Morphpublishing
Research
open access academic journal

Peer reviewed

Assessment of UAS Detect-and-Avoid Robustness Under Sensor Degradation, Erroneous Inputs, and Interference Scenarios

Moulaye Ould Cheikh[a], **Ely Oumar Kane**[b]

Abstract: Uncrewed aircraft systems require reliable detect-and-avoid functionality to support operations in airspace shared with crewed aircraft, other uncrewed vehicles, and complex environmental clutter. Contemporary detect-and-avoid systems integrate multiple sensing modalities, onboard navigation, and decision logic to ensure separation standards and mitigate collision risks across a wide range of encounter geometries. However, the operational envelope of these systems is shaped by non-ideal conditions, including gradual sensor degradation, transient faults, corrupt or inconsistent surveillance inputs, and intentional or unintentional interference in sensing and communications channels. Understanding how such conditions propagate through tracking, conflict detection, and maneuver selection is important for evaluating safety margins and for informing system design choices. This paper develops a structured assessment of detect-and-avoid robustness under these conditions, focusing on the interaction between sensing imperfections, estimator performance, conflict prediction uncertainty, and guidance decisions. The analysis considers heterogeneous sensor architectures, probabilistic models of degradation and faults, and interference mechanisms that perturb either measurement streams or the logical integrity of detect-and-avoid functions. Emphasis is placed on characterizing conditions under which detect-and-avoid performance degrades gradually, conditions under which it collapses abruptly, and the sensitivity of critical safety metrics to modeling assumptions. The resulting formulations and illustrative evaluations provide a basis for comparing detect-and-avoid configurations under stress, identifying parameter regimes of concern, and informing verification activities that incorporate adverse but plausible sensing and interference scenarios.

1. Introduction

Detect-and-avoid functionality is widely recognized as a key enabler for integrating uncrewed aircraft systems into shared airspace at scale [1]. A detect-and-avoid (DAA) system typically fuses measurements from cooperative surveillance channels, such as transponder-based or broadcast-based systems, with non-cooperative sensors including radar, electro-optical, or infrared payloads, and onboard navigation information. It then applies tracking algorithms, conflict detection logic, and resolution or guidance modules to maintain sufficient separation from other traffic and to avoid loss-of-separation or collision events. While baseline performance in nominal conditions is often studied

through Monte Carlo encounter models and standardized scenarios, operational deployments must withstand deviations from ideal sensing performance, transient anomalies, and intentional disruption. These effects can significantly alter the reliability of conflict detection and maneuver advisories even when nominal performance appears acceptable.

In practical environments, sensor degradation may arise from hardware aging, calibration drift, partial obstruction of fields-of-view, thermal or vibration-induced instability, or reduced signal-to-noise ratios in cluttered or low-visibility conditions [2]. Erroneous inputs can be introduced through software faults, navigation errors, incorrect ownship state estimates, inconsistent tracks between fused sources, or malformed cooperative messages. Interference mechanisms include unintentional radio frequency congestion, co-channel emissions, reflections, as well as deliberate jamming and spoofing targeting surveillance or navigation channels. Each of these classes of phenomena can perturb the internal belief state maintained by the DAA logic and can lead to either overly conservative alerts, which may burden operations, or under-responsive behavior, which directly impacts safety margins.

The robustness of DAA systems under this spectrum of off-nominal conditions is not fully characterized by standard accuracy or false-alarm metrics. Instead, robustness depends on how uncertainties propagate across a multi-layered architecture from sensing to estimation to conflict prediction to guidance and mode management. Subtle interactions may arise, such as bias in range-rate estimation amplifying conflict-time prediction error, or desynchronization between cooperative and non-cooperative tracks leading to inconsistent traffic representations [3]. Furthermore, mitigation strategies such as track quality flags, integrity monitors, and redundancy management introduce additional logic that can behave in complex ways under combined degradations.

This paper considers DAA robustness from a system-level modeling perspective, representing the detection and avoidance process as a closed-loop mapping from true environment states, through imperfect sensing and computation, to maneuver actions and induced future states. Within this representation, sensor degradation, erroneous inputs, and interference scenarios are introduced as parametric and stochastic perturbations to the sensing and decision elements. Robustness is then discussed in terms of induced distributions over safety-related metrics, rather than point performance in nominal conditions. The aim is not to prescribe specific implementations, but to provide a technical structure in which alternative architectures and parameterizations can be comparatively assessed.

The analysis is organized as follows [4]. A background description of DAA architectures is provided to establish notation and clarify the flow of information and decisions. Sensor degradation mechanisms are formulated in probabilistic and hybrid-system terms to capture both gradual and abrupt changes. Erroneous inputs are modeled as structured and unstructured faults entering the measurement and track domains. Interference and adversarial scenarios are framed as exogenous processes or strategic agents that perturb observation channels or logic. These elements are then combined into an integrated robustness assessment framework based on stochastic reachability and risk functionals. Finally, a set of simulation-style evaluations is described to illustrate how such a framework can be used to explore parameter sensitivities and scenario coverage [5]. The paper concludes with a concise summary of observations and implications for assessment practices.

2. Formal System Modeling and Robustness Objectives

The assessment of detect-and-avoid robustness under sensor degradation, erroneous inputs, and interference requires a formal representation of the coupled environment, sensing, estimation, and decision-making processes. This section introduces a modeling framework that captures this coupling with sufficient structure to support quantitative analysis, while remaining abstracted from any specific proprietary implementation. The focus is on the

Published in CURRENT ISSUE

Table 1. Key elements of the closed-loop DAA model

Component	Role	Representation	Domain
Environment state	True traffic and ownship	Joint kinematic and dynamic variables	Physical
Observations	Sensed information streams	Channel-specific mappings with noise	Measurement
Belief state	Internal situation estimate	Filtered tracks, covariances, flags	Information
DAA output	Alerts and commands	Discrete alerts, maneuver cues	Decision

Table 2. Representative sensor degradation mechanisms

Mechanism	Effect on measurements	Modeling construct	Timescale
Calibration drift	Slowly biased ranges or angles	Latent parameter evolution	Long
Alignment error	Misaligned bearings or elevation	Mode-dependent mapping	Long
Noise growth	Reduced precision, dispersion	Inflated covariance, heavy tails	Medium
Dropouts	Intermittent loss of returns	Time-varying detection probability	Short

Table 3. Classes of erroneous and inconsistent inputs

Source	Manifestation	Abstract model	Impact
Cooperative reports	Incorrect position or velocity	Mixture of nominal and faulty samples	Bias risk
Navigation faults	Ownship state error	Structured state offset in fusion	Geometry shift
Time-stamp issues	Misordered data	Desynchronization in tracks	Alert timing
Association errors	Track swaps or merges	Discrete mode in logic states	False or missed alerts

closed-loop mapping from true encounter dynamics to detect-and-avoid outputs under non-ideal sensing conditions and logic behaviors, providing a basis on which degradation and interference mechanisms can be parameterized and robustness objectives can be defined. By making explicit the dependencies between physical states, observation channels, internal belief states, and decision rules, the formulation allows robustness questions to be framed in terms of measurable or computable functionals, rather than exclusively in terms of qualitative scenarios.

Consider a discrete-time horizon indexed by k, with step size chosen to capture the fastest relevant DAA update, including both sensing and alerting cycles [6]. Let the joint true state of the ownship and all relevant intruders be denoted by x_k, including positions, velocities, and any additional variables that influence observability or maneuvering

Table 4. Interference and adversarial scenario categories

Type	Primary target	Representation	Scope
Unintentional RF congestion	Cooperative links	Increased loss, variable noise	Local or regional
Jamming	Surveillance or GNSS	Bounded interference process	Directed
Spoofing	State reporting	Structured false measurements	Strategic
Multipath and clutter	Non-cooperative sensing	Distorted returns, false tracks	Environment

Table 5. Main robustness modeling constructs

Construct	Purpose	Examples
Perturbation vector	Encodes degradation and faults	Bias levels, dropout rates, interference bounds
Belief update operator	Propagates internal state	Filters, integrity monitors, track logic
Closed-loop trajectory	Links inputs to outcomes	State, alerts, maneuvers over time

Table 6. Safety and robustness evaluation metrics

Metric	Interpretation	Use in assessment
Minimum separation	Closest approach distance	Detect erosion of safety margins
Loss-of-separation probability	Frequency of threshold violation	Quantify impact of perturbations
Alert lead time distribution	Time before predicted conflict	Assess timeliness under stress
Advisory stability	Consistency of outputs	Reveal oscillations and mode issues

behavior. The evolution of x_k is represented generically by a stochastic dynamical system driven by both ownship commands and exogenous uncertainties. A minimal but expressive form assumes that

$$x_{k+1} = f(x_k, u_k, d_k),$$

where u_k is the ownship command issued as a consequence of DAA and other guidance functions, and d_k captures exogenous influences such as intruder maneuvers or wind realizations. The function f may encode high-fidelity aircraft dynamics or simplified kinematic models; robustness conclusions depend on its fidelity only through how accurately relative motion and reachable sets are represented in critical regions of the state space. [7]

Sensing enters through a set of observation channels indexed by j, each associated with a sensing or data source

Published in CURRENT ISSUE

Table 7. Simulation-based assessment elements

Element	Role	Illustration
Encounter set	Defines traffic geometries	Head-on, crossing, overtaking cases
Degradation profiles	Realize sensor aging and faults	Drifts, step changes, outages
Interference patterns	Stress communication and sensing	Pulsed jamming, partial spoofing
Response models	Map alerts to maneuvers	Automated or supervised execution

such as cooperative surveillance, primary radar, electro-optical tracking, inertial navigation, barometric or satellite-based altitude, and crosslink data. For each channel, define an observation function and error term so that the nominal measurement at time k is written as

$$z_k^{(j)} = h^{(j)}(x_k) + v_k^{(j)},$$

with $v_k^{(j)}$ representing channel-specific noise and imperfections under nominal assumptions. The collection of measurements available to the DAA logic at time k is denoted $z_k = \{z_k^{(j)}\}$, recognizing that some channels may be asynchronous or intermittent. Sensor degradation, erroneous inputs, and interference will be modeled as perturbations of the $h^{(j)}$ mappings, of the distributions of $v_k^{(j)}$, and of the composition of z_k actually delivered to the system.

The DAA system maintains an internal belief state b_k summarizing its information about x_k and potentially about sensor health and logic modes. This belief state includes, in general, state estimates, covariances, track lists, integrity flags, and the history of alerts and maneuvers. One may view b_k as a sufficient statistic used by the DAA decision rule. The update of b_k is induced by an estimation and monitoring operator E that processes new measurements and previous beliefs [8]. In abstract form,

$$b_{k+1} = E(b_k, z_{k+1}^*, \psi_k),$$

where z_{k+1}^* denotes the actual inputs presented to the estimator, possibly corrupted or incomplete, and ψ_k denotes configuration or mode variables representing internal logic states such as filter modes, alert levels, or sensor selection statuses. The operator E subsumes prediction, filtering, data association, integrity checks, and track management. Robustness analysis hinges on how E amplifies or attenuates deviations arising from degraded or erroneous z_{k+1}^*, including heavy-tailed or biased perturbations that may not match tuning assumptions.

On top of b_k, the DAA alerting and guidance functions implement a decision mapping G that selects advisories or direct control actions based on the inferred traffic situation and system modes. Denote by y_k the conflict-relevant output of DAA at time k, such as no alert, traffic alert, resolution advisory, or a continuous maneuver command. Then

$$y_k = G(b_k, \psi_k),$$

and the ownship command u_k entering the state dynamics emerges from an interaction between y_k, the vehicle control system, and any human operator or supervisory autonomy [9]. For robustness assessment that focuses on the DAA contribution, it is convenient to model u_k as the output of a policy Π that maps y_k and possibly b_k or

other context into commands. This leads to

$$u_k = \Pi(y_k, \chi_k),$$

where χ_k captures external constraints or mission logic that may influence whether and how DAA advisories are executed. The composition of f, E, G, and Π defines a closed-loop system whose behavior under perturbed sensing and logic conditions is the subject of the robustness evaluation.

Non-ideal sensing effects are represented by introducing a perturbation structure on the nominal measurement model and processing chain [10]. Let ϕ be a vector of perturbation parameters and stochastic processes that encode degradation, faults, and interference. These elements include, for example, channel-specific detection probabilities, bias patterns, misalignment angles, noise scale factors, message dropout and corruption rates, timing offsets, and interference intensities. Rather than fixing ϕ, robustness assessment considers ϕ ranging over a set that represents plausible or design-basis deviations. For a given realization of ϕ, the actual measurement delivered to the DAA system is denoted $z_k^*(\phi)$, representing the combined effect of physical sensing, upstream processing, and any adversarial manipulation, so that

$$z_k^*(\phi) = H(x_k, \phi, \omega_k),$$

with H encompassing both nominal functions and perturbations, and ω_k denoting stochastic variability not captured directly in ϕ. This compact representation allows unified treatment of gradual sensor degradation, sporadic erroneous inputs, and structured interference patterns as different components or regimes of ϕ.

Within this framework, robustness concerns can be formulated in terms of how perturbations ϕ influence safety-relevant outcomes derived from the closed-loop trajectories [11]. Let S denote a functional of the trajectory $\{x_k, b_k, y_k, u_k\}$, such as the minimum separation distance during a given encounter, the indicator of a loss-of-separation event, the distribution of alert lead times, or an integrated cost that penalizes both missed conflicts and unnecessary maneuvers. Then S becomes a random quantity driven by initial encounter conditions, stochastic uncertainties, and perturbations ϕ. The mapping

$$\phi \mapsto \mathcal{L}(S \mid \phi)$$

describes how the law of S depends on perturbation realizations. Robustness assessment is then interpreted as the problem of characterizing this dependence over a region of ϕ that encodes the classes and intensities of degradation, erroneous inputs, and interference considered operationally relevant or of design interest.

A central object in this analysis is the set of trajectories that lead to safety-critical outcomes. Define a critical set $\mathcal{X}_{\text{crit}}$ in the joint state space encapsulating, for instance, pairwise separation below a defined threshold or violation of regulatory minima. One may then define an event $A(\phi)$ that the closed-loop trajectory enters $\mathcal{X}_{\text{crit}}$ within a specified horizon when subject to perturbations characterized by ϕ. Formally, for a given encoding of encounter distributions and stochastic inputs, the robustness measure of interest is often the probability [12]

$$r(\phi) = \mathbb{P}\big(A(\phi)\big),$$

together with related statistics such as conditional distributions of impact geometry or alerting behavior when $A(\phi)$ occurs. The function $r(\phi)$ links perturbation models to quantitative safety metrics and is the object to be bounded, approximated, or compared across DAA configurations.

For sensor degradation, components of ϕ may represent latent states that evolve over time, inducing temporal correlation in measurement distortions. The DAA estimator E may or may not explicitly track these latent states.

Published in CURRENT ISSUE

When they are not tracked, residual biases and mis-specified covariance structures can shift the effective belief state b_k away from the true state x_k in systematic ways [13]. In coarsened terms, one can think of the estimation error $e_k = \hat{x}_k - x_k$ as being driven not only by zero-mean noise but also by slowly varying or mode-dependent biases governed by ϕ. These biases may remain within the apparent uncertainty bounds of the estimator, leading to undetected erosion of conflict prediction accuracy. Robustness modeling explicitly accommodates this by including in ϕ processes that induce such structured deviations.

Erroneous inputs and intermittent faults are represented through perturbations in H that yield $z_k^*(\phi)$ inconsistent with nominal statistics, even if individual anomalies are bounded in magnitude. For example, ϕ may specify a fault rate and an error distribution for cooperative reports, as well as the logic by which faulty and nominal measurements are intermixed. The propagation of such errors through E depends on filter design, gating thresholds, and track management rules. In this way, the same fault model can induce different robustness characteristics in different DAA designs, and the framework captures these differences at the level of induced distributions of S rather than only at the measurement layer.

Interference and adversarial manipulation are naturally expressed within this parameterization by allowing parts of ϕ to be selected according to strategic or worst-case criteria rather than purely stochastic ones [14]. In a conservative analysis, one defines an admissible set Φ_{adm} corresponding to bounded interference capabilities or to constraints derived from spectrum regulations and physical limitations. Robustness questions are then expressed in terms of worst-case functionals, such as the supremum of $r(\phi)$ over $\phi \in \Phi_{\text{adm}}$, or in terms of identifying subsets of Φ_{adm} for which $r(\phi)$ exceeds specified thresholds. This formulation admits both game-theoretic interpretations, where an adversary selects perturbations to maximize risk, and engineering interpretations, where Φ_{adm} encodes expected ranges of interference intensities and spatial coverage.

Within this formal setting, robustness objectives can be organized without relying on enumerated scenario lists. One objective is stability of safety performance, in the sense that small or moderate perturbations in ϕ lead to limited changes in the distribution of S. Another objective is resilience to discrete mode changes, wherein the system transitions between sensing and logic configurations without producing abrupt increases in $r(\phi)$ or pathological alerting patterns. A further objective is discriminability, meaning that internal integrity and monitor functions should, with high probability, distinguish between nominal and significantly perturbed regimes in ϕ in time to adapt sensing weights or trigger mitigations that constrain $r(\phi)$.

The modeling approach also supports the construction of equivalent or reduced-order representations that are more tractable for analysis while still reflecting key sensitivities. For instance, complex sensor and fusion behaviors can, in specific contexts, be abstracted into stochastic error models on relative state estimates and integrity flags, characterized by conditional distributions parameterized by ϕ [15]. Similarly, detailed pilot or autonomy response models encoded in Π can be abstracted into distributions of achieved avoidance maneuvers as functions of alerts and geometries. The validity of such abstractions is scenario-dependent, but once accepted, they allow robustness metrics like $r(\phi)$ to be estimated or bounded using fewer dimensions, facilitating parameter sweeps and rare-event analyses.

Finally, this formal system representation clarifies how robustness assessments should be interpreted. Because $r(\phi)$ and related measures are defined relative to explicit models for encounters, perturbations, and decision mappings, conclusions drawn from any given set of simulations or analyses are conditional on those modeling choices. The objective is not to eliminate this conditionality, but to expose it. By viewing sensor degradation, erroneous inputs, and interference as structured components of ϕ that feed through a well-defined closed-loop mapping from states to safety outcomes, the assessment of detect-and-avoid robustness can focus on transparent

relationships between assumptions and results, enabling more consistent comparison of different architectures and parameterizations under a shared analytical language. [16]

3. Background on Detect-and-Avoid Architectures

A DAA system can be viewed as an information-processing and control stack that transforms physical encounter conditions into advisories or automated maneuvers. Let the joint state of ownship and surrounding traffic at discrete time index k be denoted by x_k, including positions, velocities, and other relevant variables in a suitable coordinate frame. The underlying dynamics are represented generically as

$$x_{k+1} = f(x_k, u_k) + w_k$$

where u_k is the ownship control input selected by guidance or by the remote or onboard pilot, and w_k represents exogenous disturbances such as wind or unmodeled maneuvers by other aircraft. The function f may encapsulate six-degree-of-freedom dynamics or reduced-order kinematics, depending on fidelity requirements.

Sensing subsystems provide measurements z_k influenced by the true state x_k and sensing imperfections [17]. For cooperative surveillance, measurements often approximate relative positions and velocities derived from broadcast states. For non-cooperative sensing such as radar or electro-optical systems, measurements are typically in range, bearing, and elevation or pixel-space coordinates. A generic measurement model can be written as

$$z_k = h(x_k) + v_k$$

with v_k capturing noise and distortions. In practical DAA implementations, multiple heterogeneous sensors produce asynchronously sampled measurements that are fused into a consolidated traffic picture [18]. Data association, track initiation and maintenance, and outlier rejection are critical components that shape the effective information delivered to conflict detection logic.

Conflict detection modules evaluate whether the inferred trajectories of ownship and intruders may violate separation criteria within a lookahead horizon. These criteria might be based on horizontal and vertical distance thresholds or other definitions of protected volumes. Conflict detection can rely on deterministic projections using current estimates or on stochastic predictions that account for process and estimation uncertainty. Resolution modules then compute advisories or trajectories u_k that reduce predicted conflict probabilities while respecting flight envelope, mission, and airspace constraints [19]. Some architectures implement advisories only, leaving final decisions to a remote pilot, while others implement partial or full automation in executing avoidance maneuvers.

Robustness emerges from the coupling of all these elements. Estimator performance depends on sensor health and interference. Conflict prediction quality depends on estimator outputs, ownship performance models, and assumptions about intruder behavior. Guidance decisions depend on conflict predictions and on supervisory logic that may inhibit or modify advisories in specific contexts. Traditional performance metrics, such as probability of detection or false-alarm rate for conflicts under nominal noise conditions, do not fully describe behavior when sensors degrade or inputs become inconsistent [20]. Instead, it becomes important to understand the sensitivity of conflict detection and guidance to variations in noise distributions, biases, missed detections, false tracks, and message manipulations that can arise in realistic environments.

4. Modeling Sensor Degradation in Detect-and-Avoid Pipelines

Sensor degradation is modeled here as a combination of parametric drift, stochastic dispersion, and mode transitions affecting the observation process. Let θ_k denote a vector of latent degradation parameters at time k. The

Published in CURRENT ISSUE

measurement model can be extended as

$$z_k = h(x_k, \theta_k) + v_k,$$

with v_k representing residual noise after accounting for θ_k [21]. The parameter θ_k may capture range bias, scale errors, misalignment angles, reduced detection probability, and other relevant factors. Gradual degradation can be represented as a stochastic process such as

$$\theta_{k+1} = \theta_k + \eta_k,$$

where η_k is a small disturbance, potentially with covariance that reflects environmental and mechanical stress. Abrupt faults can be represented by jump processes or discrete modes. A hybrid formulation introduces a mode variable m_k that evolves as a Markov chain and switches the mapping between x_k and z_k.

In such a hybrid model, each mode m_k corresponds to a sensor condition, such as nominal, partially degraded, saturated, or failed [22]. For a given mode, the effective measurement function and noise statistics are determined by $(h^{(m)}, R^{(m)})$, with $R^{(m)}$ denoting the covariance of v_k under mode m. The transition probabilities between modes define likely sequences of degradation events, including rare catastrophic failures and more probable mild degradations. The DAA estimator may or may not explicitly infer m_k; many practical implementations operate with filters tuned to nominal or slightly conservative assumptions, which can lead to mis-calibrated uncertainty under significant degradation.

From a robustness assessment perspective, one is interested in how deviations in θ_k and m_k influence the belief over relative states used for conflict detection. If $\hat{x}_k$ denotes the filter estimate and P_k its error covariance, then degradation typically increases P_k, but may also introduce structured bias. For instance, a small bias in bearing measurements can systematically distort lateral position estimates over time. Even if P_k appears acceptable according to internal consistency checks, biased estimates can shift predicted closest point of approach and alter whether a potential conflict is detected. Modeling must therefore consider both dispersion and bias, not only variance inflation. [23]

Advanced formulations can represent the estimation problem under degradation as a partially observable system in which both x_k and θ_k (and possibly m_k) are unknown. Estimators may attempt joint state and parameter estimation using Bayesian or adaptive techniques, but DAA certification constraints often limit algorithmic complexity. For robustness analysis, one may instead specify families of admissible degradation trajectories and analyze worst-case or distributionally robust behavior. For example, one can constrain θ_k to lie in a compact set capturing plausible miscalibrations and then study whether the DAA logic maintains conflict detection performance over that set. Alternatively, one can treat θ_k as a random process with specified statistics and evaluate the resulting probability of missed or late conflict detection.

By structuring degradation in this way, assessment can move beyond scalar performance margins to examine which combinations of degradation modes, encounter geometries, and traffic behaviors most significantly influence safety metrics [24]. This enables a more systematic exploration of robustness than ad hoc stress tests that adjust sensor parameters independently or uniformly.

5. Robustness to Erroneous and Inconsistent Inputs

Erroneous inputs to DAA systems may arise from misreported cooperative surveillance data, navigation faults, corrupted time stamps, misassociated tracks, or software errors in upstream processing. Unlike gradual degradation, such errors can be intermittent, structured, and partially correlated with operational conditions. To model their influence, consider the measurement sequence as a mixture of nominal and faulty components. Let z_k^* denote the

value provided to the DAA estimator at time k [25]. A simple probabilistic abstraction can be

$$z_k^* = \begin{cases} z_k, & \text{with probability } 1-\epsilon_k, \\ \tilde{z}_k, & \text{with probability } \epsilon_k, \end{cases}$$

where z_k follows the nominal sensing model and $\tilde{z}_k$ represents an erroneous input that may depend on x_k, past values, or adversarial choices. The parameter ϵ_k may vary in time and across channels. This abstraction supports analysis of both random and scenario-driven error patterns.

When multiple sensors or feeds are fused, consistency checks and cross-validation can mitigate isolated erroneous inputs, but may be less effective when faults align across channels or when consistency metrics are themselves affected by timing or synchronization issues. Let $\hat{x}_k$ be obtained from a filter that assumes Gaussian noise and no gross errors. Under the mixture model, the effective error distribution becomes heavy-tailed [26]. Robust estimation theory indicates that such mismatches can lead to significant degradation in estimation accuracy and integrity. A robust DAA assessment must therefore characterize the distribution of estimation errors under mixtures, not only under Gaussian assumptions.

One representation of robustness is through influence functions that describe how sensitive $\hat{x}_k$ is to perturbations in individual measurements. Filters with bounded influence or mechanisms that down-weight outliers reduce sensitivity to isolated erroneous inputs. However, in DAA, delays or suppression of valid but unusual measurements can also affect timely conflict detection. This introduces a trade-off between false alarm rejection and sensitivity to genuine, low-probability conflict geometries. A comprehensive assessment therefore examines parameter regimes for which the chosen robustness mechanisms maintain an acceptable balance, when exposed to realistic encounter and fault statistics. [27]

A more structural modeling approach treats erroneous inputs as bounded or stochastic disturbances entering an augmented dynamical system that includes estimator states and conflict logic states. Define an augmented state ξ_k that concatenates $\hat{x}_k$, internal filter variables, and logic indicators such as track quality and alert states. The augmented evolution can be expressed as

$$\xi_{k+1} = F(\xi_k, z_k^*),$$

with F representing the combined estimation and logic update. Robustness questions can then be framed in terms of reachable sets of ξ_k under specified bounds or distributions of $z_k^* - z_k$. For example, one can ask whether there exist error realizations within specified bounds that drive the system into regions corresponding to missed alerts, spurious alerts, or oscillatory advisories.

This formulation supports both worst-case (adversarial disturbance) and probabilistic (stochastic disturbance) analyses [28]. In the former, one examines whether any pattern of erroneous inputs consistent with assumed bounds can cause unacceptable behavior. In the latter, one characterizes probabilities of undesirable outcomes given distributions over erroneous input events. Both viewpoints are relevant for DAA robustness assessment: worst-case analyses address safety margins with conservative modeling, while probabilistic analyses align with risk-informed decision making when complete elimination of errors is infeasible.

6. Interference and Adversarial Scenarios

Interference scenarios extend beyond random errors by introducing structured disruptions of sensing and communication mechanisms. These include unintentional electromagnetic interference, spectrum congestion, multipath-induced distortions, as well as deliberate jamming and spoofing attacks targeting surveillance links,

Published in CURRENT ISSUE

navigation signals, or intra-system communications. Such phenomena can simultaneously affect multiple aircraft and systems, introducing correlated uncertainties difficult to address through simple redundancy. [29]

At the measurement level, interference can be represented as an additive or multiplicative disturbance injected into the observation process. For a cooperative channel, one may write

$$z_k^c = h^c(x_k) + i_k,$$

where i_k summarizes the net effect of interference. In jamming scenarios, the effective signal-to-interference ratio degrades, which can be abstracted by increased variance or dropout probability of z_k^c. In spoofing scenarios, i_k may be structured to shift apparent positions or velocities in specific directions. For non-cooperative sensors, interference may produce false returns or obscure genuine targets, altering detection probabilities and clutter characteristics.

When interference is strategic, it is useful to model the interaction between the DAA system and the interfering agent as a dynamic game [30]. Let the DAA system choose estimation and decision policies π, and the adversary choose interference actions a_k. The observation model and subsequent DAA behavior become functions of a_k, and one can define performance or safety loss functions capturing, for instance, probabilities of undetected conflicts. A conservative robustness analysis may consider worst-case interference over an admissible set of a_k, leading to min-max formulations. For example, one can analyze whether for all interference sequences with bounded magnitude and rate, the DAA maintains detection of conflicts that would be detected without interference.

An alternative, complementary viewpoint considers interference processes as stochastic with specified temporal and spatial characteristics [31]. Here, interference events are modeled through random fields or point processes in time-frequency space, influencing different channels with given probabilities. The DAA architecture can incorporate integrity monitoring, such as cross-checks between sensors or sanity checks on kinematic feasibility of reported tracks. Robustness assessment then examines how these monitors respond to interference realizations and whether they effectively trigger mode changes, reweight sensors, or inhibit reliance on suspect inputs in time to preserve safety margins.

A particular concern arises when interference partially degrades situation awareness without being detected by integrity monitors. In such latent failure modes, conflict detection continues based on corrupted or incomplete data, and standard fault flags do not indicate abnormality. Robustness analysis in this regime focuses on identifying conditions under which interference patterns can evade existing monitors while inducing significant changes in conflict prediction [32]. This motivates systematic exploration of parameterized interference models, including spatially localized jamming, simultaneous partial outages in cooperative and non-cooperative channels, and coordinated spoofing that preserves superficial consistency between channels while distorting absolute geometry.

7. Integrated Robustness Assessment Framework

To systematically evaluate DAA robustness under sensor degradation, erroneous inputs, and interference, it is useful to frame the problem as a stochastic reachability and risk assessment task. Consider the closed-loop system defined by environment dynamics, sensing, DAA logic, and resulting ownship actions. Let S denote a safety-relevant quantity, such as minimum separation distance achieved in an encounter, or an indicator of loss-of-separation. For a given configuration of degradation and interference parameters, described collectively by ϕ, and for a given encounter scenario distribution, one can regard S as a random variable $S(\phi)$ induced by all stochastic elements [33].

A basic robustness measure is the probability that S violates a safety threshold [34]. Denoting by A the event of violation, one may evaluate

$$r(\phi) = P(A \mid \phi).$$

This function captures how safety performance changes with specific degradation or interference conditions. For assessment, one often considers sets of parameters Φ representing plausible or design-basis conditions and seeks either upper bounds on $r(\phi)$ over $\phi \in \Phi$ or characterizations of parameter regions where $r(\phi)$ remains below acceptable levels.

A refined perspective describes robustness not only through scalar probabilities but also through risk functionals that weight severity. For example, one may define an expectation of a loss function $L(S)$ that increases with severity of separation violations [35]. Alternatively, one may impose chance constraints, requiring that the probability of crossing critical thresholds remains below specified levels under all ϕ in a set. These formulations align with both deterministic safety margins and probabilistic safety targets and provide a bridge between modeling and assurance arguments.

Computing such measures directly may be challenging due to dimensionality and nonlinearity of the closed-loop system. However, the structure of the DAA pipeline and the relatively low dimension of key relative states enable focused techniques. Scenario-based methods approximate $r(\phi)$ via ensembles of encounters and randomized realizations of degradation and interference processes. Importance sampling and rare-event simulation methods can be used to estimate low probabilities associated with severe outcomes [36]. Analytical bounds can be constructed using concentration inequalities and Lipschitz-type properties of the mapping from uncertainties to S for certain components, although care is required due to discrete logic and mode switching.

The integrated framework also facilitates comparison of architecture variants. For instance, one may analyze configurations with different sensor fusion algorithms, integrity monitors, or guidance logics, each represented by a different mapping from observations to actions but evaluated under the same ensemble of perturbations. Relative robustness is then expressed by differences in $r(\phi)$ or in risk functionals across configurations over the parameter sets of interest. Such comparative analysis avoids overemphasis on nominal performance and focuses on stability of safety metrics under challenging but relevant conditions.

Finally, the framework supports sensitivity analysis [37]. By differentiating or perturbing $r(\phi)$ with respect to components of ϕ, one can identify which forms of degradation or interference have the largest influence on robustness. This information can guide design priorities, such as strengthening specific integrity checks, adding redundancy in selected channels, or adjusting conflict detection thresholds for resilience to particular uncertainties.

8. Simulation-Based Evaluation and Discussion

While the integrated framework is defined abstractly, practical assessment relies on constructing simulation campaigns that instantiate representative encounter models, sensor behaviors, and interference patterns. A typical evaluation process samples initial conditions for ownship and intruder trajectories, including relative positions, velocities, and maneuver intentions, from distributions reflecting anticipated operations. The environment model includes wind, turbulence, and other disturbances [38]. The DAA logic is implemented with fidelity consistent with available specifications, including estimator design, conflict detection algorithms, maneuver generation, and mode management policies.

Sensor degradation is injected according to the models described earlier, with parameters drawn from specified distributions or selected as fixed stress-test values. For instance, one may include slowly drifting alignment errors,

Published in CURRENT ISSUE

periods of reduced detection probability, and abrupt but recoverable failures. Erroneous inputs are introduced as intermittent corrupted messages, misassociated measurements, or inconsistent timestamps, with rates and magnitudes aligned with engineering judgment or collected data. Interference scenarios are modeled as time-varying processes affecting specific channels, including partial outages, noise bursts, and structured spoofing of some cooperative reports.

For each realization of these elements, the closed-loop simulation produces time histories of estimated states, conflict alerts, avoidance maneuvers, and actual separations [39]. Derived metrics such as minimum separation, alert lead time, and maneuver aggressiveness are recorded. Repeating this process generates empirical distributions from which probabilities of safety threshold violations and other robustness measures can be estimated. To focus on regions of interest, sampling can be biased toward encounter geometries that are more sensitive to uncertainties, such as head-on or crossing trajectories with small time-to-go, or toward degradation patterns that are likely to stress specific aspects of the DAA logic.

Interpretation of such results benefits from disaggregating contributions from different perturbation mechanisms. For example, one may examine how much of the change in violation probability between nominal and stressed conditions is attributable to increased estimator dispersion versus systematic bias, or how interference in cooperative channels interacts with the presence or absence of non-cooperative sensors. Identifying joint effects is particularly important because some robustness features, such as track quality flags or cross-sensor consistency checks, are designed under assumptions that may not hold when multiple degradation mechanisms occur simultaneously. [40]

An additional aspect concerns the temporal characteristics of robustness. Certain DAA architectures may tolerate brief sensor outages but become vulnerable under longer persistent degradations. Others may be sensitive to rapid alternation between nominal and degraded modes, which can complicate track management and cause spurious alert oscillations. Assessing robustness under realistic temporal patterns of faults and interference thus requires constructing sequences that capture both duration and timing relative to critical phases in encounters. This temporal dimension is essential for understanding whether integrity monitors and fallback strategies react sufficiently early and consistently.

Overall, simulation-based evaluation within the described framework provides a means to explore complex dependencies that are difficult to capture analytically [41]. It can highlight parameter regimes and scenario classes where robustness is limited, even when nominal performance indicators appear satisfactory. While numerical values obtained from specific simulations are sensitive to modeling assumptions, the structure of the analysis encourages explicit documentation of those assumptions and facilitates comparison of alternative DAA designs under consistent stress scenarios.

9. Conclusion

This paper has examined detect-and-avoid robustness for uncrewed aircraft systems under conditions of sensor degradation, erroneous inputs, and interference. By representing the DAA pipeline as a closed-loop system from physical states through sensing and estimation to conflict detection and guidance, it becomes possible to embed non-ideal sensing phenomena as structured perturbations and to study their impact on safety-relevant metrics. Sensor degradation was modeled using parametric drift and mode-switching mechanisms that influence both dispersion and bias in state estimation, highlighting the importance of considering hybrid failure modes rather than relying solely on variance inflation. Erroneous and inconsistent inputs were formulated through mixture and disturbance models, connecting robustness to properties of estimators, integrity monitors, and decision logic operating under heavy-tailed and correlated uncertainties. [42]

Interference and adversarial scenarios were incorporated as exogenous or strategic perturbations of observation channels, emphasizing cases where partial or latent failures can challenge existing monitoring strategies. An integrated robustness assessment framework based on stochastic reachability and risk measures was outlined to relate these modeling constructs to probabilities and severities of safety threshold violations across parameter sets of interest. Simulation-based evaluation within this framework was discussed as a practical means for exploring how encounter geometries, degradation processes, and interference patterns jointly influence detect-and-avoid performance.

The formulations presented here support a structured analysis of DAA behavior under a range of off-nominal conditions without prescribing specific implementation details. They underscore the relevance of characterizing both gradual and abrupt deviations from nominal sensing assumptions and of analyzing their propagation through estimation, conflict prediction, and guidance layers. Such assessments can inform system design choices, tuning decisions, and verification activities aimed at understanding where robustness is strong and where it is limited under realistic operational and interference conditions, without overstating the conclusions drawn from any single model or scenario set. [43]

References

[1] N. Chauhan, R. Kumar, S. Mukherjee, A. Hazra, and K. Giri, "Ultra-resolution unmanned aerial vehicle (uav) and digital surface model (dsm) data-based automatic extraction of urban features using object-based image analysis approach in gurugram, haryana," *Applied Geomatics*, vol. 14, no. 4, pp. 751–764, 10 2022.

[2] J. Li-Chee-Ming and C. Armenakis, "A feasibility study on using visp's 3d model-based tracker for uav pose estimation in outdoor environments," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. XL-1/W4, pp. 329–335, 8 2015.

[3] H. Hussein, H. A. Elsayed, and S. M. A. El-Kader, "Intensive benchmarking of d2d communication over 5g cellular networks: prototype, integrated features, challenges, and main applications," *Wireless Networks*, vol. 26, no. 5, pp. 3183–3202, 9 2019.

[4] null Robert Spousta and null Steve Chan, "Hold the drones: Fostering the development of big data paradigms through regulatory frameworks," *Journal of Communication and Computer*, vol. 12, no. 3, 3 2015.

[5] L. Pádua, P. Marques, J. Hruška, T. Adão, E. Peres, R. Morais, and J. J. Sousa, "Multi-temporal vineyard monitoring through uav-based rgb imagery," *Remote Sensing*, vol. 10, no. 12, pp. 1907–, 11 2018.

[6] J. Flórez, J. Ortega, A. Betancourt, A. García, M. Bedoya, and J. S. Botero, "A review of algorithms, methods, and techniques for detecting uavs and uas using audio, radiofrequency, and video applications," *TecnoLógicas*, vol. 23, no. 48, pp. 269–285, 5 2020.

[7] J. J. Rasmussen, J. Nielsen, J. C. Streibig, J. E. Jensen, K. S. Pedersen, and S. I. Olsen, "Pre-harvest weed mapping of cirsium arvense in wheat and barley with off-the-shelf uavs," *Precision Agriculture*, vol. 20, no. 5, pp. 983–999, 12 2018.

[8] I. Q. García, N. V. Vélez, P. A. Martínez, J. V. Ull, and B. F. Gallo, "A quickly deployed and uas-based logistics network for delivery of critical medical goods during healthcare system stress periods: A real use case in valencia (spain)," *Drones*, vol. 5, no. 1, pp. 13–, 2 2021.

[9] M. M. Nowak, K. Dziób, and P. Bogawski, "Unmanned aerial vehicles (uavs) in environmental biology: a review." *European Journal of Ecology*, vol. 4, no. 2, pp. 56–74, 1 2019.

[10] T. Schrader, J. Bredemeyer, M. Mihalachi, J. Rohde, and T. Kleine-Ostmann, "Concept and design of a uas-based platform for measurements of rf signal-in-space," *Advances in Radio Science*, vol. 14, pp. 1–9, 9 2016.

[11] L.-P. Chi, C.-H. Fu, J.-P. Chyng, Z.-Y. Zhuang, and J.-H. Huang, "A post-training study on the budgeting criteria set and priority for male uas design," *Sustainability*, vol. 11, no. 6, pp. 1798–, 3 2019.

[12] D. Connor, K. Wood, P. G. Martin, S. Goren, D. A. Megson-Smith, Y. Verbelen, I. Chyzhevskyi, S. Kirieiev, N. Smith, T. Richardson, and T. B. Scott, "Corrigendum: Radiological mapping of post-disaster nuclear environments using fixed-wing unmanned aerial systems: A study from chornobyl." *Frontiers in robotics and AI*, vol. 6, pp. 149–, 1 2020.

[13] P. Boucher, "Domesticating the drone: The demilitarisation of unmanned aircraft for civil markets." *Science and engineering ethics*, vol. 21, no. 6, pp. 1393–1412, 11 2014.

[14] S. Zhang, C. D. Lippitt, S. M. Bogus, and P. Neville, "Characterizing pavement surface distress conditions with hyper-spatial resolution natural color aerial photography," *Remote Sensing*, vol. 8, no. 5, pp. 392–, 5 2016.

[15] A. L. Wilber, J. M. P. Czarnecki, and J. D. McCurdy, "An argis pro workflow to extract vegetation indices from aerial imagery of small plot turfgrass research," *Crop Science*, vol. 62, no. 1, pp. 503–511, 12 2021.

[16] Y. Zhang, J. Li, W. Fu, J. Ma, and G. Wang, "A lightweight yolov7 insulator defect detection algorithm based on dsc-se." *PloS one*, vol. 18, no. 12, pp. e0 289 162–e0 289 162, 12 2023.

[17] O. Cetin and G. Yilmaz, "Real-time autonomous uav formation flight with collision and obstacle avoidance in unknown environment," *Journal of Intelligent & Robotic Systems*, vol. 84, no. 1, pp. 415–433, 1 2016.

[18] "Arctic change 2020 abstracts (continued)," *Arctic Science*, vol. 7, no. 1, pp. 240–368, 3 2021.

[19] A. Canolla, M. B. Jamoom, and B. Pervan, "Interactive multiple model sensor analysis for unmanned aircraft systems (uas) detect and avoid (daa)," in *2018 IEEE/ION Position, Location and Navigation Symposium (PLANS)*. IEEE, 2018, pp. 757–766.

[20] R. C. Cardoso, G. Kourtis, L. A. Dennis, C. Dixon, M. Farrell, M. Fisher, and M. Webster, "A review of verification and validation for space autonomous systems," *Current Robotics Reports*, vol. 2, no. 3, pp. 273–283, 6 2021.

[21] C. T. White, A. Petrasova, W. Reckling, and H. Mitasova, "Automated land cover change detection through rapid uas updates of digital surface models," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. XLII-3/W11, pp. 155–159, 2 2020.

[22] A. C. Canolla, M. B. Jamoom, and B. Pervan, "Unmanned aircraft systems detect and avoid sensor hybrid estimation error analysis," in *17th AIAA Aviation Technology, Integration, and Operations Conference*, 2017, p. 4384.

[23] M. Muthusamy, M. R. Casado, G. Salmoral, T. Irvine, and P. Leinster, "A remote sensing based integrated approach to quantify the impact of fluvial and pluvial flooding in an urban catchment," *Remote Sensing*, vol. 11, no. 5, pp. 577–, 3 2019.

[24] C. Hoffmann, C. Weise, T. Koch, and K. Pauly, "From uas data acquisition to actionable information – how an end-to-end solution helps oil palm plantation operators to perform a more sustainable plantation management," *ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. XLI-B1, pp. 1113–1120, 6 2016.

[25] M. Herrero-Huerta, P. Rodríguez-Gonzálvez, and K. M. Rainey, "Yield prediction by machine learning from uas-based mulit-sensor data fusion in soybean," *Plant methods*, vol. 16, no. 1, pp. 1–16, 6 2020.

[26] E. Denney and G. Pai, "Tool support for assurance case development," *Automated Software Engineering*, vol. 25, no. 3, pp. 435–499, 12 2017.

[27] W. Zhang, C. Witharana, A. K. Liljedahl, and M. Kanevskiy, "Deep convolutional neural networks for automated characterization of arctic ice-wedge polygons in very high spatial resolution aerial imagery," *Remote Sensing*, vol. 10, no. 9, pp. 1487–, 9 2018.

[28] K. Neace, R. A. Roncace, and P. Fomin, "Goal model analysis of autonomy requirements for unmanned aircraft systems," *Requirements Engineering*, vol. 23, no. 4, pp. 509–555, 7 2017.

[29] J. Gallik and L. Bolešová, "suas and their application in observing geomorphological processes," *Solid Earth*, vol. 7, no. 4, pp. 1033–1042, 7 2016.

[30] L. Pellone, S. Ameduri, N. Favaloro, and A. Concilio, "Sma-based system for environmental sensors released from an unmanned aerial vehicle," *Aerospace*, vol. 4, no. 1, pp. 4–, 1 2017.

[31] I. González-Hernández, S. Salazar, R. Lozano, and O. Ramírez-Ayala, "Real-time improvement of a trajectory-tracking control based on super-twisting algorithm for a quadrotor aircraft," *Drones*, vol. 6, no. 2, pp. 36–36, 1 2022.

[32] C. Cromwell, J. Giampaolo, J. P. Hupy, Z. Miller, and A. Chandrasekaran, "A systematic review of best practices for uas data collection in forestry-related applications," *Forests*, vol. 12, no. 7, pp. 957–, 7 2021.

[33] A. C. Canolla, M. B. Jamoom, and B. Pervan, "Interactive multiple model hazard states prediction for unmanned aircraft systems (uas) detect and avoid (daa)," in *2018 AIAA Information Systems-AIAA Infotech@ Aerospace*, 2018, p. 2011.

[34] J. Bae, J. Lee, A. Jang, Y. K. Ju, and M. J. Park, "Smart sky eye system for preliminary structural safety assessment of buildings using unmanned aerial vehicles." *Sensors (Basel, Switzerland)*, vol. 22, no. 7, pp. 2762–2762, 4 2022.

[35] K.-Y. Li, N. Burnside, R. S. de Lima, M. V. Peciña, K. Sepp, V. H. C. Pinheiro, B. R. C. A. de Lima, M.-D. Yang, A. Vain, and K. Sepp, "An automated machine learning framework in unmanned aircraft systems: New insights into agricultural management practices recognition approaches," *Remote Sensing*, vol. 13, no. 16, pp. 3190–, 8 2021.

[36] J. W. Crampton, "Assemblage of the vertical: commercial drones and algorithmic life," *Geographica Helvetica*, vol. 71, no. 2, pp. 137–146, 6 2016.

[37] J. Reuder, M. Ablinger, H. Ágústsson, P. Brisset, S. Brynjólfsson, M. Garhammer, T. Jóhannesson, M. O. Jonassen, R. Kuhnel, S. Lämmlein, T. E. de Lange, C. Lindenberg, S. Malardel, S. Mayer, M. Müller, H. Ólafsson, Ólafur Rögnvaldsson, W. Schäper, T. Spengler, G. Zängl, and J. Egger, "Flohof 2007: an overview of the mesoscale meteorological field campaign at hofsjökull, central iceland," *Meteorology and Atmospheric Physics*, vol. 116, no. 1, pp. 1–13, 1 2011.

[38] G. Lu, "Concentrated stream data processing for vegetation coverage monitoring and recommendation against rock desertification," *Processes*, vol. 10, no. 12, pp. 2628–2628, 12 2022.

[39] A. K. G and K. Santhi, "Dynamic routing for flying ad hoc networks," *IJARCCE*, vol. 6, no. 4, pp. 161–170, 4 2017.

Published in CURRENT ISSUE

[40] J. Kersten and V. Rodehorst, "Enhancement strategies for frame-to-frame uas stereo visual odometry," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, vol. XLI-B3, pp. 511–518, 6 2016.

[41] K. Schweiger and L. Preis, "Urban air mobility: Systematic review of scientific publications and regulations for vertiport design and operations," *Drones*, vol. 6, no. 7, pp. 179–179, 7 2022.

[42] P. Marcoň, J. Janoušek, J. Pokorný, J. Novotný, E. V. Hutová, A. Širůčková, M. Cap, J. Lázničková, R. Kadlec, P. Raichl, P. Dohnal, M. Steinbauer, and E. Gescheidtova, "A system using artificial intelligence to detect and scare bird flocks in the protection of ripening fruit." *Sensors (Basel, Switzerland)*, vol. 21, no. 12, pp. 4244–, 6 2021.

[43] H. Nawaz, H. M. Ali, and A. A. Laghari, "Uav communication networks issues: A review," *Archives of Computational Methods in Engineering*, vol. 28, no. 3, pp. 1349–1369, 3 2020.