requirement	Verification Type
----------	-------	-------------	-------------------

Functional	FUN-1	The UAV shall be capable of spoofing sensor data to mimic various environmental conditions and object types (e.g., buildings, natural terrain, other vehicles).	Flight test to show spoofed outputs of target environments
	FUN-3	The UAV shall be able to dynamically adjust spoofing parameters based on the perceived environment and mission objectives.	Vary spoof parameters in UI and observe
	FUN-4	The UAV shall have the ability to selectively spoof specific sensors or data streams while maintaining the integrity of others	Run tests where only camera is spoofed while LiDAR is not
	FUN-5	The system shall include a user interface (ground station or onboard) to configure spoofing parameters, select spoofing profiles, and monitor spoofing activity	Inspect and test UI screens and selections
	FUN-7	The UAV must have the ability to record the spoofing activity to the local storage including the original sensor data, spoofed sensor data and related parameters	Run scenario, export logs, analyze raw vs spoofed parameters
	FUN-8	The UAV shall incorporate a neural network processing unit capable of real-time analysis of sensor data for environment recognition, target identification, and autonomous spoofing adaptation.	Benchmark inference time on test data

	FUN-9	The system needs to implement methods for uncertainty estimation for the neural networks and detect adversarial inputs that might cause erroneous behavior.	Use adversarial samples
<b>Performance</b>	PER-1	The spoofed sensor data shall be accurate to within 90% of the target environment or object characteristics.	Compare spoofed outputs to baseline data
	PER-2	: The spoofing system shall be capable of maintaining a consistent spoofing profile over a period of 10 minutes.	Run continuous spoof for 10 minutes and check consistency
	PER-3	The neural network processing unit shall achieve a minimum inference speed of target sensor data.	Measure neural network interface latency in ms
	PER-4	The neural network shall have an accuracy of at least 85% in identifying and classifying target objects or environments	Confusion matrix on validation set
	PER-5	The time it takes to retrain the neural network must be less than 30 seconds.	Time retrain cycle on embedded devices
<b>Compliance</b>	COM-1	All sensor spoofing activities are isolated and do not violate FCC law.	Inspect architecture to confirm spoofing isolation (no RF emission)
	COM-2	All drone testing shall comply with FAA requirements.	Check FAA waiver paperwork and inspect flight plan
<b>Environmental</b>	ENV-1	The drone shall be able to operate in the same environments that it spoofs	Operate UAV in test environment while spoofing (chamber)
<b>Reliability</b>	REL-1	The UAV shall have a failsafe mechanism to revert to a non-spoofing mode in case of system failure or critical error.	Kill the spoof module and confirm system returns to regular state
	REL-2	The UAV shall maintain stable flight and navigation even while actively spoofing sensor data.	Measure UAV stability during spoofing test flight
<b>Power</b>	POW-1	The neural network processing unit shall be power-efficient to minimize impact on flight endurance.	Measure power draw under load in comparison to a stable state
<b>Mechanical</b>	ME-1	The UAV shall be able to carry the sensor spoofing payload while maintaining a minimum of 40 feet and speed of 15mph while flying.	Flight test at such speed and altitude with max payload
<b>Input/Output</b>	I/O-1	The UAV shall be able to spoof at least 2 different types of sensor data: GPS, LiDAR,	Demo spoofed LiDAR + camera

		camera imagery (visible and infrared), radar or acoustic sensors.	
	I/O-2	The system shall have a laser.	inspect installation, test safe operation
	I/O-3	The system shall be capable of optical camera, with a 15-25m detection range and 360-degree field of view.	Measure FOV and range under controlled test
Testing	TEST-1	The UAV must be able to log all of the sensor data, spoofed sensor data, neural network data, and control data to local storage for later analysis.	review logs, confirm all streams recorded
	TEST-2	The ground/handheld control station shall be three miles from your control station.	Range test with ground station
Configuration	CON-1	The system shall support the integration of multiple neural network models for different sensor types and spoofing objectives.	Confirm 2 models' execution
	CON-2	The UAV shall be capable of receiving updated spoofing profiles and training data wirelessly.	Confirm updates pushed wirelessly
	CON-3	The neural network shall be trainable and re-trainable in the field with new data.	Perform retain cycle in a realistic scenario
Cost	COST-1	Less than \$500	Cost analysis and BOM inspection
Schedule	SCH-1	System must be presented in a satisfactory state, meeting all requirements before April 26, 2025.	PDR 10/24

## Target Specifications

Target specifications are quantified and provide a rationale. List all assumptions that were made below the table.

Table 01-5 Target Specifications

Req ID	Metric	Units	Marginal Value	Target (Ideal) Value	Traceability / Rationale

<b>PER-2</b>	Sustained time maintaining spoofing profile	Minutes	10 minutes	20 minutes	The spoofing profile should be able to be maintained continuously for the duration of the flight/test.
<b>PER-3</b>	Neural network inference time	Milliseconds	50ms	25ms	Comparable inference times for coprocessors (e.g NVIDIA Jetson). Inference must be real-time to adapt to changing environments and spoofing methods.
<b>PER-4</b>	Neural network classification accuracy	Accuracy percentage	85%	90%	Given enough data, and since the data model can be retrained with new samples while deployed, it should reach 90 percent accuracy.
<b>PER-5</b>	Neural network retrain time	seconds	30	20	Assuming fine-tuning scenarios from a base model, maximize accuracy thus using the maximum training time per the requirements.

Table 01-6 Standards and Statutory Requirements

This table supports the compliance requirements in the requirements spreadsheet.

Req. #	Requirement	Source Document (e.g., standard, regulatory requirements)	Details
COM-1	The sensor spoofer shall not interrupt services with legitimate users	Communications Act of 1934, 18 U.S.C. § 1367(a)	Any device designed to “intentionally block, jam, or interfere with authorized radio communications” is illegal with no academic exemptions. Testing should be done in a reasonably controlled environment
COM-2	Drone operation & construction shall respect all relevant laws	Code of Virginia 4VAC5-30-400, U.S.C §4480	The UAV has to be registered (N/A if lending) since it will likely be over 0.55 lbs. Recreational drone operations require line-of-sight, which makes TEST-2 requirement difficult, need to mimic such distances in test procedure.

## Benchmarking Information

Table 01-7 Benchmarking Information

Feature / Requirement	Target Requirement	<existing alternative #1>	<existing alternative #2>	<existing alternative #3>
<b>PER-2</b> Sensor spoofing detection accuracy	85%	90%	45%	37%

Note that direct comparisons to existing systems is difficult since many implementations do not use a neural network-based approach for detecting/changing spoofing methods.

## References

[1] IEEE, "IEEE Code of Ethics | IEEE," [ieee.org](https://www.ieee.org/about/corporate/governance/p7-8), 2020.  
<https://www.ieee.org/about/corporate/governance/p7-8>

[2] R. Nagata et al., "SLAMSpoofer: Practical LiDAR Spoofing Attacks on Localization Systems Guided by Scan Matching Vulnerability Analysis," [arXiv.org](https://arxiv.org/abs/2502.13641), 2025.  
<https://arxiv.org/abs/2502.13641>

[3] rnl-admin, "GPS spoofing affecting civilians in the Middle East – Radionavigation Laboratory," [Utexas.edu](https://radionavlab.ae.utexas.edu/gps-spoofing-affecting-civilians-in-the-middle-east/), 2024. <https://radionavlab.ae.utexas.edu/gps-spoofing-affecting-civilians-in-the-middle-east/> (accessed Oct. 02, 2025).