Designation: F3442/F3442M − 20

Standard Specification for Detect and Avoid System Performance Requirements[1]

This standard is issued under the fixed designation F3442/F3442M; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This specification applies to unmanned aircraft (UA) with a maximum dimension (for example, wingspan, disc diameter) ≤25 ft, operating at airspeeds below 100 kts, and of any configuration or category. It is meant to be applied in a "lower risk" (low- and medium-risk airspace as described by Joint Authorities for Rulemaking on Unmanned Systems (JARUS)) airspace environment with assumed infrequent encounters with manned aircraft; this is typically in classes G and E airspace (below about 1200 ft above ground level (AGL)), Class B, C, D (below about 400 to 500 ft AGL), below obstacle clearance surface (FAA Order 8260.3, as amended), or within low altitude authorization and notification capability (LAANC) designated areas below the altitude specified in the facility map.

1.1.1 Traffic encountered is expected to be mixed cooperative and non-cooperative traffic, instrument flight rules (IFR) and visual flight rules (VFR), and to mostly include low-altitude aircraft—including rotorcraft, small general aviation, crop dusters, ultralights, and light sport aircraft, but not transport category aircraft.

1.1.2 This includes, but is not limited to, airspace where all aircraft are required[2] to be cooperative (for example, within the Mode C veil in the U.S.).

1.2 Ultimate determination of applicability will be governed by the appropriate civil aviation authority (CAA).

1.3 This specification assumes no air traffic control (ATC) separation services are provided to the UA.

1.4 While some architectures may have limitations due to external conditions, this specification applies to daytime and nighttime, as well as visual meteorological conditions (VMC) and instrument meteorological conditions (IMC).

1.5 This specification is applicable to the avoidance of manned aircraft by unmanned aircraft systems (UAS), not UA-to-UA or terrain/obstacle/airspace avoidance (both to be addressed in future efforts). Likewise, birds or natural hazard (for example, weather, clouds) avoidance requirements are not addressed.

1.6 This specification does not define a specific detect and avoid (DAA) architecture[3] and is architecture agnostic. It will, however, define specific safety performance thresholds for a DAA system to meet to ensure safe operation.

1.7 This specification addresses the definitions and methods for demonstrating compliance to this specification, and the many considerations (for example, detection range, required timeline to meet well-clear, and near mid-air collision (NMAC) safety targets) affecting DAA system integration.

1.8 The specification highlights how different aspects of the system are designed and interrelated, and how they affect the greater UAS system to enable a developer to make informed decisions within the context of their specific UAS application(s).

1.9 It is expected this specification will be used by diverse contributors or actors including, but not limited to:

1.9.1 DAA system designers and integrators,

1.9.2 Sensor suppliers,

1.9.3 UA developers,

1.9.4 Ground control station (GCS) designers,

1.9.5 UAS service suppliers, and

1.9.6 Flight control designers.

1.10 Except for DAA system integrators for whom all the "shalls" in this specification apply, not all aspects of this specification are universally relevant. Nonetheless, familiarity with the entire specification will inform all actors/contributors of how their contributions affect the overall DAA capability and is strongly recommended.

1.11 The values stated in either SI units or inch-pound units are to be regarded separately as standard. The values stated in each system are not necessarily exact equivalents; therefore, to ensure conformance with the standard, each system shall be used independently of the other, and values from the two systems shall not be combined.

1.12 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the*

[1] This specification is under the jurisdiction of ASTM Committee F38 on Unmanned Aircraft Systems and is the direct responsibility of Subcommittee F38.01 on Airworthiness.

Current edition approved May 1, 2020. Published July 2020. DOI: 10.1520/F3442_F3442-20.

[2] Refer to 14 CFR § 91.215 and 14 CFR § 91.225 in the United States, or to the international equivalent for exceptions.

[3] ACAS sXu is intended to serve as a reference architecture for this specification.

responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.

1.13 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

2. Referenced Documents

2.1 When external standards, documents, or studies are referenced by this specification, the latest revision applies unless otherwise stated herein. Standards referenced should not be considered normative unless explicitly stated.

2.2 *ASTM Standards:*[4]

F3060 Terminology for Aircraft

ASTM TR1-EB Autonomy Design and Operations in Aviation: Terminology and Requirements Framework

2.3 *Other Documents:*

14 CFR § 1.1 General definitions[5]

14 CFR § 91.111 Operating near other aircraft[5]

14 CFR § 91.113 Right-of-way rules: Except water operations[5]

14 CFR § 91.215 ATC transponder and altitude reporting equipment and use[5]

14 CFR § 91.225 Automatic Dependent Surveillance-Broadcast (ADS-B) Out equipment and use[5]

14 CFR § 107.37 Operation near aircraft; right-of-way rules[5]

FAA AC (Advisory Circular) 25.1322-1 Flightcrew Alerting (Dec. 13, 2010)[6]

FAA Order 8260.3 United States Standard for Terminal Instrument Procedures (TERPS)[6]

JARUS Specific Operations Risk Assessment (SORA) (package) V2.0, 30 January, 2019[7]

Public Law 112-95 § 331 FAA Modernization and Reform Act of 2012—Definitions[5]

RTCA DO-365A Minimum Operational Performance Standards (MOPS) for Detect and Avoid (DAA) Systems, published May 2017[8]

3. Terminology

3.1 See Terminology F3060 and ASTM TR1-EB for definitions and abbreviations.

3.2 *Use of Shall, Should, and May*—The use of *shall* indicates a requirement, *should* indicates a recommendation, and *may* is used to indicate that something is permitted.

3.3 *Definitions:*

3.3.1 *alert function, A1F, n*—the function within the DAA system tasked with notifying the avoid function (whether human or automated system, or both) of the presence of an intruder.

3.3.2 *avoid function, A2F, n*—the function within the DAA system tasked with providing the flight guidance necessary to maneuver away from the potential hazard posed by detected intruder(s). Avoidance may be executed automatically by a flight controller or manually by a pilot.

3.3.3 *beyond visual line of sight, BVLOS, n*—operation when the UA cannot be seen by the individuals responsible for see-and-avoid with unaided (other than corrective lenses or sunglasses, or both) vision, but where the location of the sUA is known through technological means without exceeding the performance capabilities of the C2 link.

3.3.4 *controlled airspace, n*—an airspace of defined dimensions within which air traffic control service is provided in accordance with the airspace classification.

3.3.4.1 *Discussion*—For example, in the United States, Classes A, B, C, D, and E airspace.

3.3.4.2 *Discussion*—Controlled airspace does not automatically imply separation services, or that the location of all traffic is known.

3.3.5 *detect and avoid, DAA, n*—a subsystem within the UAS providing the situational awareness, alerting, and avoidance necessary to maintain safe BVLOS operation of the ownship in the presence of intruders.

3.3.6 *DAA cycle, n*—the maximum time from the presence of the intruder to the execution of an avoidance maneuver.

3.3.7 *detect function, DF, n*—the function within the DAA system tasked with maintaining temporal and spatial awareness of intruders.

3.3.8 *encounter, n*—the event associated with the presence of an intruder.

3.3.9 *encounter rate, n*—the number of encounters per unit time.

3.3.10 *intruder, n*—a manned aircraft external to ownship within or projected to be in the ownship's vicinity in the near future.

3.3.10.1 *Discussion*—This definition is deliberately equivocal since the DAA system architecture and technologies employed, as well as ownship maneuvering capabilities, will shape the specific definitions of "vicinity" and "near future."

3.3.11 *loss of well-clear risk ratio (LR) measurement, n*—the LR is the quotient of the probability of a loss of well-clear (LoWC) given an encounter with a DAA system, and the probability of loss of well-clear given an encounter without a DAA system. The lower the LR, the better the DAA system is at preventing a loss of well-clear. The LR is a measurement to ensure that a portion of the mitigation happens before loss of well-clear as opposed to after loss of WC. See Fig. 1. See also Ref (**1**).[9]

[4] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[5] Available from U.S. Government Publishing Office (GPO), 732 N. Capitol St., NW, Washington, DC 20401, http://www.govinfo.gov.

[6] Available from Federal Aviation Administration (FAA), 800 Independence Ave., SW, Washington, DC 20591, http://www.faa.gov.

[7] Available from Joint Authorities for Rulemaking on Unmanned Systems (JARUS), http://jarus-rpas.org/content/jar-doc-06-sora-package.

[8] .Available from RTCA, Inc., 1828 L St., NW, Suite 805, Washington, DC 20036. 6

[9] The boldface numbers in parentheses refer to the list of references at the end of this standard.

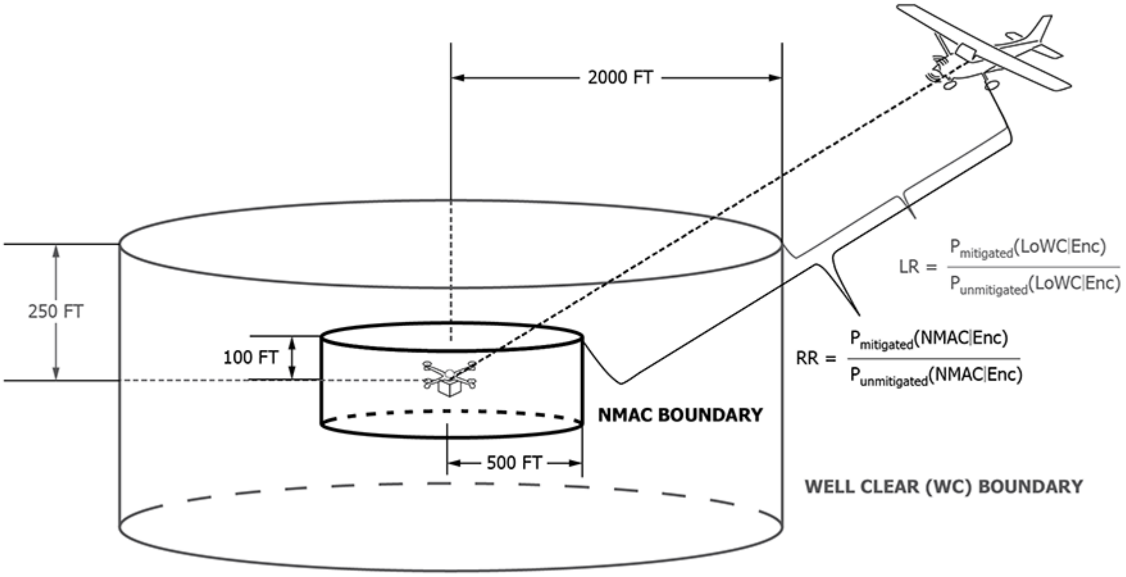
2000 FT
250 FT
100 FT
500 FT
NMAC BOUNDARY
WELL CLEAR (WC) BOUNDARY
$LR = \frac{P_{mitigated}(LoWC|Enc)}{P_{unmitigated}(LoWC|Enc)}$
$RR = \frac{P_{mitigated}(NMAC|Enc)}{P_{unmitigated}(NMAC|Enc)}$

FIG. 1 RR and LR Illustration

3.3.12 *mid-air collision, MAC, n*—two aircraft colliding with each other while in flight.

3.3.13 *near mid-air collision, NMAC, n*—two aircraft coming within 100 ft vertically and 500 ft horizontally of each other while in flight.

3.3.14 *NMAC risk ratio (RR) measurement, n*—the RR is the quotient of the probability of an NMAC given an encounter with the DAA system and the probability of an NMAC given an encounter without the DAA system. The lower the RR, the better the DAA system is at preventing an NMAC.

3.3.14.1 *Discussion*—The RR used in this assessment is not a measurement of the avoid function. The RR is a measurement from an encounter to an NMAC, and it is a measurement of all DAA systems components used in mitigating NMAC. See Fig. 1.

3.3.15 *operational volume, n*—the volume of airspace in which the UAS operation intends, or is authorized, to take place.

3.3.15.1 *Discussion*—The term *operational volume* in this specification is aligned with the JARUS use of the term in Annex C of the Specific Operations Risk Assessment (SORA) and is different from the UAS traffic management (UTM)/U-Space communities' use of the term. "Area of operation," or the intersection of acceptable air and ground risk in accordance with the concept of operations, is how this concept might be described in UTM/U-Space.

3.3.16 *ownship, n*—the UA controlled by the pilot flying and for which the pilot in command (PIC) is responsible.

3.3.17 *pilot flying, n*—an individual or system that manipulates the flight controls of an aircraft during flight; may or may not be the pilot in command.

3.3.18 *pilot in command, PIC, n*—the person who has final authority and responsibility for the operation and safety of the ownship flight; has been designated as PIC before or during the flight; and holds the appropriate category class and type-rating, if appropriate, for the conduct of the flight. **(14 CFR § 1.1)**

3.3.19 *remain well-clear (RWC) function, n*—DAA system function where the UAS takes appropriate action to prevent an intruder from penetrating the WC boundary (and thus causing a loss of separation). The action is expected to be initiated within a sufficient timeframe to conform to accepted air traffic standards. Any UAS maneuvers will be in accordance with regulations and procedures.

3.3.20 *risk ratio measurement, n*—used to measure the performance of a DAA system(s); the probability of an outcome with the DAA system(s), divided by the probability of an outcome without the DAA system(s), see Fig. 1. The lower the risk ratio, the better the DAA system is at mitigations.

3.3.21 *rural area, n*—all areas not defined as urban (see 3.3.26).

3.3.22 *track, n*—the specific collection of data that a particular DAA system accumulates and is used in determining whether an intruder aircraft is a collision risk or loss of well-clear risk, or both.

3.3.23 *uncontrolled airspace, n*—an airspace that is not controlled (see 3.3.4).

3.3.24 *unmanned aircraft, UA, n*—any aircraft that is operated without the possibility of direct human intervention from within or on the aircraft. **(Public Law 112-95 § 331)**

3.3.25 *unmanned aircraft system, UAS, n*—a system comprised of an unmanned aircraft and associated elements, including communication links, and the components that control the unmanned aircraft that are required for the pilot in command to operate safely and efficiently in the national airspace system. **(Public Law 112-95 § 331)**

3.3.26 *urban area, n*—a town, outer suburban, suburban, residential area, urban, metro, city, or open-air assembly of people, or combinations thereof.

3.3.27 *visual line of sight, VLOS, n*—unaided (corrective lenses or sunglasses, or both, excepted) visual contact between a PIC and a UA sufficient to maintain safe operational control of the aircraft, know its location, and scan the airspace in which it is operating to see and avoid other air traffic or objects aloft or on the ground.

3.3.28 *well-clear (WC) boundary, n*—for UA in lower-risk airspace as defined above 2000 ft horizontally and ±250 ft vertically (**1**).

3.3.28.1 *Discussion*—Remaining well-clear is meant to support compliance with 14 CFR § 91.111 and § 91.113 or § 107.37 (or international equivalents) and reduce the chance of creating a collision hazard and therefore a collision.[10]

4. Significance and Use

4.1 This specification outlines the system objectives, activities, and evidence required to demonstrate adequate design and safe use of a detect and avoid (DAA) system. Such systems, in concert with other systems and equipment, enable unmanned aircraft systems (UAS) to operate beyond the visual line of sight (BVLOS) of the pilot in command (PIC). As the name suggests, these systems comprise a function for sensing potential flight hazards and assessing hazard severity ("detect") and a function for maneuvering the aircraft out of the way of the hazard ("avoid"). Such systems may also support operations within the PIC's visual line of sight (VLOS).

4.1.1 While there are many possible static and dynamic hazards to UA flight (for example, obstacles, birds, terrain, weather, other UAs), this specification addresses the safe operations of the UA in the presence of manned aircraft, which may or may not be cooperative with the UA, otherwise known as "intruders."

4.1.2 Despite the diversity in emerging DAA systems, these systems share the following attributes:

4.1.2.1 *Intruder Level of Cooperation*[11]—Cooperative systems rely on information being supplied by the intruder (for example, intruder transponder, automatic dependent surveillance-broadcast (ADS-B) Out) whereas non-cooperative systems do not rely on the intruder supplying information. Many DAA systems use a combination of cooperative and non-cooperative sensors for obtaining information regarding an intruder.

4.1.2.2 *DAA Level of Autonomy*—DAA systems may range from fully manual to fully automated functionality. In the fully manual construct, the PIC is presented with data and it is up to them to decide and execute any needed maneuvers. In the fully automated construct, the system is responsible for determining and executing any necessary maneuvers. A spectrum of functional allocation is possible in between these two architectures.

4.1.2.3 *Location of DAA Systems and Functionality*—The architecture of a given DAA system may use any combination of airborne and ground components. The proximity of DAA functions to the UA versus the GCS each pose unique benefits and challenges regardless of system timing and latency, UA payload, sensor orientation, field of regard or surveillance coverage, range, track accuracy, etc.

4.1.2.4 *Sensor Type*—The greatest differentiation between DAA systems is in sensors. Sensing technologies vary and include radio frequency (radar, passive radio frequency reception), light (camera, light detection and ranging (LiDAR)), and acoustic approaches. Each offers distinct advantages and disadvantages. Therefore, DAA systems may utilize multiple sensor categories to achieve comprehensive detection and appropriate levels of uncertainty and information quality.

5. System Description

5.1 *Overview:*

5.1.1 This section identifies the set of objectives that the DAA system, including the pilots if they are required to be "in the loop," must meet as a complete unit.

5.1.2 Two classes of DAA equipment are covered by this specification: Class 1 for operations in low-risk airspace and Class 2 for operating in low- or medium-risk airspace as defined by the CAA. See 5.3.1 for more information.

5.1.3 This specification does not address integration of DAA equipment with other safety systems such as geographical containment systems (that is, geofencing) and terrain avoidance systems.

5.2 *System Verification:*

5.2.1 If required to do so by the CAA, the applicant/proponent shall provide to the CAA or CAA-approved test organization, or both, evidence of physical verification demonstrating the DAA system meets all required performance criteria identified or generated in response to this specification.

5.2.2 Physical verification may take the form of field tests against actual targets and objectives or lab tests against representative targets, as long as data is supplied confirming equivalency to real targets. An approach to verifying these requirements will be defined in an ASTM test method currently under development.

5.2.3 Analysis and simulation should be used as a form of performance verification when physical performance is impractical (for example, difficult corner cases, extensive time-based testing, or sheer volume of test case permutations). In these situations, the analysis or simulation shall still be substantiated using a sampling of physical test data to establish validity.

5.3 *Safety:*

5.3.1 *Air Collision Risk Classification of Operational Volume*—In order to assess risk, the airspace needs to be classified into categories based on airborne collision risk under which a UAS would encounter a manned aircraft. In a manner similar to the JARUS SORA, this specification assumes four unmitigated airborne collision risk classification levels: High, Medium, Low, and Extremely-Low Air Risk. However, only DAA system performance for DAA Class 1 and Class 2 systems (to be used in low- and medium-risk airspace, respectively), is in scope for this specification. As a DAA standard, this specification does not specify the method for determining the airspace risk classification level for a given operation, but general guidance is given to provide context for the system performance in low and medium air risk airspace.

[10] Alternative well-clear means may be appropriate in proximity to terrain or obstacles when justified.

[11] Intruder equipage entirely determines cooperative versus non-cooperative status.

5.3.1.1 *High Air Risk (Out of Scope for this Requirements Document)*—This is airspace where manned aircraft predominately fly or the manned aircraft encounter rate is frequent, or both. The competent authority is expected to require the operator to comply with recognized DAA system standards as available and appropriate to the application (for example, those developed by RTCA SC-228 (see RTCA DO-365A) or EUROCAE WG-105, or both).

5.3.1.2 *Medium Air Risk*—This is airspace where manned aircraft predominately do not fly (excluding helicopters and crop dusters) or the manned aircraft encounter rate is occasional, or both. This is generally uncontrolled airspace and/or airspace that goes from the ground to between 300 to 1200 ft AGL (with 500 ft AGL used as a common default), above which most manned aircraft operations are conducted. This includes airspace away from Class B, C, and D aerodromes, or near Class B, C, and D aerodromes with additional strategic mitigations.

5.3.1.3 *Low Air Risk*—This is airspace where manned aircraft predominately do not fly (excluding helicopters and crop dusters) or the manned aircraft encounter rate is remote or improbable in accordance with guidelines from the competent authority, or both. This is generally uncontrolled airspace and/or airspace that goes from the ground to between 300 to 1200 ft AGL (with 500 ft AGL used as a common default), above which most manned aircraft operations are conducted and away from urban population centers, towns, outer suburban, suburban, residential areas, metro, or cities, or combinations thereof, and outside all aerodromes.

5.3.1.4 *Extremely Low Air Risk (Out of Scope for this Requirements Document)*—This is airspace where manned aircraft predominately do not fly or the manned aircraft encounter rate is extremely improbable, or both. It is generally defined as airspace where the risk of collision between a UAS and manned aircraft is acceptable without the addition of any tactical mitigation (for example, a DAA system). An example of this may be UAS flight operations in some parts of Alaska or northern Sweden where the manned aircraft density is so low that the airspace safety threshold could be met without any mitigation.

5.3.2 *Local Air Risk Assessment of Operational Volume* (see 3.3.15)—If a local airspace authority or air navigation service provider (ANSP), or both, has conducted an airspace characterization and classified the collision risk of the operational volume, that collision risk assessment will be used as the method for categorizing the airspace. Strategic mitigations may also be used in determining the operational volume airspace categorization.

5.3.3 *Generalized Collision Risk Assessment of Operational Volume*—If a local classification of the collision risk of the operational volume does not exist, the example generalized air risk assessment in 5.3.4 can be used. The JARUS SORA is a generalized air risk assessment.

5.3.4 *Generalized Air Risk Assessment Descriptions:*

5.3.4.1 These airborne collision risk classifications are generalized classifications. As with any generalization, when the area becomes more refined, there will be specific areas where the generalized classification levels will be true, and other specific areas where the generalized classification levels will not be true. The operator will work with the local airspace authority to ensure that the appropriate air risk classification is assigned to the operational volume.

TABLE 1 Example Generalized Collision Risk Airspace Classification Summary

Airspace	Airspace Description
Medium Air Risk	Uncontrolled Airspace Below 500 ft AGL in controlled airspace, at least 5 nm away from the center point of Class B, C, and D aerodromes Below 500 ft AGL over an urban area Below 500 ft AGL in/over/around Class E, F, or G aerodromes Near Class B, C, and D aerodromes with additional strategic mitigations, for example, remaining below facility map altitudes
Low Air Risk	Uncontrolled airspace, below 500 ft AGL, over a rural area, outside all aerodromes

5.3.4.2 As with any classification scheme, it is always a balance between too few classifications and too many classifications.

5.3.4.3 *Example Generalized Airspace Air Risk Classification Summary*—See Table 1.

5.4 *UAS DAA Performance Requirements:*

5.4.1 The risk ratios in this specification are "logic" risk ratios in accordance with the International Civil Aviation Organization (ICAO)[12] definition. Included is nominal system performance: logic, specified surveillance performance, field of view limitations, expected pilot performance, specified/nominal C2 link performance, expected latencies for all components. Not included are failures: corrupted logic, sensor failures, C2 link failures, DAA equipment failures/faults, non-responsive pilot. Performance under failure conditions should be addressed through system safety assessments. Note that JARUS specifies total system risk ratios.

5.4.2 In this specification, the risk ratios discussed by the ICAO remotely piloted aircraft systems (RPAS) panel[12] have been used but are applied to a smaller well-clear boundary (for example, 2000 ft). This adjustment leads to a similar RR even with lower performing UAS DAA equipage. (See Ref (**2**).) The smaller well-clear boundary is used due to the lower closure rates and smaller P(MAC|NMAC) due to the small size of the UAS.

5.4.3 The RR and LR performance requirements in this section shall be verified using statistically significant set(s) of encounters that are representative of the operational environment airspace. Encounter sets are representative when they include appropriate and realistic distributions of ownship and intruder flight dynamics, speeds, vertical rates, and encounter geometrics for the airspace class, altitude, and geographic region where the DAA equipment is expected to operate. For cooperative intruders, encounter sets and the mix of Mode C, Mode S, and ADS-B equipped intruders for verifying ratios are

[12] See https://www.icao.int/safety/UA/Pages/Remotely-Piloted-Aircraft-Systems-Panel-(RPASP).aspx.

defined in DAA test methods. Limitations on the DAA equipment shall be identified based on limitations of the encounter sets used to verify the performance requirements.

5.4.4 In operational volumes with low and medium air risk, DAA performance for NMAC avoidance (RR) requirements are based on the ICAO work cited in 5.4.2 and are dependent on the equipage type of the intruder.

5.4.4.1 For intruders equipped with a transponder or ADS-B, the DAA system RR shall be ≤0.18.

5.4.4.2 For non-cooperative intruders, the DAA system RR shall be less than or equal to 0.30.

5.4.5 In operational volumes with low and medium air risk, DAA performance for remain well-clear (LR) requirements are based on the ICAO work cited in 5.4.2 and are dependent on the equipage type of the intruder.

5.4.5.1 For intruders equipped with a transponder or ADS-B Out, the DAA system LR shall be ≤0.40.

5.4.5.2 For non-cooperative intruders, the DAA system LR shall be ≤0.50.

5.4.6 *DAA Performance Summary*—See Table 2.

5.5 *UAS DAA Robustness Requirements:*

5.5.1 The robustness of the DAA system shall be characterized by the availability and assurance level of the system. This approach is similar to that adopted by JARUS.

5.5.2 *DAA System Availability:*

5.5.2.1 The approach to system availability here is derived from the JARUS process for UAS Special Operation Risk Assessment. The level of system availability of the DAA system differentiates Class 1 and 2 systems. Loss of function includes failures such as sensor failures, C2 link failures, and DAA equipment failures, which are not captured in the RR and LR performance requirements.

5.5.2.2 For Class 1 equipment (operational volumes with low air risk), the allowable loss of function and performance shall be less than 1 per 100 flight hours (1E-2 Loss/FH).

5.5.2.3 For Class 2 equipment (operational volumes with medium air risk), the allowable loss of function and performance shall be less than 1 per 1000 flight hours (1E-3 Loss/FH).

5.5.3 *DAA System Assurance:*

5.5.3.1 The approach to system assurance here is derived from the JARUS process for UAS Special Operation Risk Assessment. The level of system assurance of the DAA system differentiates Class 1 and 2 systems. Hazardously misleading information is introduced by undetected software and hardware faults which aren't captured in the RR and LR performance requirements. Hazardously misleading information does not include information, such as false tracks, that does not result in a hazardous maneuver. Likewise, hazardously misleading information does not include faults that are detected and covered by the loss of function requirements in 5.5.2.

TABLE 2 Summary of DAA Performance Guidance for UAS

Intruder Equipage	DAA Quantitative Performance Requirements	
	NMAC Risk Ratio (RR)	Loss of Well-Clear Risk Ratio (LR)
Transponder or ADS-B Out	≤0.18	≤0.40
Non-cooperative	≤0.30	≤0.50

5.5.3.2 For Class 1 equipment (operations in low air risk airspace), the allowable introduction of hazardously misleading information shall be less than 1 per 10 000 flight hours (1E-4 Loss/FH).

5.5.3.3 For Class 2 equipment (operations in low or medium air risk airspace), the allowable introduction of hazardously misleading information shall be less than 1 per 100 000 flight hours (1E-5 Loss/FH).

5.6 *Reliability and Maintenance:*

5.6.1 A methodology for anticipating failures and accomplishing appropriate maintenance actions should be identified for the major subsystems or components of the DAA system, as well as the system as a whole.

5.6.1.1 If required, the DAA system shall have a maintenance plan and maintenance schedule in accordance with the maintenance instructions provided by the manufacturer. The maintenance instructions shall provide direction as to verification of proper installation and calibration of the system to ensure continued performance is met in the field.

5.6.2 The DAA system shall have a test function for detecting probable "static" system failures. "Static" system failures are degradations in the condition of the system that would prevent correct operation (for example, memory faults, device failures, wear out). These are different than "dynamic" errors which are due to unforeseen events during runtime. Test function requirements should be based on system safety principles considering rate, exposure, and criticality of latent failure.

5.6.3 The DAA system shall detect and notify the PIC of any degradation or loss of function that requires PIC action or take predefined automated contingency action to mitigate the risk if required by the operational safety case, within a timeframe appropriate for the alerting condition. A degradation of function includes *(1)* any partial loss of functionality or *(2)* any reduction of performance as required or advertised by the system. This does not prescribe specific mechanics of how a degradation or loss of function alert is to be communicated; depending on the safety assessment, it may be appropriate to have no in-flight indication or action. If notification is required, it may be a dedicated message, a special error code in an existing message, an invalid value in the field representing the loss of functionality, or a maintenance code. The DAA system shall persist the notification of degradation or loss of function until the functionality is fully restored. Human factors and training should be considered in the design of PIC notification.

5.7 *Security:*

5.7.1 The PIC shall be notified of any changes to DAA software, hardware, or configuration. This notification may take many forms, including technical or operational means, such as inspection or automatic reporting.

5.7.2 Making any changes to DAA software, hardware, or configuration shall be restricted to authorized and qualified personnel. This restriction may be implemented through various mechanisms, including technical or operational means.

5.7.3 Any changes to DAA software, hardware, or configuration shall require confirmation that the modified information is correct and uncorrupted. Confirmation may come in any combination of cyclic redundancy code (CRC)/checksums, digital signatures, embedded registers, pin-strapping, or manual checklists, or combinations thereof.

5.7.4 There shall be a means to prevent any changes to the DAA software, hardware, or configuration from inadvertently or maliciously occurring, or a suitable preflight check to detect and prevent takeoff if it were to occur. This requirement may be implemented through various mechanisms, including technical or operational means.

5.7.5 Control of the DAA system during flight shall only be accessible via authorized means.

5.8 *Environment:*

5.8.1 The DAA system shall satisfy performance requirements across the range of environmental conditions as defined by the manufacturer and communicated to the customer.

5.8.2 The DAA system integrator shall identify all environmental limitations of the system where it does not meet the performance requirements in 5.4 and document them in the operator's manual and technical specifications documents.

6. System Timing

6.1 Fig. 2 outlines each segment of time from acquisition of an intruder by the detect function to the execution of the avoidance maneuver. Regardless of whether the system is airborne or ground-based, uses a pilot-in-the-loop or full-autonomy, the timing of every DAA system can be described in terms of the model in Fig. 2. Depending on the system, it is permissible that some of the terms be zero or combined to a measurable level.

6.2 The maximum time from acquisition of an intruder by the detect function to confirmation of the maneuver beginning is described in terms of the model in Fig. 2.

6.3 *Detection Function (DF) Timing:*

6.3.1 t_{Scan} = The maximum time between sensor updates of the detected intruder, setting the minimum time precision of the DF.

6.3.2 t_{Relay} = The maximum latency from the sensor to its sensor processing/fusion, including any publishing rate of the sensor.

6.3.3 t_{Filter} = The maximum time required to pre-process the sensor data (for example, filtering, fusion, tracking) before passing along to the Alert function.

6.3.4 $t_{Publish}$ = The maximum latency from the filter processing to the presentation of the data to the Alert function, including any publishing rate of the filter processing.

6.3.5 The DF has flexibility in the time required to ascertain the presence of an intruder, as long as the safety performance (see 5.4) is met. The system trade-off is in the additional range at which intruders must be detected to satisfy alert times, which provide the appropriate safety performance and in the responsiveness of the system to a dynamically changing environment.

6.4 *Alert Function (A1F) Timing:*

6.4.1 $t_{Classify}$ = The maximum time required in the determination and prioritization of the hazard level of each updated intruder.

6.4.2 t_{Notify} = The maximum time required to present the updated list of intruder hazards to the avoid function, including any publishing rate of the classifier.

6.5 *Avoid Function (A2F) Timing:*

6.5.1 t_{Plot} = The maximum time required for the avoid function to determine a satisfactory avoidance trajectory.

6.5.2 t_{Vector} = The maximum latency, including any publishing rate, of transferring the avoidance trajectory to the vehicle command.

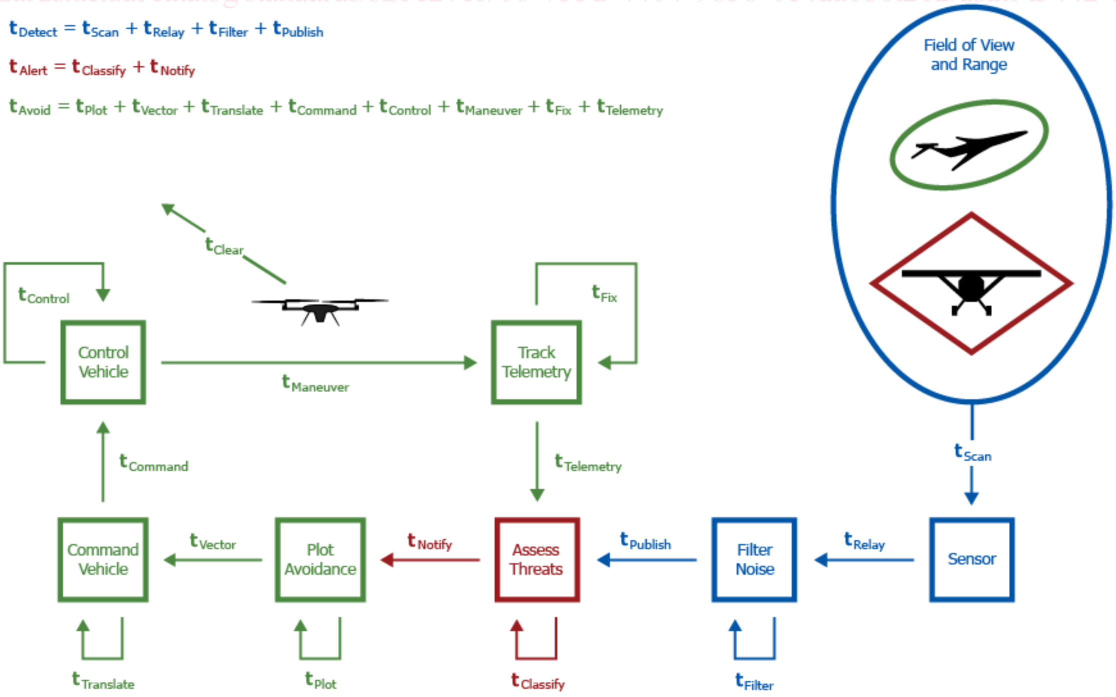

FIG. 2 System Timing Model

6.5.3 $t_{Translate}$ = The maximum time needed to convert the trajectory to one or more vehicle command(s).

6.5.4 $t_{Command}$ = The maximum latency, including any publishing rate, of transferring the vehicle commands to the UA flight control.

NOTE 1—t_{Plot}, t_{Vector}, and $t_{Command}$ may be combined into a single human processing time if conducted manually by a human.

6.5.5 $t_{Control}$ = The maximum delay from receiving to initiating execution of the vehicle commands.

6.5.6 $t_{Maneuver}$ = The time allotted for executing the maneuver. This may be the maximum time required to execute a maneuver sufficient to generate full separation (horizontally or vertically) to maintain well-clear.

6.5.7 t_{Fix} = The maximum time required to determine the updated position and orientation of the ownship.

6.5.8 $t_{Telemetry}$ = The maximum latency, including publishing rate, of relaying the updated position and orientation of the UA to the alert function.

7. Detection Function

7.1 *Overview*—This section defines the functionality, behavior, and performance required of the DF within an integrated DAA system. The role of the DF is to gather information regarding potential intruders that may pose a threat to the UA ownship and present the information in a form usable by follow-on functions (for example, adequately complete, timely, accurate, clean, and suited for the intended information consumer).

7.2 *Function:*

7.2.1 The DF shall surveil the airspace.

NOTE 2—The DF may work with sensors that provide raw surveillance measurements or surveillance tracks.

7.2.2 Upon detecting the presence of an intruder, the DF shall determine the track of the intruder as required by the alert function (A1F) in order to identify and prioritize hazards.

NOTE 3—A track may be based on information from a single sensor or the fusion of information from multiple sensors. Such track parameters may include: *(1)* lateral position, *(2)* velocity (speed and direction), *(3)* altitude, and *(4)* closure rate. These parameters may be absolute to the surrounding environment (for example, latitude, longitude, altitude) or relative to the UA ownship (for example, range, bearing, angular elevation).

7.2.3 The DF shall output the track(s) of all detected intruders to the A1F.

7.2.4 *Track Coasting:*

7.2.4.1 When an intruder with an existing track is no longer detected, the DF should continue the track by extrapolating that intruder's trajectory to the current time using its last known position and velocity and report it to the A1F as a coasted track. The DF may use intruder trend data, up to and including the last known position and velocity vector, for extrapolating the coasted track. However, the DF shall not use an intruder's registered flight plan for extrapolation because the intruder may deviate from the flight plan at any time. (Refer also to A1F track coasting requirements in 8.2.9.)

7.2.4.2 The DF should designate any track for which the intruder was not detected in the last surveillance cycle (t_{Scan}) as a coasted track and indicate the time coasted.

7.3 *Performance*—An approach to verifying these requirements will be defined in an ASTM test method currently under development.

7.3.1 *Capacity*—The DF vendor shall identify the maximum number of targets that can be tracked simultaneously without violating the DF timing budget, as described in Section 6. The DAA integrator shall identify the maximum number of aircraft and non-aircraft tracks passed on to the A2F so as not to violate assumptions concerning PIC workloads nor violate good human factors engineering considerations. The DAA system integrator shall demonstrate this maximum number is sufficient to meet LR and RR requirements given the air vehicle traffic rates in the operational environment, the rates for false tracks (for example, sensor noise and ground clutter), and the rates for tracks of non-interest (for example, real tracks on non-aircraft objects such as cars, birds, clouds).

NOTE 4—A false track is an illusionary type of non-aircraft track.

7.3.2 *Field of View (FOV)/Field of Regard (FOR)*—The DF vendor shall identify the FOV/FOR of each sensor in terms of azimuth and minimum/maximum angular elevation or coverage volume. The DAA system integrator shall demonstrate that this coverage meets the overall DAA system RR and LR performance requirements, and that the FOV/FOR meet any operational minimum coverage requirements.

NOTE 5—Regulatory requirements for small UAS to give way to all manned traffic may drive requirements for greater FOV/FOR than would be required to meet LR and RR requirements.

7.3.3 *Range*—The DAA system integrator shall identify the detection and usable track range(s) needed from the DF for relevant intruders as defined by the encounter models, demonstrating that the detection and usable track range(s) provide sufficient detection performance to meet overall system RR and LR requirements. The DF shall detect intruders out to the range(s) identified above for each sensor across its full FOV/FOR.

7.3.4 *Sensitivity*—The DAA system integrator shall demonstrate that the DF can acquire and maintain an intruder track of acceptable quality to meet LR and RR requirements across the range of intruder flight performance relative to the orientation of the DF sensor(s). The DF vendor shall demonstrate this detection sensitivity across the combined FOV/FOR and range(s) of the DF. Sensitivity may vary by sensor type and could include such considerations as the range of possible velocities, attitude, and angle of approach relative to the sensor, volume level, range of lighting conditions, etc.

7.3.5 *Precision*—The DAA system integrator shall identify and demonstrate the precision of the track necessary to meet LR and RR requirements and shall include this precision in the determination of the maximum detection ranges required of each sensor, as defined in 7.3.3.

7.3.6 *Accuracy*—The DAA system integrator shall identify and demonstrate that the aggregate accuracy of the sensor(s) is sufficient to ascertain the position and velocity of an intruder to the level necessary to meet the required LR and RR. System accuracy must consider the precision of the sensors, as defined in 7.3.5 (Note: precision error will manifest itself as quantization error for accuracy), and the effects of latency due to measurement delay, as identified in 6.3.

7.3.7 *Interference, Ambient Noise, and Clutter*—The DF shall meet all the performance requirements of this specification in the presence of interference, noise, and clutter sources found within the operational environment as specified in 7.3.7.1 – 7.3.7.3.

7.3.7.1 *Interference*—Interference is defined as any signal that diminishes the usable signal to noise ratio for a DAA system. Sources of interference will vary by sensor modality but may include such examples as other RF transmissions in the same band (radar), direct sunlight (camera), wave cancellation (acoustic), etc.

7.3.7.2 *Ambient Noise*—Ambient Noise is defined as the detected ambient background signals measured under quiescent, operational conditions. The ambient noise level is the level where the signal from an aircraft can no longer be distinguished from ambient background measurements under quiescent operating conditions. For radar, the ambient noise level may be specified as the signal amplitude at which an aircraft return signal cannot be distinguished from the RF noise floor. For a camera, the ambient signal level may be that contrast ratio at which a relevant aircraft cannot be identified against operational background scenes. For acoustics, the ambient noise level may be specified as the signal amplitude at which an aircraft signature cannot be distinguished from flow and platform noise during operational conditions. Note that this specification does not preclude the use of dynamic configuration, adaptive thresholding, or other forms of modifying the response of the system to variation of ambient noise due to changes in the environment.

7.3.7.3 *Clutter*—Clutter is defined as the measured signals generated by sources other than aircraft that may be present in addition to noise. Clutter is situational and episodic, whereas ambient noise is always present during operation. For radar, clutter may be echo returns from objects in the environment that are not aircraft, like automobiles. For cameras, clutter may be images of clouds, birds, or moving trees. For acoustics, clutter may be the sound of a train. Hazardous objects including birds, ground obstacles, and possibly clouds (depending on the operational limitations) should not be counted as clutter in the determination of DAA system performance. The DAA system integrator shall identify possible sources of clutter based on the sensor modalities used.

7.4 *Timing of Built-in-Tests (BIT)*—The DF shall provide an indication when BITs and configuration are complete, and detection/tracking of intruders is available or, conversely, when the system is not available. In the event of a midflight restart, the PIC shall be continuously alerted to the loss of function until such time as the DF resumes detection of intruders.

8. Alert Function

8.1 *Overview:*

8.1.1 This section defines the functionality, behavior, and performance required of the alert function (A1F) within an integrated DAA system. The role of the A1F is the identification and prioritization of hazards from the intruder information received from the DF. These hazards, or "alerts," are then provided to the avoid function (A2F) for determining appropriate UA response.

8.1.2 For pilot-in-the-loop systems and for automated avoidance systems as appropriate, the A1F also provides alert information to a visual/aural component for apprising the PIC of hazards and the changing status of alerts.

8.1.3 This specification does not define the allocation of A1F between the UA and GCS. It is conceivable, especially for airborne DAA, that parts of the alerting function could be onboard the UA while other parts could be in the GCS or a sensor console, or both, but many other architectures could be envisioned.

8.2 *Function:*

8.2.1 At a minimum, the A1F shall issue an alert for an intruder if it determines that the UA must maneuver to remain well-clear from that intruder. This alert shall be declared early enough to permit resolution of the hazard (within the appropriate LoWC and NMAC risk ratio thresholds) and no later than the occurrence of loss of well-clear. For a pilot-in-the-loop system, this alert shall be annunciated as a warning-level alert in accordance with AC 25.1322-1, Section 6(b), indicating that immediate pilot awareness is required and immediate pilot action is required.

8.2.2 Additional levels of alerting may be employed for prioritization of alerts and as appropriate for the system concept of operations (CONOPS) (for example, additional alert levels might be desirable for a pilot-in-the-loop system).

8.2.2.1 The A1F may issue a lower-priority alert for an intruder if that aircraft does not or is not currently expected to lose well-clear. These alerts are intended to highlight intruder aircraft (for example, for PIC awareness) that may abruptly become a LoWC or NMAC hazard if either the intruder or the ownship maneuvers. If implemented for a pilot-in-the-loop system, these alerts shall be annunciated as advisory or caution-level alerts in accordance with AC 25.1322-1.

8.2.2.2 The A1F may issue a higher-priority alert for an intruder if it determines that the UA must maneuver to avoid NMAC with that intruder. If implemented, this alert shall be declared early enough to permit resolution of the hazard (within the appropriate NMAC risk ratio threshold) and no later than the occurrence of NMAC. If implemented for a pilot-in-the-loop system, this alert shall be annunciated as a warning-level alert in accordance with AC 25.1322-1, indicating that pilot action is required.

8.2.3 The A1F shall pass the following information regarding the intruder to the A2F. The same data should be passed to the display as is relevant for the system CONOPS. The accuracy and precision of this data is dependent on the underlying DF.

8.2.3.1 Alert status (on/off or alert level for systems implementing multiple alert levels);

8.2.3.2 Bearing of the intruder relative to ownship trajectory;

8.2.3.3 Velocity (speed and direction) of the intruder (including vertical velocity, if available);

8.2.3.4 Range of the intruder from the ownship;

8.2.3.5 Vertical separation of intruder from the ownship, if available.

8.2.4 For an ownship automatically flying a pre-determined flight plan, the A1F may calculate alerts along the planned horizontal or vertical flight path, or both, using the future positions and velocities along the flight path. For an ownship not flying according to a pre-determined flight plan or forced to temporarily deviate from its flight plan, the A1F shall calculate the alerts using the current position and velocity vector of the ownship.

8.2.5 For an intruder, the A1F shall calculate alerts using the current state (for example, position and velocity) of the intruder. A registered flight plan shall not be used for calculation of alerting for an intruder since the intruder may deviate from its flight plan at any time.

8.2.6 The A1F shall update alerts and targets in the following prioritized order consistent with AC 25.1322-1 Flightcrew Alerting:

(1) Warning-level alerts
(2) Caution-level alerts
(3) Advisory alerts
(4) Other detected traffic

8.2.7 For alerts of the same priority level, the A1F shall further prioritize the alerts by a criterion associated with reduced collision risk, such as by increasing order of time to Closest Point of Approach (CPA).

8.2.8 For an intruder meeting the criteria of multiple alerts (for example, both caution and warning-level alert criteria), the A1F shall assign the highest priority alert to the intruder based on the priority rules in this section.

8.2.9 *Alerting on Coasted Tracks:*

8.2.9.1 The A1F may coast a non-current track by extrapolating the intruder's trajectory to the current time using its last known position and velocity.

8.2.9.2 If the A1F implements track coasting, it may use intruder trend data (for example, turn rate) up to and including the last known position and velocity vector for extrapolating the coasted track. However, the A1F shall not use an intruder's registered flight plan for extrapolation because the intruder could deviate from the flight plan at any time.

8.2.9.3 If the A1F implements track coasting, a maximum coasting time shall be identified at which the appropriate NMAC and LoWC risk ratios are still achieved.

8.2.9.4 The A1F shall provide alerts on any tracks that have been coasted for less than the identified maximum coast time in the same manner as current tracks (that is, in accordance with 8.2.5).

8.2.9.5 The A1F shall generate no alerts on coasted tracks exceeding the maximum coast time.

8.2.9.6 The A1F shall pass no information on coasted tracks exceeding the maximum coast time to the A2F.

8.3 *Timing*—The A1F shall output the updated alert status of an intruder no later than $t_{Classify} + t_{Notify}$ (as defined in 6.4) after receiving new data on the intruder from the DF and subject to the timing analysis of 9.3.

8.4 *Human Machine Interface:*

8.4.1 Even for systems with a high degree of autonomy, some level of human interaction or oversight will be needed. This section addresses those human machine interface (HMI) considerations. Unless otherwise specified, all requirements for display of information in this section can be satisfied either graphically or as part of a data label.

8.4.2 At a minimum, all traffic meeting the alerting conditions in 8.2.1 and, if implemented, 8.2.2 shall be displayed.

8.4.3 The DAA traffic display shall provide traffic information appropriate to the DAA system CONOPS for each displayed traffic element. More/different information may be appropriate for a pilot-in-the-loop system than for a fully automatic one. Some examples of traffic information that may be displayed are as follows:

8.4.3.1 Horizontal position (range and azimuth of traffic symbol on display),

8.4.3.2 Traffic directionality (if applicable),

8.4.3.3 Traffic altitude,

8.4.3.4 Traffic vertical direction indicator (an indication of climb or descent) when vertical rate is available and is greater than or equal to a threshold established by the developer (nominally, 500 ft/min), and

8.4.3.5 Horizontal velocity trend (for example, predictor line or history trail).

8.4.4 The traffic display shall not display traffic coasted beyond that maximum coasting time of 8.2.9.3.

8.4.5 The traffic display shall use the following colors to present alert information (see AC 25.1322-1):

8.4.5.1 Warning-level alerts – Red.

8.4.5.2 Caution-level alerts – Amber or yellow.

8.4.5.3 Advisory-level alerts – Any color except red, green, or amber/yellow, consistent with flight deck philosophy.

8.4.5.4 Non-alert traffic – Any color except red, green, or amber/yellow, consistent with flight deck philosophy.

8.4.6 Iconography should provide more than one dimension of encoding. This may take many forms, including color and symbol shape.

8.4.7 The A1F should avoid information clutter on a display. Therefore, other intruder parameters beyond what is specified in 8.4.3 may be called up by the operator upon request. Examples of methods by which this may be done include:

8.4.7.1 A separate window or table in alert priority order, and

8.4.7.2 Expanded parameter detail when the operator selects a specific alert icon (for example, data block).

8.4.8 Warning-level alerts and caution-level alerts, and only warning and caution-level alerts, shall include distinct aural indications (also known as "aural alerts").

8.4.9 The A1F may inhibit or suppress (as described by AC 25.1322-1) aural alerts when directed by the operator. This is provided as an aid to minimizing operator workload during critical phases of the mission. If the capability to inhibit or suppress aural alerts has been implemented, the display shall indicate to the PIC when the aural alerts have been inhibited or suppressed.

9. Avoid Function

9.1 *Overview:*

9.1.1 This section defines the functionality, behavior, and performance required of the avoid function (A2F) within the integrated DAA system. The purpose of the A2F is to calculate an avoidance maneuver for the ownship that reduces the likelihood of an undesired interaction with an intruder.

9.1.2 Avoidance functions may be automated or performed manually by a pilot based on the A1F output.

9.2 *A2F Behavior:*

9.2.1 Note the following requirements do not define the solution methodology. Any number of algorithms and human-decision aids may be configured to achieve this prioritization of objectives. The requirements in this subsection do not apply to DAA systems where a human solely performs the A2F.

9.2.2 In the presence of one or more actionable alerts, the A2F shall calculate and initiate a maneuver, which increases horizontal or vertical minimum separation, or both, from the identified intruder(s) to the point of placing those intruders beyond the alerting threshold. (Note: this requirement fundamentally defines what is meant by "avoidance.") Complete avoidance (that is, separation from the intruder beyond the alerting threshold) may not be immediately possible until after a series of executed avoidance maneuvers. This is particularly the case in the presence of multiple alerts or additional constraints to viable avoidance vectors (for example, obstacles, airspace restrictions). In these situations, the objective is to continue avoiding to the point that no intruder poses a potential hazard to ownship.

9.2.3 Pilot-actionable A2F information shall be displayed to enhance pilot situational awareness, even where the A2F function is automatic.

9.2.4 If the A2F cannot determine a viable maneuver to resolve all alerts, in the absence of a more rational approach, the A2F should prioritize avoidance objectives (in descending order) as follows:

9.2.4.1 Avoid alerts in increasing order of time to CPA.

9.2.4.2 Avoid alerts in increasing order of range (that is, diverging courses).

9.2.4.3 If a tiered alerting scheme is used, the A2F should further prioritize alerts by order of importance. For example (again prioritized in descending order):

(1) Avoid alerts to prevent NMAC in increasing order of time to CPA.

(2) Avoid alerts to prevent NMAC in increasing order of range (that is, diverging courses).

(3) Avoid alerts to prevent LoWC in increasing order of time to CPA.

(4) Avoid alerts to prevent LoWC in increasing order of range (that is, diverging courses).

9.2.5 The A2F shall not command maneuvers exceeding the safety envelope of the UA.

9.2.6 There shall be a manual or automatic mechanism to avoid risk to people and property on the ground due to DAA maneuvers.

9.3 *Timing:*

9.3.1 The DAA system integrator shall perform a timing analysis to determine the timing elements for the DAA system.

9.3.2 The A1F and A2F shall update provided information at a rate commensurate with the timing analysis.

9.3.3 The A2F shall initiate an updated avoidance maneuver to the ownship no later than $t_{Plot} + t_{Vector} + t_{Translate} + t_{Command} + t_{Control}$ after receiving an actionable alert list from A1F commensurate with the timing analysis.

9.3.4 If the A2F is responsible for providing the ownship position to the A1F, the A2F shall publish to the A1F the new position of the ownship no later than $t_{Maneuver} + t_{Fix} + t_{Telemetry}$ after an actionable avoidance maneuver is initiated as defined in the timing analysis.

9.3.5 At a minimum, the A2F shall identify an avoidance maneuver in a time sufficient for the maneuver to be executed such that loss of well-clear or NMAC, or both, are avoided within the respective risk ratio thresholds.

10. Incident Log

10.1 *Overview*—An incident log is necessary for recreating the events leading up to an NMAC or other incident and to ascertain how the DAA system affected the incident. This information is also vital for continued maturation of the DAA system.

10.2 *Function:*

10.2.1 The DAA system shall include a log generation function for post-incident analysis.

10.2.2 At a minimum, the DAA system shall record in the log all intruders that have entered the alert threshold during operation of the DAA system.

10.2.3 The DAA system shall update the data in the log no less than once per second.

10.2.4 The DAA system shall record in the log all parameters supplied by the DF regarding the intruder. (See 8.2 for the minimum set of parameters the DF must capture for each detected target.)

10.2.5 There should be a mechanism for quickly identifying events in post-flight analysis.

10.2.6 The DAA system shall uniquely timestamp each entry in the log so as to establish the exact chronology of events.

10.2.7 For each entry in the log, the DAA system shall record the lateral and vertical position, velocity, and heading of each ownship and intruder.