UNCLASSIFIED

# Joint Interagency Task Force 401

# Common Criteria for CUAS Characterization (C4)



















**1 May 2026**

## Message from the Director

Teammates,

The threat posed to our nation by small, unmanned aircraft systems (sUAS) spans military, homeland security, and law enforcement responsibilities. Once considered hobbyist tools, sUAS have transformed into threat multipliers capable of disrupting operations, conducting surveillance, and delivering harmful payloads. The proliferation of sUAS provides precision reconnaissance and strike capabilities to individuals and small groups previously reserved for nation-state militaries. They are inexpensive, adaptable, and lethal.

JIATF 401's mission is to synchronize the DoW's counter-drone efforts to rapidly deliver joint capabilities at scale to protect US and allied forces and assist federal agencies and departments in defending critical infrastructure and the homeland. The JIATF's one measure of effectiveness is to quickly deliver state of the art C-sUAS capabilities into the hands of warfighters. Achieving this outcome requires more than innovation; it demands a disciplined approach to testing, evaluation, and continuous improvement that translates promising technologies into operationally relevant solutions at scale. In this dynamic environment, JIATF 401 will act decisively to accelerate delivery of C-sUAS technologies to protect personnel, facilities, and assets. By prioritizing rapid innovation and scalable solutions, our Joint Forces and Interagency partners keep pace with the threat.

To ensure warfighters and state, local, territorial, and tribal law enforcement are equipped with the most effective systems, JIATF 401 must establish standardized assessment protocols that enable objective comparisons for informed procurement decisions. A unified framework is essential for fostering interoperability, accelerating fielding, and ensuring results are comparable across all domains.

This Common Criteria for CUAS Characterization (C4) establishes the foundation for C-sUAS evaluations and assessments. The guidelines enclosed are not a replacement for other established developmental, operational tests, or safety certifications conducted by the Services and the interagency. Rather, what we provide here is an authoritative approach for accelerating the evaluation of commercial C-sUAS technologies. By providing common criteria, we ensure consistency, scalability, and speed in evaluating emerging C-sUAS technologies while leveraging advanced modeling and simulation tools to inform analysis.

As C-sUAS technologies evolve, this framework will adapt to meet the complexity of threats while maintaining a consistent methodology that ensures commonality and operational effectiveness across the Joint Force and Interagency partners.

Matthew S. Ross
Brigadier General, U.S. Army
Director, Joint Interagency Task Force 401

# Table of Contents

## Contents

Message from the Director ..... i

1. INTRODUCTION ..... 1

2. ORGANIZATIONAL ROLES & RESPONSIBILITIES ..... 1

3. THREAT CHARACTERIZATION ..... 2

4. C-sUAS CAPABILITY CHARACTERIZATION CRITERIA ..... 3

4.1 Core Capability Areas (Detect, Track, Identify, Defeat) ..... 3

4.2 Key Performance Benchmarks ..... 5

4.2.1 Examples for Detect KPPs ..... 5

4.2.2 Examples for Track KPPs ..... 6

4.2.3 Examples for Identify and Characterize KPPs ..... 6

4.2.4 Examples for Target Quality KPPs ..... 7

4.2.5 Examples for Defeat KPPs ..... 7

4.2.6 Examples for Automation KPPs ..... 8

4.2.7 Examples for C2 KPPs ..... 9

4.2.8 Examples for Survivability KPPs ..... 9

4.2.9 Examples for Ancillary System Characteristics KPPs ..... 9

4.2.10 Examples for Cost KPPs ..... 10

4.3 Operator & System Usability ..... 10

4.4 Mission Impact & Risk Assessment ..... 10

4.4.1 Public and Blue Force Safety Assessment ..... 10

4.4.2 System Resilience to Countermeasures ..... 11

5. EVALUATION METHODOLOGIES & DESIGN ..... 11

5.1 Evaluation Principles ..... 12

5.2 Scenario Design ..... 14

*5.2.1Example test matrix* ..... 14

5.3 Evaluation Environment ..... 15

5.4 Mission Engineering (ME) and Modeling & Simulation (M&S) for Assessment ..... 16

6. DATA COLLECTION & ANALYSIS ..... 16
7. REPORTING & DATA MANAGEMENT ..... 16
Appendix A - Acronyms & Abbreviations ..... A-1
Appendix B - Government References ..... B-1

# 1. INTRODUCTION

Despite years of dedicated testing and significant investment across the Department of War (DoW), the Counter-small Unmanned Aircraft Systems (C-sUAS) enterprise faces a significant paradox: we are data-rich but information-poor. A vast and growing repository of test data, representing gigabytes of effort from countless evaluations, remains largely unusable for enterprise-level analysis. We lack a holistic process for curating our test data for improving decision-making. The lack of common criteria and evaluation standards, combined with data existing in disparate silos of unknown provenance and inconsistent quality, makes it nearly impossible to aggregate, compare, or leverage data for strategic insights.

Standards provide the common lexicon and schemas necessary to transform our approach to informing rapid assessment and acquisition of C-sUAS technologies. This approach establishes the principles that every test event, demonstration, operational assessment, or technical assessment is a data collection opportunity that must not be wasted. By requiring that all evaluations capture sets of core data points, JIATF 401 will be able to systematically aggregate and synthesize information, creating a single, coherent, and reliable body of evidence from all evaluation events across the DoW.

The adoption of these common critiera is the critical enabler for the future of C-sUAS development. High-quality data serves as the essential element for advanced Mission Engineering tools and Modeling & Simulation (M&S) environments. It will allow for more rigorous system comparisons, robust analysis of capability gaps, and high-fidelity predictions of operational performance in scenarios that are too costly or complex for live testing alone. Ultimately, by creating a coherent and reliable body of evidence, this approach will directly inform and improve decision-making, accelerating the delivery of the most effective, reliable, and integrated C-sUAS technologies to the warfighter and interagency partners.

# 2. ORGANIZATIONAL ROLES & RESPONSIBILITIES

**JIATF 401**: Provides and maintains the C4 and publishes applicable guidance on sUAS threats.

Key Duties: Coordinates test and evaluation resources as necessary to support C-sUAS evaluations. Coordinates with the appropriate resource manager for consolidating and organizing all test and evaluation data produced from an event and ensures that it is made available to all stakeholders.

**C-sUAS Evaluator**: An entity that analyzes and evaluates C-sUAS for performance, reliability, safety, and survivability.

Key Duties: Defines evaluation objectives based on defined Measures of Effectiveness/Performance (MOE/MOP), observes evaluation execution, adjudicates incidents, generates final reports, including the Capabilities & Limitations (C&L) Report and Safety Release.

**Range Operations**: Responsible for all logistical, instrumentation, and facility support required to execute an evaluation.

Key Duties: Manages evaluation site setup, range scheduling (airspace/surface), frequency authorizations, data collection, OPSEC, EOD support, and coordination of all equipment and supplies.

**Analysis Team**: The central hub for processing all raw test and evaluation data into a usable format for analysis.

Key Duties: Reduces and analyzes data, identifies and reports system performance issues, and provides quick-look summaries to the appropriate evaluators and other stakeholders.

**Threat Analysis and Planning Team**: A cross-service function responsible for defining threat context for all testing.

Key Duties: Establishes threat profiles, develops threat Tactics, Techniques, and Procedures (TTPs), and collaborates with test planners to ensure threat-representative configurations are consistently and appropriately used during testing.

**Modeling & Simulation (M&S) Analyst**: Responsible for creating, validating, and executing digital models of the C-sUAS, threats, and operational environment to support and expand upon live test events and decision-making.

Key Duties: Develops and maintains high-fidelity models of C-sUAS systems and threats; conducts Verification, Validation, and Accreditation (VV&A) of simulations against live test data; designs and runs virtual test scenarios, including those beyond the scope of live testing (e.g., large-scale swarms); and provides M&S data to Mission Engineering and Analysis teams.

**Mission Engineering Analyst**: Responsible for analyzing the end-to-end performance of the C-sUAS kill chain to assess the system's operational effectiveness and its overall impact on mission success.

Key Duties: Conducts Engagement Timeline Analysis (ETA) to identify kill chain bottlenecks; performs trade space analysis using live and simulated data; links system-level Measures of Performance (MOPs) to mission-level Measures of Effectiveness (MOEs); assesses system performance against defined enemy courses of action; and identifies capability gaps to inform future requirements.

## 3. THREAT CHARACTERIZATION

Hostile sUAS present a dual threat to U.S. forces through intelligence, surveillance, and reconnaissance (ISR) operations and direct kinetic attacks. In response, any C-sUAS system must be scalable, modular, and easily upgradable. Within this context, "defeat" is defined as any action, kinetic or non-kinetic, that neutralizes a hostile UAS and prevents it from completing its intended mission.

Enemy sUAS are increasingly difficult to detect, classify, and defeat as the commercial market produces faster and smaller platforms. To keep pace with this rapidly evolving threat, C-sUAS capabilities must be adaptable and joint in nature. Future C-sUAS operations will be part of a larger, multi-domain effort requiring integrated capabilities that can be quickly adapted to any operational

environment. This will be achieved through an open, modular architecture that leverages a system-of-systems approach.

# 4. C-sUAS CAPABILITY CHARACTERIZATION CRITERIA

## 4.1 Core Capability Areas (Detect, Track, Identify, Defeat)

This section consolidates a recommendation of the most critical MOEs and MOPs for evaluating the end-to-end performance of C-sUAS systems against Group 1-2 UAS threats[1]. These common MOEs and MOPs are a baseline. Nothing in this document prohibits C-sUAS system evaluators from screening additional criteria. Evaluators must evaluate which criteria (or sections of criteria) are actually relevant to their assessment efforts. A unified time reference is essential in the measurement of these MOEs and MOPs .

*4.1.1 Criterion 1 - Detection & Tracking*: The system's ability to find and maintain awareness of sUAS threats through all modalities.

### MOE 1.1: UAS Detection

MOP 1.1.1: Probability of Detection: The proportion of hostile UAS correctly detected by the system.

MOP 1.1.2: Detection Range (ground): The distribution of ranges at which initial detection occurs.

MOP 1.1.3: Detection Range (slant range): The distribution of ranges and altitude at which initial detection occurs.

MOP 1.1.4: False Alarm Rate: The number of false sUAS detections per unit of time.

### MOE 1.2: UAS Tracking

MOP 1.2.1: Probability of Track: The proportion of detected sUAS that are successfully tracked.

MOP 1.2.2: Track Continuity: The percentage of time a stable track is maintained on a sUAS.

MOP 1.2.3: Track Accuracy: The 3D positional error of the track compared to ground truth.

*4.1.2 Criterion 2 - Classification & Identification*: The system's ability to determine the nature of a detected threat.

### MOE 2.1: Target Classification & Identification

MOP 2.1.1: Probability of Correct Classification: The proportion of sUAS correctly classified by the system.

[1] Evaluators should reference The Department of Defense Unmanned Aircraft Categorization Review Report to Congress, November 2022.

MOP 2.1.2: Probability of Correct Identification: The proportion of sUAS correctly identified by type/model.

MOP 2.1.3: Identification Range & Time: The distribution of ranges and times at which correct identification is achieved.

MOP 2.1.4: Mis-Identification Rate: The proportion of sUAS that are incorrectly identified.

*Criterion 3 - Threat Defeat & Denial*: The system's ability to neutralize a hostile UAS and prevent it from completing its mission.

### MOE 3.1: Threat Engagement & Defeat

MOP 3.1.1: Probability of Engagement: The proportion of identified hostile sUAS that are engaged by the system.

MOP 3.1.2: Probability of Kill/Defeat ($P_K$): The proportion of engaged sUAS that are successfully defeated or denied their mission.

MOP 3.1.3: Defeat Range: The distribution of ranges at which the sUAS is successfully neutralized.

MOP 3.1.4: Defeat engagement time: The measure of time from the engagement command to successful defeat.

*Criterion 4 - System Interoperability & Reliability*: The system's ability to operate effectively within its intended environment and alongside other systems.

### MOE 4.1: Electromagnetic Compatibility

MOP 4.1.1: Impact on Co-located Systems: Characterize the frequency, power, and different modalities of the system and how these might affect nearby systems.

MOP 4.1.2: Impact to ordnance, personnel, and fuel: Determine Hazard Electromagnetic Radiation to Ordnance (HERO), Hazard Electromagnetic Radiation to Personnel, and Hazard Electromagnetic Radiation to Fuel (HERF).

### MOE 4.2: System Reliability & Maintainability

MOP 4.2.1: Mean Time Between System Abort (MTBSA): The average operating time between critical system failures that halt the mission.

MOP 4.2.2: Mean Time to Repair (MTTR): The average time required to diagnose and repair a system failure, excluding administrative or logistics delays.

*Criterion 5 - Operational Viability*: The system's ability to be safely and effectively operated by trained personnel in a mission environment.

### MOE 5.1: Cybersecurity

MOP 5.1.1: Risk Management Framework (RMF) Compliance: The system is compliant with the RMF and has received an Authority to Operate (ATO) and Authority to Connect (ATC).

### MOE 5.2: Environmental Survivability

MOP 5.2.1: Contested Environment Operation: The system must not experience degradation from threat Electronic Warfare (EW).

### MOE 5.3: System Safety

MOP 5.3.1: Hazard Prevention: The system design shall eliminate or control potential health and safety hazards to personnel, including musculoskeletal, noise, radiation, and chemical risks, in accordance with established military standards.

MOP 5.3.2: Collateral Damage Mitigation: The system shall successfully exchange restricted firing sectors with the C2 system to minimize collateral damage and prevent fratricide.

## 4.2 Key Performance Benchmarks

This section outlines the Key Performance Parameters (KPPs) and Key System Attributes (KSAs) that define the essential operational capabilities for many C-sUAS systems. KPPs represent the most critical attributes that a system must achieve to be considered militarily effective; failure to meet a KPP indicates that the system is incapable of fulfilling its intended mission. For each KPP presented, performance is defined by two distinct levels: a Threshold and an Objective. The Threshold value represents the minimum acceptable performance required for the system to be effective, while the Objective value represents the desired capability or a significant increase in operational utility.

To ensure an objective assessment, evaluators must formally define and document the specific numerical values for both the Threshold and Objective for each KPP prior to test execution. These pre-established benchmarks are not merely for post-test analysis; they must be explicitly integrated into the data collection plan to ensure the test is designed to capture the precise data needed to render a clear judgment. During test and evaluation, evaluators will collect this data by executing structured test scenarios, and the final assessment will explicitly state whether the system met the "Threshold," fell short, or achieved the "Objective" for each KPP.

### 4.2.1 Examples for Detect KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 1.1 | Range | km | The minimum distance from desired standoff the system must detect a threat. |
| KPP 1.2 | Accuracy | % | The probability of detection of a threat at the minimum distance range. |
| KPP 1.3 | Field of View | deg | The ability to detect sufficiently greater than the mission requirement and provide sufficient coverage. |
| KPP 1.4 | Min Altitude | m | The minimum altitude (in meters) above ground level (AGL) to detect at the minimum range. |

| | | | |
|---|---|---|---|
| KPP 1.5 | Max Altitude | m | The maximum altitude (in meters) above ground level (AGL) to detect at the minimum range. |
| KPP 1.6 | Quantity | # | The minimum number of targets with the specified radar cross section (RCS) that can be simultaneously detected at the minimum range. |
| KSA 1.7 | Automation | Y/N | The system automatically recognizes detections as tracks which include velocity and movement, which is displayed visually in the C2. |
| KPP 1.8 | Resolution | m | The distance at which the sensor can resolve different standard target sizes. |

### 4.2.2 Examples for Track KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 2.1 | Range | km | The minimum distance from the designated boundary to continuously track/maintain awareness of a threat from the desired standoff. |
| KPP 2.2 | Accuracy | +/- % | The percent deviation from the true position and speed of a target being tracked at range and the sensor reported position and speed. |
| KPP 2.3 | Quantity | # | The minimum number of targets with the specified RCS that can be simultaneously tracked within the tracking range area. |
| KPP 2.4 | Automation | Y/N | Does the system automatically maintain awareness of target maneuvers? |
| KSA 2.5 | Update / Revisit Rate | per sec | The amount of time for all of the tracks to be updated/refreshed by the system. |

### 4.2.3 Examples for Identify and Characterize KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 3a.1 | Range | km | The minimum distance to determine positively that the target is a sUAS. |
| KPP 3a.2 | Accuracy | % | The probability of classification of a threat at the minimum categorization range. |
| KSA 3a.3 | Automation | Y/N | Does the system perform automated sensor fusion to classify the target as a sUAS? |
| KPP 3b.1 | Range | km | The minimum distance at which the system can identify the type, make, model, or other identifying features of the sUAS. |
| KSA 3b.2 | Automation | Y/N | Does the system perform automated sensor fusion to identify the sUAS specific features? |

### 4.2.4 Examples for Target Quality KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 4.1 | Range | km | The minimum distance from the sensor to achieve weapons-quality data on the threat. |
| KPP 4.2 | Accuracy | % | The probability of obtaining weapons-quality data at the minimum target range. |
| KSA 4.3 | Quantity | # | The number of simultaneous targets that have been categorized and identified as threat sUAS with weapons-quality information on. |
| KSA 4.5 | Automation | Y/N | Does the system provide weapons-quality information automatically without input from the operator? |

### 4.2.5 Examples for Defeat KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 5.1 | Range | km | The minimum distance from the weapon to defeat a sUAS threat. |
| KPP 5.2 | Quantity (Simultaneous) | # | The number of drones the system can simultaneously defeat to the $P_k$ percentage. Example: "Simultaneous defeat is defined to mean multiple (#) of UAS targets defeated in less than X second(s) from a single effector." |
| KPP 5.2a | Quantity | # | Number of drones an attack can simultaneously assume control. |
| KPP 5.2b | Quantity | # | Number of drones a narrow band RF system can simultaneously attack. |
| KPP 5.2c | Quantity | # | Number of drones a laser can defeat within a unit of time. |
| KPP 5.2d | Quantity | # | Number of drones a high-power microwave weapon can simultaneously defeat. |
| KPP 5.2e | Quantity | # | Number of drones a kinetic system can simultaneously defeat. |
| KPP 5.3 | Quantity (Over Time) | #/hour | The number of drones that the system must defeat over a period of time to the $P_k$ percentage. |
| KPP 5.4 | Effectiveness | % | The percent ($P_k$) to defeat all drones within the required minimum distance. Must define total # of 'soft' kills and 'hard' kills. Evaluation must define 'soft' and 'hard' kills before evaluation. |
| KPP 5.4a | Effectiveness | % | $P_k$ of drones an attack can simultaneously assume control (i.e., electronic takeover). |
| KPP 5.4b | Effectiveness | % | $P_k$ of drones a narrow band RF system can simultaneously attack. |
| KPP 5.4c | Effectiveness | % | $P_k$ of drones a laser can defeat within a unit of time. |

| | | | |
|---|---|---|---|
| KPP 5.4d | Effectiveness | % | $P_k$ of drones a DE weapon can simultaneously defeat. |
| KPP 5.4e | Effectiveness | % | $P_k$ of drones a kinetic system can simultaneously defeat. |
| KPP 5.5 | Launcher Capacity | Qty. | Number of rounds. Additionally, evaluator should note capacity of magazine(s), pod(s), and/or missile capacity. |
| KPP 5.5 | Cyclic Rate | Rounds/minute | Rate of fire. Note: Depending on the system, the evaluator can consider other measures appropriate to the technology (e.g., time between engagements). |
| KPP 5.6 | Number of engagements per interceptor | Qty. | Interceptor's ability to handle one or more engagements simultaneously. Evaluator shall note if an effector has multiple interceptors. |
| KSA 5.7 | Collateral Effects/Damage | Y/N | Does the system accomplish the defeat objectives while operating within the acceptable parameters of collateral effects/damage? Optionally, an evaluator may classify degradation or damage by a percentage, if objectively measurable. |
| KPP 5.8 | Cost per engagement | $ | Total cost / Total # of Successful Engagements. |

### 4.2.6 Examples for Automation KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 6.1 | Workload | # ppl | The number of people required to operate the system. |
| KSA 6.2 | Decision Aids | Spec. | ID Recommendation. |
| KSA 6.2a | Decision Aids | Y/N | Weapons Pairing. |
| KSA 6.2b | Decision Aids | Y/N | Engagement Zone (earliest & latest). |
| KSA 6.2c | Decision Aids | Y/N | Time to intercept / impact. |
| KSA 6.2d | Decision Aids | Y/N | Engagement success. |
| KSA 6.2e | Decision Aids | Y/N | Collateral effects. |
| KSA 6.2f | Decision Aids | Y/N | Sensor Fusion. |
| KSA 6.2g | Decision Aids | Y/N | Audible alerts. |
| KPP 6.3 | Workload | # ppl | The number of people required to setup the system. |

### 4.2.7 Examples for C2 KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 7.1 | Architecture | Spec. | Open / Closed / Proprietary Software & integration options. |
| KPP 7.2a | Interoperability | Y/N | Sensor integration. |
| KPP 7.2b | Interoperability | Spec. | Data integration. |
| KPP 7.2c | Interoperability | Spec. | Interface Development. |
| KPP 7.3 | Common Operating Picture (COP) | # | # of displays and HMI units that the operator must use to monitor and consummate an engagement. |
| KSA 7.4 | Classification | Y/N | Ability to ingest multi-level security data with an overall up to XXX classification (provide classification level). |
| KSA 7.5 | Networkability | Y/N | Ability to connect systems via a network interface. |

### 4.2.8 Examples for Survivability KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 8.1 | IP Rating | Y/N | Min Ingress Protection Code Certification / Rating of XXX |
| KSA 8.2 | Resilient | Y/N | Ability to operate in a contested environment |
| KSA 8.3 | Vulnerability | Y/N | Cybersecurity Risk Present |
| KSA 8.3a | Vulnerability | Y/N | Component Manufacturer or place of Origin |
| KSA 8.3b | Vulnerability | Y/N | Unsecure or misconfigured network connection |
| KSA 8.3c | Vulnerability | Y/N | Data handling or transfer/purposeful or accidental human interaction |
| KPP 8.4 | Reliability | Time | Time between system failures |
| KPP 8.5 | System Spec | Spec. | Network (logical/Physical) |
| KPP 8.6 | System Spec | Y/N | Corrosion |
| KPP 8.7 | System Spec | Spec. | CPU |
| KPP 8.8 | System Spec | Spec. | Hardware |
| KPP 8.9 | System Spec | Version | Software |
| KPP 8.10 | System Spec | List | External Components |
| KPP 8.11 | System Spec | List | Environmental |

### 4.2.9 Examples for Ancillary System Characteristics KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 9.1 | Battery Life | Hrs. | Battery life duration |
| KPP 9.2 | Weight | Lbs. | System weight |
| KPP 9.3 | Labor Cost | $ | Cost of personnel |
| KPP 9.4 | Setup | Time | System emplacement |

### 4.2.10 Examples for Cost KPPs

| KPP | Measure | Units | Description |
|---|---|---|---|
| KPP 10.1 | System Cost | $ | Cost of system procurement and initial installation |
| KPP 10.2 | Component Cost | $ | Cost of individual component system and installation |
| KPP 10.3 | Maintenance Cost | $ | Lifecycle cost of |
| KPP 10.4 | Labor Cost | $ | Cost of personnel |

## 4.3 Operator & System Usability

The capabilities of a C-sUAS are irrelevant if its operator cannot use it effectively under pressure. Operator and system usability assesses the critical sociotechnical systems aspects, recognizing that the system operator is an integral component of the kill chain and overall system effectiveness. In a high-stress, multi-target environment, operators are inundated with data from disparate sensors; a poorly designed system can lead to information overload, high cognitive load, and slow, error-prone decision-making. Therefore, any evaluation must focus on the clarity and intuitiveness of the user interface (UI) and user experience (UX), scrutinizing how effectively the system fuses complex data into a clear, actionable common operating picture. The objective is to ensure the system empowers the operator by reducing cognitive load and enabling rapid, confident decisions. Evaluators will use one or more of the accepted human factors assessments as deemed appropriate for their evaluation:

- NASA Task Load Index (TLX)
- Situation Awareness Global Assessment Technique (SAGAT)
- System Usability Scale (SUS)

## 4.4 Mission Impact & Risk Assessment

A mission impact and risk assessments provide a holistic evaluation that moves beyond technical performance to answer the ultimate question: does this C-sUAS provide a net positive effect on the overall mission? A mission impact analysis assesses the system's direct contribution to protecting the defended asset and enabling friendly operations, while also considering any negative impacts, such as its logistical footprint, power requirements, or potential interference with friendly systems. Conversely, a risk assessment quantifies the consequences of both action and inaction. It weighs the risk of a threat successfully completing its mission against the risks generated by the C-sUAS itself, including the potential for collateral damage from kinetic debris fields or the electromagnetic effects of non-kinetic systems. This comprehensive assessment forces evaluators to make a balanced judgment, ensuring that a C-sUAS is not only effective but also operationally suitable and safe for its intended environment.

### 4.4.1 Public and Blue Force Safety Assessment

A comprehensive safety assessment is a prerequisite for all C-sUAS testing and evaluation, ensuring the protection of both the public and friendly forces. This evaluation must rigorously analyze all

potential hazards, from the predictable debris fields of kinetic intercepts and the far-reaching electromagnetic effects of non-kinetic systems to the uncontrolled descent of a neutralized UAS. The assessment culminates in the establishment of clear safety footprints, and real-time monitoring procedures designed to mitigate all identified risks, thereby ensuring that test objectives can be achieved without compromising personnel or public safety.

### 4.4.2 System Resilience to Countermeasures

System Resilience to Countermeasures testing is a critical and advanced phase of C-UAS evaluation that shifts the focus from "what the system can do" to "what can be done to the system." Its purpose is to rigorously assess a C-UAS's ability to maintain its core functions—detect, track, identify, and defeat—while being actively targeted by an adversary in a contested operational environment. This form of testing is fundamental to understanding a system's true survivability and mission assurance, as it assumes that enemy forces will not be passive targets but will instead employ their own tactics to disrupt or disable friendly defensive capabilities.

## 5. EVALUATION METHODOLOGIES & DESIGN

The ultimate measure of a C-sUAS is not merely its ability to defeat a threat, but its ability to do so *in time* to protect a defended asset. The Engagement Timeline Analysis is a critical evaluation framework designed to dissect the C-sUAS kill chain into a series of discrete, measurable time gates. By quantifying the duration of each phase from initial detection to final neutralization, evaluators can move beyond a simple pass/fail assessment to a more comprehensive understanding of a system's speed, efficiency, and operational viability.

This framework is designed to be applied against a spectrum of defined threat scenarios, most notably the enemy's Most Likely Course of Action (MLCOA) and Most Dangerous Course of Action (MDCOA). This ensures the system is evaluated not only under expected conditions but also stressed against the scenarios that pose the greatest challenge to its performance and the safety of the defended asset.

Before any timeline analysis can begin, the threat scenarios that will serve as the evaluation criteria must be clearly defined. These scenarios dictate the conditions under which the timeline is measured.

| Scenario Element | Most Likely Course of Action (MLCOA) Examples | Most Dangerous Course of Action (MDCOA) Examples |
|---|---|---|
| **Threat Profile** | A single, commercially available Group 1 or 2 sUAS (e.g., quadcopter). | A coordinated swarm of multiple Group 1/2 UAS, potentially mixed with a high-speed Group 3 fixed-wing sUAS. |

| | | |
|---|---|---|
| **Flight Profile** | A predictable, relatively slow flight path (e.g., 20-30 mph) at a medium altitude (e.g., 200-400 ft AGL). | A high-speed, low-altitude ingress profile (terrain masking) on a direct attack vector. May include pop-up maneuvers or jinking. |
| **Mission Objective** | Intelligence, Surveillance, and Reconnaissance (ISR), loitering outside a known perimeter. | A saturation attack designed to overwhelm defenses and kinetically impact a specific, high-value asset. |
| **Electronic Signature** | Standard, unmodified RF command-and-control link. | RF-silent operation (GPS waypoint navigation), potentially coupled with active electronic attack (jamming) against C-sUAS sensors. |

**Baseline Performance (MLCOA)**: The timeline analysis is first run against the MLCOA scenario. This establishes the system's baseline performance under expected, low-stress conditions.

**Performance Under Stress (MDCOA)**: The analysis is then run against the MDCOA scenario. This is where the true resilience of the system is tested.

**Expected Outcomes**: Evaluators will likely see an increase across all delta times. The Time to Detect may increase due to jamming. The Time to Decide may increase significantly as the operator is saturated by multiple tracks. The Time to Effect for kinetic systems may increase as they must engage multiple targets sequentially.

**Comparative Analysis**: The framework provides a standardized, quantitative basis for comparing different C-sUAS systems. Instead of a simple: System A had 8 kills and System B had 7, the analysis can state, System A had a faster Total Engagement Time against single targets, but its Decision-Action Latency degraded by 300% during the swarm attack, whereas System B's performance remained consistent, making it more resilient to saturation.

## 5.1 Evaluation Principles

To ensure that the testing and evaluation of C-sUAS is rigorous, credible, and produces actionable insights, all evaluators should adhere to the following core principles. These principles are designed to move beyond simple performance metrics to a holistic assessment of a system's true operational utility and mission effectiveness.

**Mission-Focused Evaluation**: The ultimate measure of a C-sUAS is not its technical specifications, but its ability to successfully protect a defended asset. All test scenarios, data collection, and analysis must be explicitly tied to a clear operational mission. The central question should always be: Does the system enable mission success under realistic conditions? This principle requires

evaluators to assess performance within the context of the complete kill chain and against defined threat timelines, rather than evaluating components in isolation.

**Test Against a Credible and Diverse Threat**: A system is only as good as the threat it can defeat. Evaluations must be conducted against a spectrum of threats that accurately represent both the Most Likely and Most Dangerous enemy courses of action. This includes a diverse range of sUAS platforms (Groups 1-3, fixed-wing, multi-rotor), varying mission profiles (ISR, kinetic attack), and advanced tactics such as swarming, low-altitude ingress, and RF-silent operations. Testing against a single, simplistic threat profile will produce misleading and overly optimistic results.

**System-of-Systems Approach**: Modern C-sUAS are rarely monolithic solutions. Evaluations must treat the C-sUAS as an integrated system-of-systems, assessing not only the performance of individual sensors and effectors but also the quality of the data fusion, the efficiency of the C2 workflow, and the interoperability between components. A technically superior sensor is of little value if its data cannot be effectively utilized by the rest of the architecture.

**Quantify Performance in a Contested Environment**: A C-sUAS must be assumed to operate in an environment where the adversary is actively working to disrupt it. Therefore, evaluations must include dedicated Red Teaming events to test the system's resilience to countermeasures. This involves subjecting the system to plausible electronic attack (jamming/spoofing) and sensor saturation tactics to measure performance degradation under duress and identify critical vulnerabilities.

**The Operator is Part of the System**: Except in fully autonomous systems, the human operator is a critical component of the C-sUAS. An evaluation should assess Human-in-the-Loop (HITL) performance, measuring operator workload, situational awareness, decision-making accuracy, and trust in automation. A system with a confusing interface or one that induces high cognitive load is a system that will fail under stress, regardless of its technical potential.

**Adherence to Common Standards for Data-Driven Decisions**: To ensure that evaluation results are comparable, aggregable, and can inform enterprise-level decisions, all data collection and reporting must adhere to a common, standardized formats. This principle ensures that every test event, regardless of the service or agency, contributes to a larger body of evidence. This curated data is the essential fuel for advanced Modeling & Simulation (M&S) and Mission Engineering (ME) efforts that allow for deeper analysis and more informed investment decisions.

JIATF 401 recognizes that every test, demonstration, and evaluation will have a unique set of objectives and constraints. Therefore, participating organizations are strongly encouraged to coordinate with JIATF 401 early in the planning process to discuss their specific requirements. This early collaboration will allow the JIATF to recommend the most effective data collection strategy, ensuring that unique event objectives are met while still aligning with the common data standard for enterprise-wide aggregation.

**Rigorous Safety and Collateral Effects Assessment**: The protection of friendly forces and the public is the non-negotiable prerequisite for any test and evaluation event. A rigorous safety assessment must precede all live testing, keep out zones, safety stand-offs, range safety officers, establishing clear safety footprints and rules of engagement. Furthermore, evaluations must include a formal methodology for measuring and characterizing the potential collateral effects of the C-sUAS, including kinetic debris fields and electromagnetic interference, to ensure the system is not only effective but also safe and suitable for its intended operational environment.

## 5.2 Scenario Design

Effective C-sUAS scenario design is the cornerstone of any meaningful test and evaluation effort, as it provides the essential context against which system performance is measured. It transforms testing from a simple technical measurement into a mission-focused assessment by creating a realistic operational narrative. A well-designed scenario meticulously defines the threat profile, the complexity of the physical and electromagnetic environment, and the specific tactics the sUAS will employ. This rigor ensures that a C-sUAS is not just evaluated against a spec sheet, but is truly stressed against credible, challenging conditions, providing the only reliable way to validate its true operational effectiveness.

### *5.2.1Example test matrix*

This notional test matrix outlines a series of complex flight scenarios, detailing the specific test conditions for both fixed-wing and multi-rotor UAS. For each test run, it varies key parameters such as launch points, flight paths, speeds, and altitudes. To maintain clarity, variables that remain constant throughout the event (e.g., C-sUAS location, navigation mode) should be documented separately rather than repeated in the table. It is also highly recommended to supplement this matrix with visual diagrams of the flight routes to enhance situational awareness for the evaluation team.

| Test Matrix (Sample) | | | | | | | |
|---|---|---|---|---|---|---|---|
| Profile | Mission | Target Platform | Elevation (ft AGL) | Speed (mph) | Time | LP | Data Points |
| R-1 | ISR | Raider | 400 | 20 | Day | 11/17 | 3 |
| R-2 | OWA | C5ISR FPV | 100 | 60 | Night | 11 | 3 |
| F-1[a] | OWA (S-Curve) | Talon Pro | 800 | 70 | Day | 11/53 | 3 |
| F-2 | OWA | Mojito | 3000 | 125 | Night | 51B | 3 |
| M-1 | MULTI-ISR | Raider | 1000 | 39 | Day | 51B | 2 |
| | | C5ISR FPV | 400 | 80 | | 11 | |
| | | Squidhawk 1200 | 100 | 30 | | 10 | |
| M-2[b] | MULTI-OWA | Raider | 500 | 39 | Day | 51B | 2 |
| | | Mojito | 1000 | 125 | | 53 | |
| | | Mavic Pro | 1500 | 46 | | 11 | |

NOTE: The M-1 and M-2 mission profiles will be conducted with three UAS and different LPs, with the three UAS operating concurrently.

[a] The F-1 profile will have the platform perform a large S-curve (turn) for the profile instead of direct.
[b] The M-2 profile will consist of a coordinated launch so that all targets to arrive staggered by approximately 10 seconds.

**Table 2.1–4. Replicator 2 Defeat Performance Test Matrix (Concluded)**

LEGEND:

| | | | |
|---|---|---|---|
| AGL | – Above Ground Level | ISR | – Intelligence, Surveillance, and Reconnaissance |
| C5ISR | – Command, Control, Communications, Computers, Cyber, ISR | LP | – Launch Point |
| | | MULTI | – Multiple |
| FPV | – First Person View | OWA | – One Way Attack |

*Figure 1* – Notional Test Matrix

## 5.3 Evaluation Environment

The evaluation environment is one of the most critical variables in C-sUAS testing, as it directly influences a system's performance and the validity of the results. The ultimate goal is to test in an operationally representative environment that closely mimics the physical and electromagnetic landscape where the system will actually be deployed. Testing in a sterile, open-desert range may yield impressive technical specifications, but it creates a dangerous false sense of security, as such conditions do not reflect the complex reality of modern operational settings.

A truly representative environment is the ultimate litmus test for a C-sUAS. Urban canyons create line-of-sight blockages that challenge radar and camera tracking. Densely populated areas produce a cluttered electromagnetic spectrum saturated with Wi-Fi and cellular signals that can overwhelm RF sensors and generate high nuisance alarm rates. Atmospheric conditions like rain, fog, and thermal shimmer can significantly degrade the performance of EO/IR systems. Therefore, evaluating a system in an environment that accounts for this complex interplay of physical clutter, electromagnetic interference, and atmospheric effects for validating a C-sUAS's true operational effectiveness.

### 5.4 Mission Engineering (ME) and Modeling & Simulation (M&S) for Assessment

Mission Engineering (ME) is fundamental to developing effective C-sUAS characteristics because it places system performance within a broader operational context. Rather than evaluating a sensor or effector in isolation, ME analyzes the entire end-to-end kill chain from detection to defeat against realistic threat timelines and objectives. Modeling and Simulation (M&S) serves as the indispensable tool that complements this analysis. M&S allows for the cost-effective exploration of a vast trade space, enabling repeatable, high-fidelity testing of complex scenarios, such as coordinated swarm attacks or operations in dense electromagnetic environments, which are often too costly, dangerous, or impractical to replicate in live field trials. Through M&S, planners can conduct "what-if" analyses, quantifying how changes in a single performance parameter such as track accuracy or effector range that impact the overall mission outcome. Ultimately, the integration of ME and M&S allows the DoW to define, validate, and optimize C-sUAS system characteristics, ensuring that developed capabilities are directly tied to mission success before significant resources are committed to physical prototypes and testing.

To fully leverage ME and M&S-driven approaches, the data that fuels them must be both accessible and interpretable. Adopting common data formats for all test and evaluation activities is therefore paramount. When performance data from disparate sensor tests, live-fire events, and operational assessments is recorded in a standardized schema, it can be ingested into ME tools and simulation environments. This not only enables direct comparisons across different systems but creates a powerful digital feedback loop. Results can be used to continuously validate and refine the models, inform future live test events which ultimately increasing confidence in simulation-based findings and accelerating the development of more effective C-sUAS capabilities.

## 6. DATA COLLECTION & ANALYSIS

Rigorous data collection and analysis form the bedrock of any credible evaluation effort, transforming a simple pass/fail observation into a more comprehensive diagnostic understanding of system performance. It provides the objective evidence needed to identify critical kill chain bottlenecks, quantify performance under specific conditions, and validate system improvements over time. Ultimately, a disciplined data collection and analysis strategy moves the enterprise beyond anecdotal feedback, enabling truly data-driven decisions on system acquisition, doctrine development, and future investment.

## 7. REPORTING & DATA MANAGEMENT

To ensure the integrity, accuracy, and standardization of C-sUAS evaluation metrics, all evaluations must adhere to stringent reporting and data management protocols. It is imperative that organizations coordinate with designated test and evaluation activities capable of facilitating professional, high-fidelity data collection throughout the characterization process. Comprehensive data capture is critical for validating Key Performance Parameters (KPPs) and supporting robust

system analysis. To facilitate this requirement, JIATF 401 will actively assist organizations in coordinating the necessary data collection resources and infrastructure, ensuring that standardized methodologies are applied and that all resulting data sets meet baseline analytical standards for subsequent review, analysis, and authorized dissemination.

## Appendix A - Acronyms & Abbreviations

| | |
|---|---|
| AGL | Above Ground Level |
| API | Application Programming Interface |
| ATO | Authority to Operate |
| ATC | Authority to Connect |
| C2 | Command and Control |
| C-sUAS | Counter-small Unmanned Aircraft Systems |
| DE | Directed Energy |
| DoW | Department of War |
| DOT&E | Director, Operational Test & Evaluation |
| DP | Detection Point |
| EA | Electronic Attack |
| EO/IR | Electro-Optical/Infrared |
| ETA | Engagement Time Analysis |
| EW | Electronic Warfare |
| HEL | High-Energy Laser |
| HPM | High-Power Microwave |
| JCO | Joint C-sUAS Office |
| JIATF | Joint Interagency Task Force |
| KPP | Key Performance Parameter |
| KSA | Key System Attribute |
| LCD | Low Collateral Defeat |
| ME | Mission Engineering |

| | |
|---|---|
| M&S | Modeling & Simulation |
| MDCOA | Most Dangerous Course of Action |
| MLCOA | Most Likely Course of Action |
| MOE | Measure of Effectiveness |
| MOP | Measure of Performance |
| MTBSA | Mean Time Between System Abort |
| MTTR | Mean Time to Repair |
| NAR | Nuisance Alarm Rate |
| NASA-TLX | National Aeronautics and Space Administration - Task Load Index |
| OPSEC | Operational Security |
| OWA | One Way Attack |
| $P_k$ | Probability of Kill |
| RF | Radio Frequency |
| RMF | Risk Management Framework |
| SA | Situational Awareness |
| SAGAT | Situation Awareness Global Assessment Technique |
| sUAS | small Unmanned Aircraft Systems |
| SUT | System Under Test |
| TRMC | Test Resource Management Center |
| UAS | Unmanned Aircraft System |

# Appendix B - Government References

DoD Directive 5000.71 - Rapid Fulfillment of Combatant Commander Urgent Operational Needs and Other Quick Action Requirements.

DoD Instruction 5000.81 - Urgent Capability Acquisition

Executive Order 14305, Restoring American Airspace Sovereignty.

Executive Order 14307, Unleashing American Drone Dominance

National Science and Technology Council, The Standard Guidelines for Test and Evaluation of Counter-Unmanned Aircraft Systems Technologies.

The Department of Defense Unmanned Aircraft Categorization Review Report to Congress, November 2022.

U.S. Department of Defense Counter-Small Unmanned Aircraft Systems Strategy.


DEPARTMENT OF WAR
UNITED STATES OF AMERICA