

Aerospace - Vehicle Management Systems - Flight Control Design, Installation and Test of,
Military Unmanned Aircraft, Specification Guide For

RATIONALE

This document is published for the following reasons:

- a. Address the need for standards and guide documents for Unmanned Aircraft onboard systems.
- b. Provide recommended practices for the specification of the flight control related functions of military Unmanned Aircraft Vehicle Management Systems.
- c. Recommend a method for the specification of the appropriate level of flight control capability for an Unmanned Aircraft.
- d. Address the integration of the flight control functions with all other elements of the vehicle.

TABLE OF CONTENTS

1.	SCOPE.....	4
1.1	Vehicle Management Systems	4
1.2	Document Coverage	4
1.3	Document Exclusions	4
1.4	Related Document	4
1.5	Best Practices and Procuring Activity Approval.....	5
2.	REFERENCES.....	5
2.1	Applicable Documents	5
2.1.1	SAE Publications.....	5
2.1.2	ASME Publications.....	6
2.1.3	ASTM Publications.....	6
2.1.4	FAA Publications.....	6
2.1.5	IEEE Publications.....	6
2.1.6	International Standards Organization (ISO) Publications	6
2.1.7	ICAO Publications.....	6
2.1.8	National Aerospace Standards (NAS) Publications.....	6
2.1.9	RTCA Publications.....	7
2.1.10	U.S. Government Publications.....	7
2.2	Abbreviations, Acronyms, Symbols and Their Definitions	10
2.3	Definitions	12
2.3.1	UA Design and Operational Categorization Schemes.....	12
2.3.2	Flight Control Functional Classifications.....	19
2.3.3	VMS Operational State Classifications	20
2.3.4	VMS Criticality Classifications.....	21
2.3.5	VMS Component Structural Classifications.....	21

SAE Technical Standards Board Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2012 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE ARP94910

**SAE values your input. To provide feedback
on this Technical Report, please visit
<http://www.sae.org/technical/standards/ARP94910>**

Documents

Document Sharing Hub

2.3.6	Document Definitions	21
2.3.7	Definitions of Terminology for Precision Ship Board Landing	21
2.3.8	Safety and Operability Terminology Definitions	22
2.3.9	Definitions of Modal and Other Auxiliaries	22
3.	RECOMMENDATIONS	23
3.1	General System Recommendations	23
3.1.1	Safety and Operability Considerations	23
3.1.2	Reliability Considerations	28
3.1.3	Redundancy Considerations	29
3.1.4	Maintainability Considerations	31
3.1.5	Survivability Requirements	32
3.1.6	Electromagnetic Interference (EMI) Limits	35
3.2	System Performance Recommended Requirements	35
3.2.1	General VMS Flight Control Performance Recommendations	35
3.2.2	Primary Flight Control Recommended Requirements	42
3.2.3	Secondary Flight Controls	43
3.2.4	Ground Control Modes	44
3.2.5	Manual, Assisted and Autonomous Control Mode Performance Recommended Requirements	46
3.3	System Testability Recommendations	60
3.3.1	System Test and Monitoring Provisions	60
3.3.2	Built-In-Test Equipment	60
3.3.3	Maintenance BIT	61
3.3.4	Preflight or Pre-engage BIT	61
3.3.5	Preflight BIT Status Annunciation Support for CS	61
3.3.6	Portable Test Equipment	61
3.3.7	Ground Power Requirements for System Test	61
3.3.8	Protection Against Dormant Failures	61
3.4	System Design Recommended Requirements	62
3.4.1	System General Design Recommended Requirements	62
3.4.2	Mechanical VMS Design	62
3.4.3	Fixed Wing V/STOL Aircraft Requirements	63
3.4.4	Rotorcraft Requirements	63
3.4.5	Electrical VMS Design	64
3.4.6	Computational Methods and Software	66
3.5	Subsystem Design Recommendations	69
3.5.1	Subsystem General Design Recommended Requirements	69
3.5.2	Electrical Power Subsystems	69
3.5.3	Hydraulic Power Subsystems	70
3.5.4	Pneumatic Power Subsystems	70
3.5.5	Actuation Subsystems	70
3.5.6	Display and Annunciation	84
3.5.7	Sensors	84
3.6	Component Design and Fabrication Recommendations	85
3.6.1	General Component Recommended Requirements	85
3.6.2	Mechanical Components	86
3.6.3	Electrical and Electronic Components	87
3.6.4	Assembly Design	90
3.6.5	Component Installation	92
3.6.6	Component Fabrication	93
4.	VERIFICATION AND VALIDATION	94
4.1	General Recommendations	94
4.1.1	Methods for Demonstration of Compliance	94
4.2	Analysis Recommendations	95
4.2.1	Simulations	96
4.2.2	Reliability and Failure Mode, Effects and Criticality Analysis	96
4.2.3	Vulnerability Analysis	96

4.2.4	Maintainability Analysis	96
4.2.5	System Safety Analysis.....	96
4.2.6	Operation in Turbulence Analysis	97
4.2.7	Stability Analysis	97
4.2.8	Nuclear Survivability Analysis	97
4.3	Software and Firmware Verification	97
4.4	Test Recommendations	98
4.4.1	General Test Recommended Requirements	98
4.4.2	Laboratory Tests	99
4.4.3	Aircraft Ground Tests	100
4.4.4	Aircraft Flight Tests	101
4.5	Qualification (Preproduction) Tests	101
4.5.1	Reliability Development Tests.....	101
4.5.2	Maintainability Demonstration.....	101
4.5.3	Human Factors Engineering Verification Tests	101
4.5.4	Production/Acceptance Testing	102
4.6	Documentation	102
4.6.1	VMS Development Plan	102
4.6.2	VMS Specification	103
4.6.3	Design and Test Data Recommendations	103
4.6.4	Software Documentation.....	105
5.	NOTES	105
APPENDIX A	RECOMMENDATION APPLICABILITY BY VMS TYPE.....	106
FIGURE 1	UA SYSTEM FUNCTIONAL ARCHITECTURE.....	18
FIGURE 2	TYPICAL SYSTEMS INTERFACES WITH VMS FLIGHT CONTROLS.....	19
FIGURE 3	SELECTION OF BASELINE VMS TYPE.....	27
TABLE 1	UNMANNED AIRCRAFT CATEGORIES	13
TABLE 2	VMS QUANTITATIVE FLIGHT SAFETY REQUIREMENTS.....	24
TABLE 3	VMS TYPES.....	26
TABLE 4	UA OPERATING AREA	27
TABLE 5	SUGGESTED VMS TYPE BASED UPON UA CATEGORY AND OPERATING AREA	27
TABLE 6	REDUNDANCY EXAMPLES	30
TABLE 7	GAIN AND PHASE MARGIN REQUIREMENTS.....	37
TABLE 8	TURBULENCE INTENSITY EXCEEDANCE PROBABILITY	39
TABLE 9	ROOT-MEAN-SQUARE GUST INTENSITIES FOR SELECTED CUMULATIVE EXCEEDANCE PROBABILITIES (FEET PER SECOND TRUE AIRSPEED)	40
TABLE 10	FAILURE TRANSIENT CASES	42

1. SCOPE

This document establishes recommended practices for the specification of general performance, design, test, development, and quality assurance requirements for the flight control related functions of the Vehicle Management Systems (VMS) of military Unmanned Aircraft (UA), the airborne element of Unmanned Aircraft Systems (UAS), as defined by ASTM F 2395-07. The document is written for military unmanned aircraft intended for use primarily in military operational areas. The document also provides a foundation for considerations applicable to safe flight in all classes of airspace.

1.1 Vehicle Management Systems

UA VMS include all components and functions used to sense vehicle position, velocity, speed, inertial attitudes, rates and accelerations, heading and altitude, to generate flight path commands and to control aircraft force and moment producers to satisfy these commands. Guidance and navigation elements and functions of the VMS normally control aircraft altitude, airspeed, heading, attitude, aerodynamic or geometric configuration, and structural modes, including commands received from a remote operator.

1.2 Document Coverage

The document recommends requirements for the general performance, design, test, development and quality assurance measures for the flight control of remotely controlled, augmented and autonomous UA. At the system performance level the document employs a functional emphasis. It recommends a practice for specifying the levels of flight control capability, particularly fault accommodation after failures, required for UA of differing size, function and operational strategy. It defines the boundaries of UA flight control to include hardware and functionality not typically considered core flight control elements in a manned aircraft, such as navigation sensors and flight path and engine power command generation. It also guides the specification of the flight control Interfaces with all other systems and subsystems of the vehicle.

At the subsystem and component levels the document addresses those aspects of hardware design that impact system performance. Among components included are the inertial sensors, global positioning sensors, air data sensors, test devices, actuators, electrical power sources, hydraulic power sources, and signal transmission lines within the vehicle and dedicated to flight control.

1.3 Document Exclusions

Because of the wide range of UA size and capability UA VMS hardware design architectures differ widely. At the system level the document avoids any hardware emphasis and does not recommend particular hardware design approaches. The document provides guidance for the specification of elements of the UA vehicle only and not the other elements of the UAS such as the Control Station (CS). For example, it addresses the integration with the up-link and down-link of the command loop but not the specification of these links. Also excluded are aerodynamic surfaces, engines and engine control systems, rotorcraft rotors and fire control devices. The requirements for UAS operation in non-segregated airspace include factors such as See and Avoid and other functions, beyond those considered for manned military aircraft. These requirements are still evolving and are beyond the scope of this document.

1.4 Related Document

This Aerospace Recommended Practice (ARP) is closely related to the Aerospace Standard AS94900, for the flight control systems of manned aircraft and follows a similar format.

1.5 Best Practices and Procuring Activity Approval

This ARP is intended as a guide to standard practice and is subject to change to keep pace with experience and technical advances. Most of the technical concepts and approaches covered by the document represent industry "best practice". They are based on sound and proven engineering practices and have demonstrated successful production experience. Others require specific approval from the procuring activity before use. This recommendation for approval is not intended to inhibit their use; but rather to ensure that the prime contractor has fully investigated their capability to perform reliably and to be sufficiently durable under the required conditions and that the prime contractor can present substantiating evidence for approval before the design is committed to.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or 724-776-4970 (outside USA), www.sae.org.

ARP490	Electrohydraulic Servovalves
ARP988	Electrohydraulic Mechanical Feedback Servoactuators
AIR1083	Airborne Hydraulic and Control System Survivability for Military Aircraft
ARP1281	Actuators: Aircraft Flight Controls, Power Operated, Hydraulic, General Specification For
ARP4058	Actuators: Mechanical, Geared Rotary, General Specification For
ARP4386	Terminology and Definitions for Aerospace Fluid Power, Actuation and Control Technologies
ARP4493	Aerospace - Direct Drive Servovalves
ARP4761	Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
AS5440	Hydraulic Systems, Military Aircraft, Design and Installation, Requirements For
AS7997	Motor, Aircraft Hydraulic, Constant Displacement, General Specification For
AS8775	Hydraulic System Components, Aircraft and Missiles, General Specification For
AS15002	Fitting, Lubrication, Hydraulic, Surface Check, Straight Threads, Steel, Type II
AS35411	Fittings, Lubrication
AS50881	Wiring Aerospace Vehicle
AS94900	Aerospace - Flight Control Systems - Design, Installation and Test of Piloted Military Aircraft, General Specification For

2.1.2 ASME Publications

Available from American Society of Mechanical Engineers, 22 Law Drive, P.O. Box 2900, Fairfield, NJ 07007-2900, Tel: 973-882-1170, www.asme.org.

2.1.3 ASTM Publications

Available from ASTM International, 100 Barr Harbor Drive, P.O. Box C700, West Conshohocken, PA 19428-2959, Tel: 610-832-9585, www.astm.org.

ASTM F 2395 - 07 Standard Terminology for Unmanned Aircraft Systems

ASTM F 2501- 06 Standard Practices for Unmanned Aircraft System Airworthiness

2.1.4 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

Advisory Circular 120-29 Criteria for Approving Category I and Category II Weather Minima for Approach

2.1.5 IEEE Publications

Available from Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854-1331, Tel: 732-981-0060, www.ieee.org or <http://www.ieee.org/web/publications/home/index.html>.

IEEE 1394.3-2003 IEEE Standard for a High Performance Serial Bus Peer-to-Peer Data Transport Protocol (PPDT)

2.1.6 ISO Publications

Available from American National Standards Institute, 25 West 43rd Street, New York, NY 10036-8002, Tel: 212-642-4900, www.ansi.org or <http://webstore.ansi.org/ansidocstore/>.

ISO/IEC 12207 Systems and software engineering - Software life cycle processes

ISO 22072 Aerospace - Electrohydrostatic actuator (EHA) - Characteristics to be defined in procurement specifications

2.1.7 ICAO Publications

Available from the International Civil Aviation Organization, Document Sales Unit, 999 University Street, Montreal, Quebec H3C 5H7 Canada, Tel: +1-514-954-8022, <http://icaodsu.openface.ca/mainpage.ch2>.

Annex 11 to the Convention on International Civil Aviation, 'Air Traffic Services'

2.1.8 NAS Publications

Available from Aerospace Industries Association, 1000 Wilson Boulevard, Suite 1700, Arlington, VA 22209-3928, Tel: 703-358-1000, www.aia-aerospace.org.

NAS 516 Fitting, Lubrication - 1/8 Inch Drive, Flush Type

NASM15981 Fasteners, Externally Threaded, Self-Locking Design And Usage Limitations For

NASM24665 Pin, Cotter (Split)

NASM33540 Safety Wiring And Cotter Pinning

NASM33588 Nut, Self-Locking, Aircraft, Reliability and Maintainability Usage Requirements For

NASM33602 Bolts, Self-Retaining, Aircraft Reliability and Maintainability, Design and Usage Requirement for

2.1.9 RTCA Publications

Available from RTCA, Inc., 1150 18th Street, NW, Suite 910, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

DO-178 Software Considerations in Airborne Systems and Equipment Certification

DO-254 Design Assurance Guidance for Airborne Electronic Hardware

DO-304 Guidance Material & Considerations for Unmanned Aircraft Systems

2.1.10 U.S. Government Publications

Available from the Document Automation and Production Service (DAPS), Building 4/D, 700 Robbins Avenue, Philadelphia, PA 19111-5094, Tel: 215-697-6257, <https://assist.daps.dla.mil/quicksearch/>.

Specifications

MIL-A-8860 Airplane Strength and Rigidity, General Specification

MIL-A-8861 Airplane Strength and Rigidity, Flight Loads

MIL-A-8865 Airplane Strength and Rigidity, Miscellaneous Loads

MIL-A-8867 Airplane Strength and Rigidity, Ground Tests

MIL-A-8870 Airplane Strength and Rigidity, Divergence, and Other Aeroelastic Instabilities

MIL-A-87229 Auxiliary Power Systems, Airborne

MIL-C-18244 Control and Stabilization Systems: Automatic, Piloted Aircraft, General Specification for

MIL-DTL-781 Terminal, Wire Rope Swaging, General Specification for

MIL-DTL-6193 Joints, Universal, Plain, Light and Heavy Duty, General Specification for

MIL-I-8500 Interchangeability and Replacementability of Component Parts

MIL-PRF-5503 Actuators: Aeronautical Linear Utility, Hydraulic, General Specification for

MIL-PRF-7958 Push-Pull Controls, Flexible and Rigid

MIL-S-8512 Support Equipment, Aeronautical, Special, General Specification for the Design of

Standards

MIL-STD-130	Identification Marking of US Military Property
MIL-STD-202	Test Method Standard, Electronic and Electrical Component Parts
MIL-STD-461	Electromagnetic Interference Characteristics
MIL-STD-464	Electromagnetic Environmental Effects Requirements for Systems
MIL-STD-704	Aircraft Electric Power Characteristics
MIL-STD-810	Environmental Engineering Considerations and Laboratory Tests
MIL-STD-882	Standard Practice for System Safety
MIL-STD-1472	Human Engineering Design Criteria for Military Systems, Equipment and Facilities
MIL-STD-1553	Digital Time Division Command/Response Multiplex Data Bus
MIL-STD-1773	Fiber Optics Mechanization of an Aircraft Internal Time Division Command/Response Multiplex Data Bus
MIL-STD-1797	Flying Qualities of Piloted Aircraft
MIL-STD-7080	Selection and Installation of Aircraft Electric Equipment

Military Handbooks

MIL-HDBK-336	Survivability, Aircraft, Nonnuclear
MIL-HDBK-454	General Guidelines for Electronic Equipment
MIL-HDBK-470	Designing and Developing Maintainable Products and Systems, Volume I and Volume II
MIL-HDBK-516	Airworthiness Certification Criteria
MIL-HDBK-781	Reliability Test Methods, Plans and Environments for Engineering Development, Qualification and Production
MIL-HDBK-838	Lubrication of Military Equipment

Publications of the Office of the Secretary of Defense (OSD)

FY 2009 - 2034	Unmanned Systems Integrated Roadmap
FY 2011-2036	Unmanned Systems Integrated Roadmap

2.1.10.1 Inactive Specifications and Standards

The requirements of these specifications apply to re-procurements of in-service equipment or of legacy systems, subsystems or components being used in new systems or later model aircraft.

MIL-E-5400	Electronic Equipment, Airborne, General Specification for
MIL-M-7969	Motor, AC, 400 Cycle 115/200 Volt System, Aircraft, General Specification for
MIL-M-8609	Motor, DC, 28 Volt System, Aircraft, General Specification for
MIL-H-8890	Hydraulic Components, Type III (-65 Deg to Plus 450 Deg F) General Specification for (ASG)
MIL-H-8891	Hydraulic Systems, Manned Flight Vehicles, Type III Design, Installation and Data Requirements For, General Specification For
MIL-M-38510	Microcircuits, General Specification For

2.1.10.2 Military Guide Specifications

Available from ASC/ENSI, Building 560, 2530 Loop Rd West, Wright-Patterson AFB OH 45433-7101, Tel: 937-255-6296.

JSSG-2001	DOD Joint Service Specification Guide, Air Vehicle
JSSG-2006	Aircraft Structures
JSSG-2008	DOD Joint Service Specification Guide, Vehicle Control and Management System
AFSC DH 1-2	General Design Factors
AFSC DH 1-4	Electromagnetic Compatibility
AFSC DH 1-5	Environmental Engineering
AFSC DH 1-6	System Safety
AFSC DH 2-1	Airframe

2.1.10.3 Rotorcraft Design Standards

Available from U.S. Army Aeroflightdynamics Directorate (AFDD) Mail Stop 243-11, Moffet Field, CA 94035.

ADS-33E-PRF	Aeronautical Design Standard Performance Specification Handling Qualities Requirements for Military Rotorcraft
-------------	--

2.1.10.4 Related U.S. Government Publications

The following related document is listed for informational purposes only.

MIL-HDBK-2069	Aircraft Survivability
---------------	------------------------

2.2 Abbreviations, Acronyms, Symbols and Their Definitions

A/D	Analog-to-Digital
AC	Alternating Current
ADS-B	Automatic Dependent Surveillance - Broadcast
AEI	All-Engines Inoperative
AFDD	Army Aeroflight Dynamics Directorate
AGL	Above Ground Level
ALS	Automatic Landing System
ANSI	American National Science Institute
AOA	Angle of Attack
ARINC	Aeronautical Radio Inc
ARP	Aerospace Recommended Practice
ASA	American Standards Association
ASG	Aerospace, Specification, General
ATF	Auto Throttle Function
BIT	Built-In-Test
c	Fault Coverage Factor
CBIT	Continuous Built-In-Test
COTS	Commercial Off-The-Shelf
CPCI	Computer Program Configuration Item
CS	Control Station
CSCI	Computer Software Configuration Item
CV/CVN	Aircraft Carrier/Aircraft Carrier Nuclear Propulsion
DAPS	Document Automation and Production Service
DC	Direct Current or District of Columbia
DDV	Direct Drive Valve
DGPS	Differential Global Positioning System
DLC	Direct Lift Control
DMC	Deck Motion Compensation
DSP	Digital Signal Processor
DTED	Digital Terrain Elevation Data
EEPROM	Electrically Erasable Programmable Read Only Memory
EGI	Embedded GPS/INS Unit
EHA	Electrohydrostatic Actuators
EHSV	Electrohydraulic Servovalves
ELT	Emergency Locator Transmitter
EMA	Electromechanical Actuator
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EO/IR	Electro-Optical/Infra-Red
ESS	Environmental Stress Screening
FAA	Federal Aviation Administration
FAR	Federal Agency Regulation
FBW	Fly-By-Wire
FCT	Fracture Critical Traceable
f_M	Open Loop Crossover Frequency
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis
FPGA	Field Programmable Gate Array
FTA	Fault Tree Analysis
FTE	Flight Technical Error
FY	Fiscal Year
GCAS	Automatic Ground Collision Avoidance System
GM	Gain Margin
GPS	Global Positioning System
GPWS	Ground Proximity Warning System

h/hc	Ratio of Altitude to Altitude Command
Hc/Ze	Ratio Altitude Command to Altitude Error
H-DOT	Vertical Rate
HSTA	Horizontal Stabilizer Trim Actuator
IAP	Integrated Actuation Package
IBIT	Initiated Built-in Test
ICAO	International Civil Aviation Organization
ICD	Interface Control Document
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IFF	Identification, Friend or Foe
IFPC	Integrated Flight and Propulsion Control
ILS	Instrument Landing System
IMU	Inertial Measurement Unit
INS	Inertial Navigation System
IR	Infra-Red
ISO	International Organization for Standardization
JPALS	Joint Precision Approach and Landing System
JSSG	Joint Service Specification Guide
JUAS COE	Joint Unmanned Aircraft System Center of Excellence
KCAS	Knots Calibrated Airspeed
KIAS	Knots Indicated Airspeed
LAL	Lateral Alert Limit
LOA	Levels of Autonomy
LOC	Loss of Command and Control Data, identifying an event or a VMS state
LRU	Line Replaceable Unit
LSO	Landing Signal Officer
LVDT	Linear Variable Differential Transformer
MBIT	Maintenance Built-In-Test
MMS	Mission Management System
MSL	Mean Sea Level
MTBF	Mean Time Between Failure
MTTR	Mean Time To Repair
N/A	Not Applicable
NA	Not Available
NAVAIDS	Navigational Aids
NDT	Non-Destructive Testing
nm	Nautical Mile
NSE	Navigation System Error
NWS	Nose Wheel Steering
OEI	One-Engine Inoperative
OFP	Operational Flight Program
OSD	Office of the Secretary of Defense
PBIT	Periodic Built-In-Test
PBW	Power-By-Wire
PCS	Propulsion Control System
PDE	Power Drive Electronics
PIO	Pilot Induced Oscillation
PLOA	Probability of Loss Of Aircraft
PLOC	Probability of Loss of Control
PM	Phase Margin
POST	Power-On Self-Test
PROM	Programmable Read-Only Memory
$Q_{M(VMS)}$	Mission Failure Rate due to VMS Failures (per flight hour)
$Q_{S(VMS)}$	Quantitative Flight Safety, Loss of Control Rate, due to VMS Failures (per flight hour)
R	Reliability of a Component
RA	Resolution Advisory
Rs	Reliability of a Subsystem

RBD	Reliability Block Diagram
ROM	Read Only Memory
RTCA	Radio Technical Commission for Aeronautics
RVDT	Rotary Variable Differential Transformer
RVSM	Reduced Vertical Separation Minimum
SAA	Sense and Avoid
SAP	Safety Assessment Plan
SAS	Stability Augmentation System
SDP	Software Development Plan
SMS	Ship Motion Sensor
SOF	Safety-of-Flight
SRA	Shop Replaceable Assembly
STOL	Short Take-Off and Landing
TA	Traffic Advisory
TACAN	Tactical Air Navigation
TCAS	Traffic Collision Avoidance System
TOW	Take-Off Weight
TSE	Total System Error
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UCS	Utility Control System
V/STOL	Vertical and/or Short Take-off and Landing
VAL	Vertical Alert Limit
VG	Turbulence Penetration Airspeed
VHF	Very High Frequency
VL	Maximum Limit Speed
VMC	Vehicle Management Computer
VMS	Vehicle Management System
V _{OMAX}	Maximum Operational Airspeed
V _{OMIN}	Minimum Operational Airspeed
VOR	VHF Omni-directional Range
VSTOL	Vertical and Short Takeoff and Landing
VTOL	Vertical Takeoff and Landing
WAAS	Wide Area Augmentation System
WOW	Weight-On-Wheels
WRA	Weapon Replaceable Assembly

2.3 Definitions

2.3.1 UA Design and Operational Categorization Schemes

2.3.1.1 Types of VMS, Categories of UA and UA Operating Area

VMS TYPE: The performance capability of a UA VMS, related to its behavior following VMS failures of differing probability. The level of this capability will be specified by the procuring activity and identified as VMS Types T0 through T4. The minimum acceptable behavior for each of these Types is specified in 3.1.1.4.1, in terms of their Operational State, defined in 2.3.3, following failure. A method for the determination of the Type applicable to each UA procurement is also suggested in 3.1.1.4.2.

UA CATEGORY: The UA Category is typically defined by its weight and performance capability and assigned by the procuring activity. VMS Types are mapped to the appropriate UA Category in 3.1.1.4.2. At the time of writing, competing categorizing schemes exist and no single standard has been generally adopted. For the purpose of this document the schemes of Table 1, as defined by the Joint Unmanned Aircraft System Center of Excellence (JUAS COE) and recorded in Figure A.4. of the OSD FY 2009-2034 Unmanned Systems Integrated Roadmap and, in more graphic form, in Figure 1 of the Unmanned Systems Integrated Roadmap FY2011-2036, has been assumed.

NOTE: The Roadmap figures define categories for complete Unmanned Aircraft Systems, though distinguished by the characteristics of the UA, the airborne element of the UAS. This ARP applies the same Category to the UA element alone.

TABLE 1 - UNMANNED AIRCRAFT CATEGORIES

UAS Category	UA Attributes			
	Maximum Gross Takeoff Weight (lb)	Normal Operating Altitude (ft)	Speed (KIAS)	Current/Future Representative UAS
Group 1	0 - 20	< 1 200 AGL	100 knots	WASP III, TACMAV RQ-14A/B, BUSTER, BATCAM, RQ-11B/C (Raven), FPASS, RQ-16A, Pointer, Aqua/Terra Puma
Group 2	21 - 55	< 3 500 AGL	< 250 knots	Vehicle Craft Unmanned Aircraft System, ScanEagle, Silver Fox, Aerosonde
Group 3	55 - 1320	< 18 000 MSL		RQ-7B (Shadow), RQ-15, RQ-21A, XPV-1, XPV-2
Group 4	> 1320		Any Airspeed	MQ-5B, MQ-8B*, MQ-1A/B/C, A-160*
Group 5		> 18 000 MSL		MQ-9A, RQ-4, RQ-4N, MQ-4C, Global Observer, X-47B

Footnotes:

1. 1 lb = 0.453 kg
2. 1 ft = 0.304 9 m
3. 1 knot = 1 852 km/h

NOTE: The two UA identified in this DoD chart with an asterisk (*) are rotary wing aircraft. All others listed in-service vehicles are fixed-wing aircraft.

Operating altitude measured Above Ground Level (AGL) or above Mean Sea Level (MSL)

UA OPERATING AREA: The area in which the UA is designed to operate. The UA Operating Area is related to its potential for injury or death to non-combatant personnel, damage to property or environment and is a primary consideration affecting the choice of VMS Type. Operating Area levels A1 through A4 are defined in 3.1.1.4.2.

AIRSPACE: The portion of the atmosphere controlled by a country above its territory, including its territorial waters. More generally, any specific three-dimensional portion of the atmosphere. For the purposes of this document the terms non-segregated and segregated airspace refer to airspace in which simultaneous operation of UA and manned aircraft is allowed or prohibited, respectively.

CLASSES OF AIRSPACE: The ICAO subdivisions of airspace into seven classes from Class A through Class G, see Annex 11, "Air Traffic Services", to the Convention on International Civil Aviation. Generally, increasing degrees of ATC control are required with increasing alphabet position. Mostly adopted world-wide though many countries use only a subset and apply some modifications.

RESTRICTED AREA: An area into which entry is prohibited without special clearance. Typically used for military sensitive zones such as test firing ranges.

WARNING AREA: An area similar to a Restricted area, requiring special clearance for entry, but over international waters.

EXCLUSION ZONE: A predefined geographical area or demarcation that the UAS should never penetrate or cross regardless of any on-board or GCS generated commands. To the best of its abilities, the UAS should also attempt to steer clear of exclusion zones while in degraded Operational States.

2.3.1.2 Flight Phase Categories

For the purpose of this document, the flight profile of the aircraft is separated into categories A, B, and C as follows. When no flight phase is stated in a recommended requirement, that requirement is recommended for all three Phase Categories.

Category A: Non-terminal Flight Phases that require rapid maneuvering, precision tracking, or precise flight-path control.

Category B: Non-terminal Flight Phases that are normally accomplished using gradual maneuvers without precise tracking, although accurate flight-path control may be required.

Category C: Terminal Flight Phases that are normally accomplished using gradual maneuvers and usually require accurate flight-path control. This may include ground handling as required, for example precision taxi on a ship flight deck.

2.3.1.3 Modes of Operation, Human Operator and Flight Characteristics

MANUAL: Those modes of operation wherein the operator provides, in at least one phase of flight, direct and continuous control of the UA, acting as an element of the UA control inner loop by directly manipulating control force effectors and engine power setting and employing visual cues, video feedback or other sensory feedback, in combination or individually. The onboard UA control system may still be augmenting stability but the trajectory of the vehicle is completely dependent upon continuous control inputs from the operator.

ASSISTED: Those modes of operation wherein the operator periodically adjusts UA outer loop controlled states such as airspeed, altitude, heading, climb/descent rate, etc., and determines or adjusts the waypoints the vehicle should fly to. In the absence of new inputs, the UA control system maintains the last controlled states.

AUTONOMOUS: Those modes of operation wherein the UA executes a pre-planned mission and the operator plays no part in the UA control outer loop but may provide decision-making, supervisory or initiation and termination inputs. In this mode of operation, the UA may also generate waypoints independently of the mission plan or otherwise alter trajectory autonomously based on decisions made aboard the vehicle.

NOTE: At the time of writing, competing schemes exist defining Levels of Autonomy (LOA) and no single standard has been generally adopted. The higher levels of mission autonomy, when defined and employed are not expected to require levels of VMS capability beyond those presently defined by this recommended practice.

OPERATOR: The human being responsible for controlling, directing or supervising the operation of the UA from a remote CS. The operator is responsible for the safe, orderly flight of one or more UA, as related to this physical control capability. The operator is often trained and identified by a government agency as a pilot. In the civil field the term is often used for the organization responsible for the UA but it is never used in this manner in this document. The term Operator is analogous to the term Pilot in Command, for a manned aircraft.

UA FLIGHT CHARACTERISTICS: Those flying characteristics necessary for a vehicle in Autonomous or Assisted modes of operation to complete its required mission tasks safely. Flight characteristics requirements would be defined by the procuring activity and derived from the vehicle:

Category, see 2.3.1.1

Operational mission requirements

Flight envelope and intended airspace operating environment

Relevant performance requirements of this document

Relevant sections of JSSG-2001 and MIL-STD-1797 for fixed wing aircraft or ADS-33E-PRF for rotorcraft

The applicable atmospheric disturbances defined in JSSG-2001, MIL-STD-1797 and ADS-33

Three levels of UA flight characteristics are defined. The levels are as follows:

Level 1: Flight characteristics clearly adequate for the mission flight phase.

Level 2: Flight characteristics adequate to accomplish the mission flight phase, but some degradation in mission effectiveness exists.

Level 3: Flight characteristics such that the aircraft can be controlled safely, but mission effectiveness is inadequate. Category A flight phases can be terminated safely, and Category B and C flight phases can be completed.

2.3.1.3.1 Out-of-Scope Flight Characteristics

UAS HANDLING CHARACTERISTICS: Defined, for the purposes of this document, to be those flight characteristics necessary for the mission effectiveness of a UAS configuration by an operator located at a CS. The inputs may be augmented, for stability or control enhancement, and they can directly alter the vehicle flight path in real time or near-real time. These requirements would also be specified by the procuring activity and derived by the “tailoring” of the requirements of JSSG-2001, MIL-STD-1797 and ADS-33.

NOTE: The ability of the UAS to perform its mission, including the UA stability required for acceptable payload sensor performance, is determined by the complex interaction of the UA flight characteristics, the CS software, hardware and flight displays and the communication time delays and latencies. UAS Handling characteristics are beyond the scope of this document.

2.3.1.4 Flight Envelopes

For the purpose of this specification, the flight envelopes are defined as follows:

Operational Flight Envelopes: The Operational Flight Envelopes define the boundaries in terms of speed, altitude, and normal acceleration within which the aircraft must be capable of operating in order to accomplish the required missions. Envelopes for each applicable Flight Phase are defined by the prime contractor in the UAS Detail Specification.

Service Flight Envelopes: For each Aircraft Normal State, the prime contractor defines, in the Aircraft Detail Specification, Service Flight Envelopes showing the combinations of speed, altitude, and normal acceleration derived from aircraft limits, as distinguished from the mission requirements. For each applicable Flight Phase and Aircraft Normal State, the boundaries of the Service Flight Envelopes can be coincident with or lie outside the corresponding Operational Flight Envelopes, but in no case do they fall inside those Operational Boundaries.

Permissible Flight Envelope: The prime contractor defines Permissible Flight Envelopes, which encompass all regions in which operation of the aircraft is both allowed and possible. These envelopes define boundaries in terms of speed, altitude, and normal acceleration. From all points in the permissible flight envelope, it should be possible to return to the service flight envelope without exceptional control system capability.

2.3.1.5 UA Control Systems and Functions

The functional architecture for the control systems of the typical UA assumed for the purposes of this document is shown in Tabular form in Figure 1. The hierarchical form of this structure is explained through the following definitions:

- a. **MISSION MANAGEMENT SYSTEM (MMS):** The top level system that controls the mission related subsystems such as; data link communication, mission payload control, weapon control, Sense and Avoid systems, and the mission task manager, to provide waypoint sequencing or generation per the specified level of autonomy. The MMS may reside in separate computer hardware or may be a software partition within the VMS.
 1. Functionally the MMS accepts guidance and navigation information from the VMS and provides commands to the lower level control systems defined in this section.
 2. The interface with the VMS will require comprehensive MMS failure detection and isolation to ensure flight safety, particularly if the MMS is not as redundant as the VMC or if the MMS is using non-redundant sensor inputs for decision making.
 3. The MMS requirements will be defined by the procuring activity based on the UA Group, size, missions, payload, and intended airspace.
 4. There may not be a clear distinction between MMS and VMS functionality, particularly in failure conditions where the VMS may assume waypoint and path generation responsibility to steer the vehicle away from population centers or exclusion zones.
- b. **VEHICLE MANAGEMENT SYSTEM (VMS):** An integrated combination of functions many of which are critical to safety of flight and which permit an air vehicle to be controlled in a manner that allows its specified missions to be accomplished satisfactorily. For the purposes of this document, the functions included are limited to primary and secondary flight control, though, because of the nature of UA control, these are defined to include the historically separate Guidance and Navigation functions and may include waypath generation and tracking, control of an electrical Environmental Control System (ECS) and hydraulic subsystem management functions required for safe flight operations.

The VMS capability may vary significantly to address unique requirements based on the specific vehicle categories, missions, intended Operating Areas and the overall weapon system specification of the procuring activity. Potential VMS Functional Architectures encompass all of the UA Categories listed in Table 1. Required VMS functions may range from a simple control law hosted in non-redundant hardware for a Group 1 Category 20 lb UA with a T0 VMS, to a complex redundant VMS for an Group 5 Category 15 000+ lb (679+ kg) vehicle with a T4 VMS which may be similar to, or exceed, the complexity of a VMS designed for a high performance manned aircraft.

The VMS design will not be a function of UA Category only; the intended operational use, Operating Area and economics may dictate a higher or lower level of VMS capability. For example, a Group 1 or 2 Category UA intended to provide surveillance capability over densely populated areas will require more fault tolerance and hence redundancy than a T0 VMS will provide, whereas a large UA intended to provide meteorological data over remote oceanic areas, and based away from populated areas and non-segregated airspace may not require the capability of a T4 VMS.

The VMS may implement flight control and actuator control with either “centralized” or “distributed” architectures. Some current Tactical UA employ a centralized, simplex, Commercial Off-The-Shelf (COTS), autopilot system including conventional autopilot functions, Autonomous modes of operation, and Global Positioning System/Inertial Navigation System (GPS/INS) with aided Attitude and Heading Reference System backup for graceful degradation in GPS denied environments.

1. The functional rather than implementation emphasis of this recommended practice is illustrated by the generic functional architecture for the onboard control subsystems of a UA shown in Figure 1. The VMS functions listed in this figure are typical of those required for a T4 VMS. Less capable VMS Types would employ only the functions needed to meet the requirements for the specific UA Category and Operating Area. The VMS commands result in control of aircraft altitude, airspeed, flight path, attitude, aerodynamic or geometric configuration, and take into consideration structural modes. The VMS includes all components used to translate trajectory commands from the MMS or other sources to appropriate flight control force and moment producers. These include the data bus to the MMS, the logic switching, system inertial, GPS and air data sensors, signal computation, test devices, mechanical transmission devices, actuators, power sources, and signal transmission lines dedicated to flight control.
 2. The VMS interfaces with the MMS, which controls mission related subsystems and waypoint sequencing, but the VMS may assume some control of MMS functions in the event of a MMS failure. Such functions may include flight termination or enforcement of pre-defined exclusion zones.
 3. The VMS includes redundancy management, analytical redundancy, mode switching and control system reconfiguration following failures.
 4. The VMS control laws provide the required vehicle stability augmentation, primary and secondary flight control, and automatic or semiautomatic flight path control capabilities such as; Select and or Hold Attitude, Altitude, Airspeed, and Heading including integration with propulsion controllers when necessary. The outer loop control may use inertial and radio navigation sensors (GPS, JPALS, etc.) which are considered components of the VMS for the purposes of this document.
 5. The VMS interfaces with the Utility Control System and Propulsion Control System for both normal control and degraded modes where some flight critical functionality may be assumed by the VMS.
- c. **UTILITY CONTROL SYSTEM (UCS):** This is defined to include all those functions required for ancillary controls such as nosewheel steering, braking, fuel and environmental control, many of which are often included within the VMS. A list of typical Utility and other functions which will interface with the flight control elements and functions of the VMS is provided in Figure 2.
- d. **PROPULSION CONTROL SYSTEM (PCS):** Defined to include all of the functions required for primary, degraded and fail safe control of the engine. These functions are sometimes considered to be part of the VMS and sometimes of the UCS.

Subsystems and Functions	Requirements Defined By:
Mission Management System (MMS)	
Data Link Receiver Modes of Operation – Manual, Assisted, Autonomous Mission Task Execution Payload Management – Weapons Control, Video, Reconnaissance Sensors Flight Termination (for operating MMS case)* Interfaces with VMS, UCS, PCS Health and Status Reporting to the CS	Prime Contractor and Approved by the Procuring Activity
Vehicle Management System (VMS)	
Interfaces with MMS – Normal, Degraded, Fail-Safe – Flight Termination Functions if MMS failed* Redundancy Management and Reconfiguration Flight Control System Functions – Control Laws – Sensors – Stability and Control Augmentation – Integrated Flight and Propulsion Control (IFPC) – Primary and Secondary Control Actuation Outer Loop Control – Sensors incl. IMU/INS, Radar Altimeter and Air Data – NAVAIDS, incl. ILS, JPALS, GPS, and DGPS – Control Laws – Autoflight Guidance and Navigation – Altitude, Attitude, Airspeed, Heading – Autonomous Modes Interfaces with UCS, incl. Mode Control Interface with PCS, incl. Emergency Power and Mode Control	VMS Functions and Requirements Defined in this ARP
Utility Control System (UCS)	
Interface with VMS, incl. Mode Control – Normal, Degraded, Fail-Safe Utility Function Sensors Utility Actuation Control	Prime Contractor and Approved by the Procuring Activity
Propulsion Control System (PCS)	
Interface with MMS & VMS, incl. Mode Control – Normal, Degraded, Fail-Safe Engine Control System Primary Power Systems Secondary Power Systems	Prime Contractor and Approved by the Procuring Activity

FIGURE 1 - UA SYSTEM FUNCTIONAL ARCHITECTURE

*NOTE: This document does not address requirements for, or implementation of, flight termination systems that may be required for test range safety during development flight testing, or for destruction of classified equipment during vehicle losses in operational service.

DGPS is the abbreviation for “Differential Global Positioning System”, ILS for “Instrument Landing System”, “IMU for Inertial Measurement Unit”, JPALS for “Joint Precision Approach and Landing System”, NAVAIDS for “Navigational Aids”

Category	Function
Power Distribution	Electrical Power Hydraulic Power
MMS	Radar Radio Aircraft Communications (TCAS, Transponder, IFF, ELT) Weapon Systems Payloads Test & Health Monitoring ECM/ECCM
UCS	Environmental Control Fire Detection and Suppression OBIGGS/OBOGGS Landing Gear Test and Health Monitoring
PCS	Engine Fuel Propeller/Rotor Test and Health Monitoring
Overhead	Networks, Routers Structures

FIGURE 2 - TYPICAL SYSTEMS INTERFACES WITH VMS FLIGHT CONTROLS

NOTE: ELT is the abbreviation for “Emergency Locator Transmitter”, IFF for “Identification, Friend or Foe”, TCAS for “Traffic Collision Avoidance System”

2.3.2 Flight Control Functional Classifications

The flight control functions provide the means for aircraft control and maneuvering and may include stability augmentation, load limiting and envelope protection and limiting. Flight control may employ, singly or in combination, mechanical, electrical or optical transmission of commands to the actuators that drive effectors that produce force or moments. The actuation power source may be hydraulic, electric, or pneumatic. While the detail hardware, firmware and software design requirements for these different configurations differ widely, the recommended performance requirements for all configurations will be defined in terms of the Category of aircraft and its Operating Area according to 2.3.1.1, Flight Phase per 2.3.1.2, Flying Characteristics per 2.3.1.3, Flight Envelopes according to 2.3.1.4 and for each Operational State per 2.3.3.

2.3.2.1 Primary Flight Control

Primary flight control functions provide control of aircraft trim state (airspeed, altitude, heading, etc.) as well as maneuvering in autonomous flight or in flight remotely controlled by the CS operator. These functions include stability augmentation provided through closed loop feedback of aircraft states as well as command of aircraft response necessary to meet task-oriented maneuvering requirements. Primary flight control may include provisions for load limiting or envelope protection and limiting. Single or multi-axes thrust vectoring for maneuver or trim control may be included in this classification. Continuous primary flight control is essential to aircraft flight safety and acceptable flying qualities. Basic primary flight control would achieve longitudinal, lateral, and directional control by moving elevators, ailerons, spoilers, rudders, and sometimes propulsion/reaction control devices.

2.3.2.2 Secondary Flight Control

Secondary flight control functions provide control of aerodynamic or propulsive configuration changes as necessary for particular flight phases such as takeoff or landing. Control of flaps, slats, trimmable horizontal stabilizer, speedbrakes or airbrakes, wing sweep, spoilers, ground-steering, braking and propulsion-reversing devices may be included. Secondary flight control is essential to satisfactory performance and may be required for flight safety.

2.3.2.3 Outer Loop Control.

In most cases navigation waypoints are predefined in the mission plan, entered/modified by the CS in real-time, or generated internally (Autonomous operation). Generation of suitable trajectories to execute the control between waypoints may be a shared responsibility between the MMS and the VMS. The VMS, however, may need to include pre-programmed strategies for waypoint and trajectory generation, in the event of an MMS functional or hardware failure, in order to meet the minimum Operational State as defined in Table 3.

2.3.3 VMS Operational State Classifications

NOTE: These definitions differ from those used in manned aircraft specifications, particularly Operational State IV, which for a manned aircraft requires sufficient control for descent and immediate emergency landing, but for a UA only requires sufficient control for some amount of influence on the impact location of the vehicle, not a safe emergency landing.

2.3.3.1 Operational State I (Normal Operation)

Operational State I is the normal state of VMS operation providing sufficient performance, safety and reliability to allow the mission tasks and system requirements of the particular UA to be met within the required flight envelope and safe operation in the intended airspace.

2.3.3.2 Operational State II (Restricted Operation)

Operational State II is the state of less than normal VMS operational performance, safety or reliability with no loss of flight critical functions. Any degradation in mission effectiveness and restrictions of flight envelope will not prevent the vehicle from completing a modified mission or from making a degraded landing at the destination of original intent.

2.3.3.3 Operational State III (Minimum Safe Operation)

Operational State III is the state of degraded VMS performance, safety or reliability which permits the vehicle safe termination of the current mission task, maneuver capability limited to cruise, navigation, transition to appropriate Operating Areas and an emergency landing.

2.3.3.4 Operational State IV (Controllable to a Safe Termination or Predetermined Heading)

Operational State IV is the state of degraded VMS operation in which neither continued safe flight nor safe landing of the vehicle is possible; but sufficient control remains to safely terminate flight, see 3.1.1.1, or, as a minimum, acquire and hold a pre-defined heading which minimizes hazards to others on the ground or in the airspace.

2.3.3.5 Operational State V (Loss of Control)

Operational State V is the immediate loss of control VMS state which allows no control of the vehicle impact site or of heading prior to impact.

2.3.4 VMS Criticality Classifications

2.3.4.1 Essential VMS Functions

A function is Essential if loss of the function results in an unsafe condition or inability to maintain VMS Operational State III.

2.3.4.2 Flight Essential VMS Functions

A function is Flight Essential if loss of the function results in an unsafe condition or inability to maintain VMS Operational State IV.

2.3.4.3 Flight Phase Essential VMS Functions

A function is Flight Phase Essential if loss of the function results in an unsafe condition or inability to maintain VMS Operational State III only during specific flight phases.

2.3.4.4 Noncritical VMS Functions

A function is noncritical if loss of the function does not affect flight safety or result in control capability below that required for VMS Operational State III.

2.3.5 VMS Component Structural Classifications

2.3.5.1 Fracture Critical Part

A primary structural or subsystem component that is predominantly designed and limited by fatigue crack initiation and crack growth requirements rather than static requirements, the single failure of which could lead to the loss of the aircraft. These parts generally call for special fracture toughness controls, quality control procedures, Non-Destructive Testing (NDT) practices, and analytic requirements.

2.3.5.2 Fracture Critical Traceable (FCT) Part

A single load path part, the single failure of which would cause the immediate loss of the aircraft. In addition to the requirements for a Fracture Critical part, an FCT part requires serialization and traceability from starting stock to tail number or major subassembly number and reverse.

2.3.6 Document Definitions

2.3.6.1 Aircraft Detail Specification

The detailed specification for the aircraft provided by the procuring activity.

2.3.7 Definitions of Terminology for Precision Ship Board Landing

AIR BOSS: A Naval term used on the flight deck of an aircraft carrier. The Air Boss is in charge of all aircraft operations on the hangar deck, the flight deck and airborne out to 5 nm (9.3 km).

LANDING SIGNAL OFFICER (LSO): A Naval aviator trained to facilitate the safe and expeditious recovery of naval aircraft aboard an aircraft carrier.

NAVIGATION SENSOR ERROR (NSE): The difference between the actual aircraft path and the desired path caused by all sensor errors and computation errors due to things such as granularity and time tag accuracies.

FLIGHT TECHNICAL ERROR (FTE): The difference between the actual aircraft path and the desired path caused by air turbulence and ship motion including the effect of the gain and phase inaccuracies of the ship motion compensation filters. FTE represents the ability of the aircraft to follow the commanded path.

PATH DEFINITION ERROR: Includes any other error sources besides the NSE and FTE errors defined above, such as errors in the surveyed locations of the GPS Antennas, Airborne INS, Ship Motion Sensor and Touchdown Point. It also includes the effects of structural flexure in either the ship or UA.

TOTAL SYSTEM ERROR (TSE): The sum of the NSE, the FTE and the Path Definition Error, all as defined in this paragraph.

2.3.8 Safety and Operability Terminology Definitions

LOSS OF CONTROL: A failure effect, the result of a single failure or multiple failures, which prevents continued flight and also prevents safe flight termination.

SAFE FLIGHT TERMINATION: Termination without harm to others on the ground or in the airspace. The form it takes is therefore dependent on the hazard potential of the vehicle, as determined by its size, category and design mission. For high hazard vehicles safe termination would demand a controlled crash at a predetermined location or outside predetermined unsafe or undesirable exclusion zones. Safe termination for lower hazard vehicles could be an uncontrolled crash along a predetermined heading. For the lightest and slowest vehicles it could be an immediate uncontrolled crash.

PROBABILITY OF LOSS OF CONTROL (PLOC): The probability of all of those single and combined failures that would cause loss of control, that is, the inability to achieve safe flight termination. Conventionally specified by the procuring activity for the entire aircraft, including all of its systems, the allocation to the VMS is made by the procuring activity or the prime contractor.

VMS PLOC: The allocated probability of the sum of all of those VMS failure conditions, for all of the elements defined in 3.1.1.2 that would cause loss of control.

VMS CRITICAL FAILURE: A failure which causes loss of VMS function and thereby contributes to the VMS PLOC.

2.3.9 Definitions of Modal and Other Auxiliaries

The following definitions apply to the usages in this ARP only.

SHALL: Denotes requirements that must be met. From SAE 2008 Style Manual - "'Shall' is to be used wherever the criterion for conformance with the specific recommendation requires that there be no deviation."

SHOULD: Denotes requirements that are desired to be met. From SAE 2008 Style Manual - "'Should' is to be used wherever noncompliance with the specific recommendation is permissible." The ARP provides many guidance statements employing this word.

WILL: Employed by this ARP in the descriptions of typical actions to be performed by the procuring activity, or the prime contractor, in the future.

MAY: Used by this ARP in the description of the possible or allowable, for example, recommended courses of action or VMS characteristics.

OR: Used by this ARP for recommendations which may be followed by satisfying any one of a set of listed options.

AND: Used for recommendations which can only be met if all of a set of listed options are satisfied. If they must all be satisfied at the same time the word "simultaneously" is added.

N/A: Used for data or recommendations that are not applicable.

3. RECOMMENDATIONS

If the recommendations of this document are invoked as contractual requirements for a UA program the following rules of precedence apply. The detail requirements for a particular system should be specified in the VMS Specification (see 4.6.2), the Aircraft Detail Specification, the contract, or the purchase order for that system and these take precedence over the recommendations of this document. See 2.1 for the precedence between this document and other documents referenced in 2.1.

The recommended flight controls requirements in this document are applicable to the Autonomous, Assisted and Manual operational modes of operation of the UA. The UA Systems requirements are defined by the procuring activity in the Air Vehicle Systems Specification.

The recommendations of this section, and of section 4, will not all be applicable to all UA. Most of the recommendations would be expected to be applicable to the UA with the highest level of VMS flight control capability, T4, and fewer of the recommendations would be applicable to UA with less VMS flight control capability. These expectations are illustrated by the recommendation applicability guide table in Appendix A. but, in practice, the UA procuring activity would specify the precise requirement applicability.

NOTE: Within this Aerospace Recommended Practice there are many actions recommended by the use of the modal auxiliary “should”. There are also many statements about the customary and appropriate contractual division of responsibility between the “procuring activity” and the “prime contractor” and these are described with present tense verbs.

3.1 General System Recommendations

The VMS should comply with the recommended requirements contained in this document to the degree specified by the procuring activity. The compliance should be in a manner such that the aircraft missions defined by the procuring activity can be performed satisfactorily. The VMS should meet all of the environmental requirements of the Aircraft Detail Specification and those recommended by this document.

3.1.1 Safety and Operability Considerations

3.1.1.1 Definitions

The quantitative flight safety recommended requirements in this standard employ terminology that requires the definitions in 2.3.8.

3.1.1.2 Flight Safety Assessment

The assessment of the quantitative flight safety of an VMS should include calculation of the PLOC and also an assessment of the consequence of a single failure or multiple failures across the Operational Flight Envelope.

The prime contractor should develop a Safety Assessment Plan (SAP) for approval by the procuring activity to address the Hazard, VMS PLOC and failure immunity requirements recommended in 3.1.1.3 and 3.1.1.4. The Fault Tree Analysis (FTA), and Failure Modes and Effects Analysis (FMEA) methods in ARP4761 should be used as a guide. A Reliability Block Diagram (RBD) representation of the end-to-end flight critical VMS functionality should be developed and provided to support the PLOC analysis.

The quantitative flight safety assessment of the VMS should include all flight critical functions, components and subsystems. These should include items such as: mechanical controls, VMS electronic set, including all control Guidance and Navigation sensors and functions, air data and aircraft motion sensors, control effectors, hydraulic system components, electrical power system components, including constant speed drives for generators and hydraulic system pump drive gear boxes. All moment producers integrally controlled by the engine control system, and the engine itself should not be included. For a Short Take-Off and Landing (STOL) or Vertical and/or Short Take-off and Landing (V/STOL) aircraft the approach to be adopted for all of the functions controlled by the engine control system should be agreed between the procuring activity and the prime contractor.

A representative mission to which this requirement applies, including mission duration, is defined by the procuring activity and described in more detail by the prime contractor, to allow the component failure rate calculations. The prime contractor, subject to approval of the procuring activity, should define whether the FTAs and RBDs will be developed for one hour of flight or be developed for the duration of one flight and the end result divided by the flight length in hours. These two approaches will give differing results when combined failures or dormant failures with long exposure times are significant to the end result. If the planned usage of the UAS provides, after a failure, for a time to return to base which is significantly shorter than the mission time, the maximum-return-to-base time should be specified by the procuring activity.

3.1.1.3 Quantitative Flight Safety

The VMS PLOC should not exceed the value specified by the procuring activity, or if otherwise specified, a value numerically equal to, the maximum acceptable aircraft Loss of Control rate due to relevant VMS failures ($Q_{S(VMS)}$). The procuring activity defines the VMS PLOC and the VMS Type requirements (see 3.1.1.4.2), based on mission requirements, Operating Area, and payload considerations. The prime contractor develops the mission system and VMS architectures, fault detection/isolation capability, fault accommodation and reconfiguration concepts to minimize the effects of component failures.

The VMS PLOC requirement should include consideration of the mission time and the time to return to base after a failure before normalizing requirements on a per-hour basis.

If the VMS PLOC is not specified by the procuring activity, the numerical requirements of Table 2 apply. They are recommended for use by the procuring activity as minimum requirements.

If the VMS PLOC requirement is an allocation from a vehicle requirement, and, in the absence of a rational analysis to support allocation from vehicle PLOA to individual subsystems, it is recommended that a value, due to relevant failures of systems and subsystems onboard the aircraft, of between 0.25 and 0.375 of the contractually defined vehicle Probability of Loss of Aircraft (PLOA) be used.

NOTES: 1. The range of allocation recommended in this ARP is a judgment based on traditional allocations and historical data from manned aircraft, modified for the broader definition of UA VMS flight control content employed through this document.

2. For UA with flight safety requirements that dictate VMS Types T3 or T4, the failure probabilities in Table 2 are consistent with the manned aircraft PLOC definition and requirements in AS94900. The PLOC requirements in Table 2 are decremented for UAs with mission requirements or Operating Areas which allow the use of VMS Types T0 through T2.

TABLE 2 - VMS QUANTITATIVE FLIGHT SAFETY REQUIREMENTS

VMS Type	Maximum Aircraft Loss of Control Rate From VMS Failures Per Flight Hour, after accounting for mission length, $Q_{S(VMS)}$
T0	1.0×10^{-3}
T1	1.0×10^{-4}
T2	1.0×10^{-5}
T3	1.0×10^{-6}
T4	1.0×10^{-8}

NOTE: Loss of Control in Table 2 means not only loss of the vehicle but also a total loss of the ability to influence the impact location.

3.1.1.3.1 Effects of Imperfect Fault Detection

PLOC calculations for VMS with multiple redundant channels, typically quadruplex, triplex or dual, should account for imperfect fault detection. The inability to correctly select and isolate the failed channel can strongly diminish the increased VMS reliability provided by the redundancy. The significance of this effect increases with diminished redundancy.

The PLOC calculation for a dual VMS with no independent tie-breaker source; can only consider in-line fault coverage of the dual redundant elements. These dual elements should be considered to have a net reliability equal to

$$R_s = R^2 + 2R(1-R)c$$

where R is the reliability of a single element (typically $e^{-\lambda t}$, where λ is the critical failure rate in failures per flight hour), R_s is the reliability of a subsystem and c is the coverage factor ranging from zero to one. The prime contractor should substantiate any coverage factors above 90% ($c \geq 0.9$).

3.1.1.4 Failure Immunity and Safety

UA differ widely in their size, speed, payload and mode of operation and consequently in their potential for harm to other aircraft and to people on the ground. Those with a potential for harm of the same order as manned aircraft must comply with the requirements of this paragraph. UA with a lower potential for harm may employ a lower level of VMS capability. For these, a lower level of failure immunity and safety may be defined by the procuring activity. See 3.1.1.4.1 for further discussion of levels of VMS capability.

A failure immunity and safety assessment should be made to determine if the fault accommodation features of the system provide a safe reaction to, and recovery from, a single failure or a combination of failures.

The VMS should strive to provide sufficient on-board fault detection capability to determine loss of any flight critical function and report the VMS status to the operator, regardless of the level of redundancy. Typically fault monitors are more effective and less prone to false detections if they are targeted at the VMS component level. For example, it is more effective to determine the health of an actuator with a monitor designed to assess actuator response (position versus command, motor currents, etc.) than to deduce a failure by the departure of the UA from the commanded flight path. This guidance, however, is not meant to exclude system-wide integrity monitors that may employ on-board aerodynamic and propulsion models that assist in fault detection and possibly with control reconfiguration to mitigate the loss of a control effector. Even in non-redundant implementations, such approaches may be appropriate to provide "get home" capability or at least a level of control sufficient to steer clear of population centers or other exclusion zones.

Within the Permissible Flight Envelope, no single failure or combination of failures in the VMS or related subsystems, which is not at least a factor of ten less probable than the VMS PLOC, should result in any of the following effects before the VMS takes effective corrective action:

- a. Flutter, divergence, or other aeroelastic instabilities of the aircraft, or a structural damping coefficient for any critical flutter mode below the fail-safe stability limit of MIL-A-8870.
- b. Uncontrollable motions of the aircraft or uncommanded maneuvers, which exceed limit airframe loads.
- c. Any asymmetric, unsynchronized, unusual operation or lack of operation of flight controls that results in worse than VMS Operational State IV.
- d. Exceedance of the Permissible Flight Envelope or inability to return to the Service Flight Envelope.
- e. VMS failures that could cause total loss of thrust.
- f. Erroneous, false, misleading, or missing aircraft information such as altitude/attitude/angle-of-attack/etc., that could result in either incorrect or no flight control commands to the UA or erroneous situational awareness to operators at the CS.

Generally, the procuring authority will also wish to specify certain failure states to be excluded from or accommodated by the above requirement, regardless of failure probability. For example, failures of turbomachinery are generally excluded from the above requirement although failures of the turbomachinery controls are not. The particular exclusions and inclusions specified will directly impact the hardware architecture adopted.

To accommodate certain failures states, regardless of their probability, the procurement authority should include wording in the Aircraft Detail Specification that requires the aircraft to maintain control for failure cases that might include, for example, complete loss of engine thrust, loss of a primary electrical power system, a single actuator jammed, or loss of GPS signals. In addition, to exclude from accommodation certain other specific failure states, the Aircraft Detail Specification should allow aircraft control to be lost for cases that might include, for example, failures of the hot sections of turbomachinery, tire bursts, birdstrikes, actuator jamming failures, or structural component fractures.

3.1.1.4.1 VMS Type Capability

The behavior of the UA following single or combinational VMS failures of different probabilities is a critical measure of VMS capability. Table 3 defines five levels of capability identified as T0 (see 2.3.1.1), the lowest, through T4, the highest, in terms of the degradation of the Operating State for failure states of different probability. At the higher levels of capability only failure states of very low probability will degrade the Operational State and, conversely, relatively probable failure states will degrade the Operational State of the lower levels of capability.

The level required, or VMS Type should be defined by the procuring activity. It will be dependent on a combination of the UA characteristics, its mission and its operational environment. A method for selecting the appropriate VMS Type is contained in 3.1.1.4.2.

NOTE: Table 3 helps to define the contribution of a VMS to the probability of a mission failure, see 3.1.2.1. It is determined by the total probability of all of the failure conditions, of those VMS elements defined in 3.1.1.2, that would prevent mission completion by causing a degradation to Operational State III or worse.

TABLE 3 - VMS TYPES

VMS Type	T0	T1	T2	T3	T4
For All Failure Conditions of Probability Greater Than or Equal to (for one flight hour)	Minimum Resulting Operational State				
1.0×10^{-3}	V	I	I	I	I
1.0×10^{-4}	N/A	II	II	I	I
1.0×10^{-5}	N/A	IV	III	II	II
1.0×10^{-6}	N/A	V	IV	III	II
1.0×10^{-7}	N/A	N/A	V	IV	III
1.0×10^{-8}	N/A	N/A	N/A	V	IV

3.1.1.4.2 Determination of Required VMS Type

The baseline required VMS Type should follow the general guidance of Table 5, based upon the combination of the UA Category, from Table 1 and its Operating Area, as defined in Table 4.

UA that are required to takeoff or land in a more stringent (higher number) Operating Area must have a VMS Type appropriate for that area or be prepared to accept flight restrictions (launch and recovery headings, speeds and fly-away altitudes) to minimize risks until a less stringent Operating Area is reached.

TABLE 4 - UA OPERATING AREA

Operating Area	Definition of UA Area of Operation
A1	Restricted Areas and Warning Areas under controlled and supervised conditions, or combat zones.
A2	Sparsely populated areas that are within Class G airspace, and/or in Restricted areas or Warning Areas, and/or in a maritime environment, and/or in combat zones.
A3	Densely populated areas, or areas of high aviation traffic density, or areas within Class B, C, D or E airspace.
A4	All classes of airspace including those outside of Restricted/Warning Areas and combat zones.

TABLE 5 - SUGGESTED VMS TYPE BASED UPON UA CATEGORY AND OPERATING AREA

UA Category	Group 1	Group 2	Group 3	Group 4	Group 5
Operating Area	VMS Type				
A1	T0	T1	T2	T3	T4
A2	T0	T1	T2	T3	T4
A3	T1	T3	T4	T4	T4
A4	T3	T3	T4	T4	T4

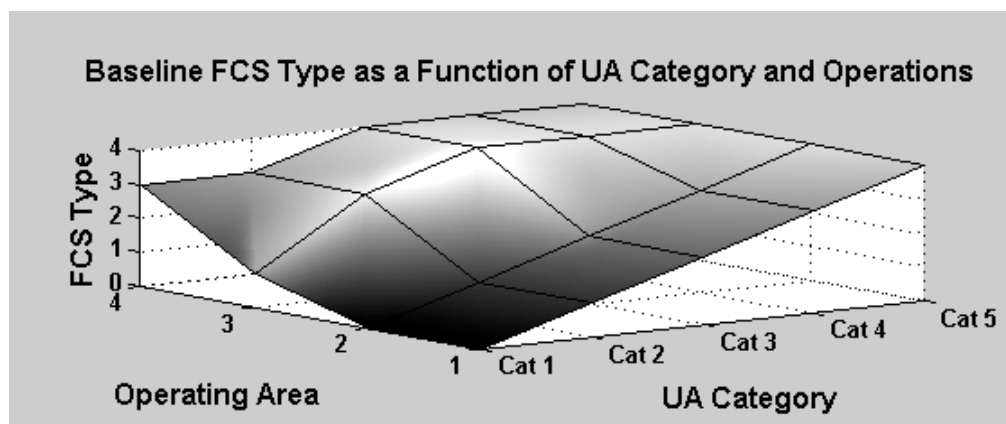


FIGURE 3 - SELECTION OF BASELINE VMS TYPE

In addition, the VMS Baseline Type may be adjusted upward for the following operational factors:

- a. Shipboard operations
- b. Aerial refueling capability
- c. Weapons carriage
- d. Payload security classification
- e. Active structural load control
- f. "Swarming" operations (Multiple UA in the same airspace)

NOTE: All of these factors would tend to increase the required capability, and hence the Type number specified, from the baseline number obtained from Table 5.

3.1.1.5 Transient Electrical Power Effects

VMC, or embedded subsystem computers such as microprocessors, Digital Signal Processors (DSP) or Field Programmable Gate Arrays (FPGA), should tolerate electrical power source variations, within the limits specified for the applicable power system in the Aircraft Detail Specification, without suffering adverse effects which result in operation at below the specified VMS Operational State, or, if not specified, below Operational State III. In the event of primary power source interruption, no adverse effects should result which limit operation or performance of flight control computers upon resumption of normal quality power. The use of independent, uninterruptable backup power for the VMC is strongly encouraged to prevent VMS dropout during momentary primary power interruptions. The hold-up time should be long enough to ensure uninterrupted VMC operation through the worst case transient electrical power system drop-out.

3.1.1.6 Priority

Essential and Flight Phase Essential flight controls should be given priority over noncritical controls and other actuated functions during simultaneous demand operation. However, no specific priority provisions, such as hydraulic priority valves, are required unless there is a likelihood of simultaneous demands which could prevent one or more Essential or Flight Phase Essential actuation systems from meeting their performance requirements. Where provided, priority controls should be highly resistant to deterioration, binding or failure while dormant under normal aircraft operations so that they will function as required when conditions dictate. If flight safety can be endangered by failure of such controls, ground checkout means for ready determination of their operability should be provided and procedures specified.

3.1.2 Reliability Considerations

VMS reliability should be consistent with overall system requirements.

3.1.2.1 Mission Accomplishment Reliability

The probability of mission failure per flight hour, $Q_{M(VMS)}$, due to relevant material failures in the VMS, should be an allocation by the prime contractor from the vehicle requirement provided by the the Aircraft Detail Specification. The allocation should be supported by failure analysis from the Safety Plan, see Note following 3.1.1.4.1.

NOTES: 1. The probability of failure-induced degradation from Operational State II to Operational State III, which would compel mission termination, see 2.3.3, is determined by the selection of VMS Type, see 3.1.1.4.2 and the total number of failure conditions that can cause degradation to Op State III.

- 2. Failures in hydraulic or electrical power sources and power distribution, or other subsystems that do not otherwise cause mission failure should be considered where pertinent.
- 3. Each mission to which this requirement applies should be established and defined by the contractor, subject to approval of the procuring activity.

3.1.2.2 Availability

The VMS availability requirement should be an allocation by the prime contractor from the vehicle requirement provided by the Aircraft Detail Specification. The allocation should be compatible with the Mean Time Between Failure (MTBF) see 3.1.2.3 and Mean Time To Repair (MTTR) specified for the VMS, the VMS mission accomplishment reliability, see 3.1.2.1, and hence the specified VMS Type, see 3.1.1.4.2.

3.1.2.3 MTBF

The VMS reliability, as measured by its MTBF, should meet the requirements of the VMS detail specification and, in combination with the VMS Type fault tolerance, allow the vehicle to achieve the mission reliability and availability specified in 3.1.2.1 and 3.1.2.2, respectively.

3.1.3 Redundancy Considerations

The prime contractor should determine the redundancy approaches to be employed by the VMS and should use the minimum levels required to satisfy the recommendations of this standard.

3.1.3.1 Redundancy

In the design of a redundant VMS, the term redundancy refers to a mechanization which will retain functional integrity after failures, and provide the same or similar flying characteristics and performance capability. In practice, it can take the form of providing duplicate or alternate components, channels, or subsystems, each capable of performing the given function. It can also take the form of analytical redundancy methods used to synthesize sensor data from remaining functional sensors, or control the vehicle through reconfiguration of commands to the remaining functional control effectors. In most cases, elements of both approaches are used, but the analytical redundancy approach requires higher integrity for the computational resources and associated electrical power. The redundancy approach determined by the prime contractor should be:

- a. Based on meeting the flight safety and mission reliability recommendations of this specification.
- b. Consistent with the use of the system test and monitoring provisions recommendations of 3.3.1 and associated subparagraphs.
- c. Based on fault accommodation features that are demonstrated by analysis and simulation to provide a safe reaction to, and recovery from, single failures, including those that are at least a factor of ten less probable than the VMS PLOC.
- d. Addressed in the firmware and software requirements definition when applicable.

3.1.3.1.1 Examples of Redundancy Levels

The differing levels of capability defined in Table 3 for the various VMS Types would be achieved with differing levels of redundancy. Examples of potential configurations with redundancy levels compatible with the Type capabilities are provided in Table 6.

- NOTES: 1. This ARP does not recommend specific architectural approaches. The possible solutions in Table 6 are examples, for illustrative purposes only.
2. These examples are considered to be similar to the architectures conventionally employed to achieve equivalent safety from control functions for manned aircraft. For UA, the different operating environment may allow the exploration of less well established approaches.

TABLE 6 - REDUNDANCY EXAMPLES

VMS Type	Possible Configuration Solution
T0	Single thread system with no analytical redundancy or control reconfiguration features.
T1	Type 0 system but special efforts made to keep processors and power sources alive for some, limited, analytical redundancy. If data link available control station provides vector.
T2	Duplex or very high integrity simplex digital processors and processor power supplies. Actuation simplex but designed for minimal hardover probability. Analytical redundancy and control reconfiguration to aid safe recovery or flight termination.
T3	Triplex or higher control & guidance processing and power sources. Analytical redundancy, control reconfiguration or sensor/actuator physical redundancy used to mitigate failure effects.
T4	Triplex or higher control and guidance processing, sensors and actuator control paths. Redundant actuation and/or split control surfaces with separate actuation. Analytical redundancy and control reconfiguration may be used to further mitigate failure effects.

3.1.3.2 Isolation and Protection of Redundant Subsystems

Redundant subsystems should employ isolation of the redundant elements to preclude failure of one portion of the system from affecting any other part of the system. Recommended requirements for isolation of electrical signal channels are defined in 3.4.5, hydraulic subsystem recommended requirements are in 3.5.3, and mechanical component recommended requirements are defined in 3.6.2.

3.1.3.3 Redundancy Management

The VMS should perform the redundancy management of the components and subsystems within the VMS itself and, where necessary, of those external to the VMS, that are essential to its flight critical functions. Redundancy management should provide failure detection and accommodation sufficient to satisfy the specified mission reliability and safety. Redundancy management should be employed at various levels within the system or channel to perform such tasks as: signal selection, fault isolation, accommodation, and actuator management. Redundancy management should accomplish all of the following, as applicable to the configuration required to achieve the capability requirements of the VMS Type (see Table 3) specified for the air vehicle:

- Provide failure detection, isolation, and accommodation to meet the recommendations of 3.1.1.4 and the transient limits in 3.2.1.10 within the time before divergence to double amplitude.
- Prevent propagation of failures among aircraft control redundant elements.
- Prevent propagation of failures from other systems or subsystems to and from aircraft control redundant elements.
- Provide physical and electrical isolation between redundant elements.
- Provide use of voting and comparison on redundant elements to the maximum extent possible.

- f. Permit re-admittance of previously failed elements back into the voting plane only when operation within tolerance is evident. The system should be able to determine that the transient motions resulting from the reset will fall within the failure transient guidelines in 3.2.1.10 prior to allowing the reset. Operator action is preferred over automatic reset logic (see NOTE).
- g. Provide for an automatic in-flight restart of the VMS to maintain aircraft control, in the event of an all-channel “generic software design or specification error”.
- h. Provide protection against shut down of the last channel remaining (sometimes known as “last man standing” logic).
- i. Voters and signal selectors for logic devices, such as switches or dials, which provide discrete inputs, should default to a fail-safe state when the truth state cannot be positively determined.
- j. Similarly, a set of fail-safe values should be defined for all proportional inputs where feasible, for default use when they cannot be positively identified as valid or are outside the expected input range. Analytical redundancy may be used to provide for continued safe operation in the case of those inputs which do not have a fixed fail-safe value.

NOTE: Permitting re-admittance of a previously failed element can result in undesired consequences when the good signals return to values near the failed signal. For example, in a triplex system a signal, such as pitch rate, which fails to a near zero value may be declared failed when the other, good, pitch rate signals deviate from zero while maneuvering. After the maneuvering has ended the good signals may return to zero while the aircraft is trimmed. If the failed signal is re-admitted after this occurs, it is possible a subsequent identical failure of another pitch rate signal may cause the remaining good signal to be declared failed, by majority vote while maneuvering, as the two failed signals may agree. This is especially problematic in triplex systems, where a 2 (failed) on 1 (good) condition can occur or quad systems, where a 2 (failed) on 2 (good) conditions can occur, both situations which are extremely difficult to isolate. Any re-admittance scheme should err on the conservative side and not allow a reset if the resulting effect cannot be determined.

3.1.4 Maintainability Considerations

VMS design and installation should permit normally assigned maintenance personnel to perform required maintenance safely and easily under all anticipated environmental conditions. Means should be provided to permit the accomplishment within the allocated maintenance budget and personnel skill level of all required organizational and intermediate level maintenance functions including: operational checkouts, system malfunction detection, fault isolation to the Line Replaceable Unit/Weapon Replaceable Assembly (LRU/WRA) level, LRU/WRA removal and replacement, inspection, repair, servicing, and testing. In addition the design should employ provisions to facilitate efficient overhaul and performance testing and evaluation at the depot level.

3.1.4.1 Operational Checkout Provisions

The VMS should be designed with provisions for operation on the ground, without operating the propulsion system, to verify system operation and freedom from failure, including verifying system redundancy and the absence of dormant system failures that would not normally be detected without intrusive operation of the system, to the maximum extent possible. Electric and electronic components should be designed to operate with the electric power generators supplied by standard ground carts. Hydraulic components should be designed to operate with the standard hydraulic ground carts. If it is not feasible or economic for a UA to interface with standard equipment, because of size or other characteristics, non-standard ground equipment may be employed.

3.1.4.2 Malfunction Detection and Fault Isolation Provisions

The VMS should have a malfunction detection probability sufficiently high to support the specified safety and mission reliability requirements. The VMS should also monitor critical performance parameters as required to isolate faults with a probability sufficient to allow the MTTR specified by the procuring activity to be met. These means may include CS displays and built-in-test functions.

3.1.4.3 Accessibility and Serviceability

The VMS components should be designed, located, and provided with easy access so that inspection, rigging, removal, repair, and replacement can be readily accomplished. Suitable provisions for rigging pins, or the equivalent, should be made to facilitate correct rigging of the VMS. In addition, all VMS components should be designed so their removal and replacement can be accomplished without disturbing the rigging insofar as practicable. Special tools required for installation and rigging should be avoided to the maximum extent possible. Any automated rigging features should allow periodic checking of the rigging accuracy achieved. If rig or other system setup information is stored in non-volatile memory within a LRU/WRA, provisions should be made for electronic transfer of this data from redundant LRU/WRAs into an LRU/WRA which has been installed to replace one removed for maintenance.

3.1.4.4 Maintenance Personnel and Safety Provisions

Systems and components should be designed to preclude injury of personnel during the course of all maintenance operations including testing. All devices which contain any type of stored energy (such as mechanical, electrical, hydraulic, or pneumatic), or which can produce energy capable of causing injury to maintenance personnel, should be provided with a positive means of disconnecting the energy source, allowing controlled release of the energy, or preventing its inadvertent release. Where positive protection cannot be provided, precautionary warnings or information should be affixed in the aircraft and to the equipment to indicate the hazard; and appropriate warnings should be included in the application maintenance instructions. Safety pins, jacks, locks, or other devices intended to prevent actuation should be readily accessible and should be highly visible from the ground, or include highly visible streamers. All such streamers should be of a type which cannot be blown out of sight such as up into a cavity in the aircraft. Streamers should be in accordance with MIL-S-8512.

3.1.5 Survivability Requirements

The VMS should withstand and operate in any unnatural, induced, hostile environment specified in the Aircraft Detail Specification. The VMS should provide at least Operational State III performance in all situations where damage sustained by the airframe and other systems would not cause total loss of control. Design options and techniques to enhance the survivability of redundant systems are provided in AIR1083.

3.1.5.1 All-Engines-Out Control

If engine generated power is normally required for VMS operation, supplementary sources of power may be needed to allow continued control for the all-engine-out case, as defined by the procuring activity. Different considerations apply during the Flight Test phase from those applicable to the operational aircraft and the ability or inability to restart the engine in flight is of prime importance.

3.1.5.1.1 Operational Vehicle

Independent supplementary sources of electrical power and, if needed, hydraulic power should be provided as necessary for VMS Types T2 through T4. The prime contractor, with the concurrence of the procuring activity, should establish the minimum time requirement for fill-in VMS electrical power after an engine loss. The design of the VMS, including its power sources, should be such that unintentional loss of any or all engine thrust and engine-generated power does not result in less than VMS Operational State III, including any necessary transition to emergency sources of power, for the duration of this specified time requirement. Provision should be made for in-flight return to normal power wherein the transition should not result in a worse VMS Operational State.

3.1.5.1.2 Flight Test Aircraft

Supplemental power should be provided for flight test vehicles with VMS Types T2 through T4. This requirement should apply at least during the envelope expansion phase, when engines are as yet unproven, airframe aerodynamics and airframe/inlet flow field interactions are not yet adequately verified in flight, or if wind milling power is insufficient to maintain at least Operational State III control capability anywhere in the aircraft Permissible Flight Envelope. This supplementary power should be provided for a minimum run time specified by the procuring activity.

3.1.5.2 Power Capacity

Sufficient electrical, hydraulic, and pneumatic power capacity should be provided in all flight phases and with all corresponding engine speed settings such that the probability of losing the capability to maintain at least VMS Operational State III aircraft performance should be at least a factor of ten less probable than the VMS PLOC, when considering the combined probability of system and component failure and the cumulative exceedance probability of turbulence. Analysis and integration studies of ground and in-flight VMS power requirements should be performed to ensure that the power demands can be met with appropriate margin and, if multiple power systems are used, are appropriately balanced between those systems.

3.1.5.3 Invulnerability Considerations for VMS Design

Degradation in VMS operation due to variations in natural environments, adverse events of nature, induced environments, onboard failure of other systems, maintenance error, operator error or enemy actions should be within the limits specified in the following subparagraphs.

3.1.5.3.1 Invulnerability to Natural Environments

VMS should be designed to withstand the full range of natural environmental extremes established for the particular aircraft or system without permanent degradation of performance below VMS Operational State I, or temporary degradation below VMS Operational State II. Reduction below State I should be experienced only at adverse environmental extremes not normally encountered and should be transient in nature only; and, the function should be recovered as soon as the aircraft has passed through the adverse environment. System component clearances with structure and other components should be adequate to preclude binding or jamming, instability, or out-of-specification operation of any portion of the system due to possible combinations of temperature effects, ice formations, if flight in icing conditions is specified by the Aircraft Detail Specification, loads, deflections, including structural deflections, and buildup of manufacturing tolerances. The environmental requirements are defined in the Aircraft Detail Specification and the recommended test methods and procedures are defined in 4.4.2.1.

3.1.5.3.2 Invulnerability to Lightning Strike and Static Atmospheric Electricity

Types T2 through T4 VMS should maintain Operational State II capability or better when subjected to electric field and lightning discharge except that a temporary, recoverable, more extensive loss of performance to State III is allowable in the event of a direct lightning strike to the aircraft. Structural and VMS bonding should meet the requirements of MIL-STD-464 and follow the guidance of its referenced documents.

3.1.5.3.3 Invulnerability to Induced Environments

VMS should withstand the full range of worst-case induced temperatures and temperature shock, acceleration, vibration, noise, and shock, induced pressures, explosive and corrosive atmospheres, electromagnetic Interferences (EMI) and nuclear environment, projected in missions for the particular aircraft, without permanent degradation or loss of the ability to maintain VMS Operational State II capability. Specific induced environmental conditions should be in accordance with the Aircraft Detail Specification. These induced environments, within structural limits, should not result in temporary degradation below VMS Operational State II capability during the exposure to the environment. Requirements for directed energy and high power microwave weapons, and nuclear radiation including Electromagnetic Pulse (EMP) should be defined by the procuring activity. The VMS should meet the applicable requirements of MIL-STD-464 and MIL-STD-461.

3.1.5.3.4 Invulnerability to Enemy Action

The specific enemy threats, and operational capability after encountering the threats, should be defined by the procuring activity. If the threats are not defined, the Essential and Flight Phase Essential VMS functions for VMS Types T3 and T4 only, including associated structure and power supplies, should withstand at least one direct encounter from the implied threat inherent to the mission defined in the Aircraft Detail Specification, without degradation below Operational State III. The prime contractor should identify the vulnerable areas (see MIL-HDBK-336) associated with the implied threat. MIL-HDBK-2069 and AIR1083 are recommended reference documents for Aircraft Survivability design.

3.1.5.3.5 System Operation and Interface

Whenever a non-critical control or other aircraft system is interfaced with Essential or Flight Phase Essential flight control channels, sufficient separation and isolation should be provided to make the probability of propagated or common mode failures to be at least a factor of ten less probable than the VMS PLOC.

3.1.5.3.6 Signal Path Protection

Where redundant signal or computing paths are provided they should be isolated or separated to meet the invulnerability requirements of 3.1.5.3 and 3.4.5.2.

3.1.5.3.7 Invulnerability to Onboard Failures of Other Systems and Equipment

The VMS should meet its failure state/reliability budget, as allocated within the weapon system, for self-generated failure (within the VMS) and for those VMS failures induced by failures of other interfacing systems within the aircraft (3.1.2.1, 3.1.1). In addition, the VMS design should comply with the following:

- a. For VMS Types T3 and T4 only, Essential and Flight Phase Essential VMS functions should retain capability at Operational State III (minimum safe) or better, after sustaining the following failures:
 1. Failure of the critical engine in a two-engine aircraft.
 2. Failure of the two most critical engines in aircraft having three or more propulsive engines.
 3. Failure of any single equipment item or structural member which, in itself, does not cause degradation below State III. This includes any plausible single failure of any onboard electrical or electronic equipment in any subsystem of the aircraft.
- b. For VMS Types T3 and T4 only, the associated structure and power supplies should be designed so that the probability of failing to maintain VMS Operational State IV, as a result of an engine or other rotor burst, should be at least a factor of ten less probable than the VMS PLOC.
- c. In the event of a detected failure that has no immediate effect, such as loss of required cooling for electrical signal computation, or a series of such failures not shown to be at least a factor of ten less probable than the VMS PLOC, which will unavoidably lead to degraded VMS operation, undegraded operation should be provided for a period of time determined by the prime contractor and approved by the procuring activity.

3.1.5.3.8 Invulnerability to Command Loss

VMS Types T3 and T4 should be designed to ensure that loss of command from the MMS results in a capability no worse than Operational State III, Type T2 should meet State IV and Types T1 and T0 may fail to State V.

3.1.5.3.9 Invulnerability to Maintenance Error

The VMS should be designed so that it is physically impossible to install or connect any component item improperly without one or more overt modifications of the equipment or the aircraft. Provisions for adjusting the VMS on the aircraft, except during initial buildup, major overhaul, software or firmware modification, or rigging during major maintenance activities, should be minimized. LRU/WRAs should be designed to permit making internal adjustments only on the bench. The system should require only a minimum of re-rigging following replacement of LRU/WRAs. In addition, all control linkages and other flight control mechanisms should be designed to minimize the probability of jamming from inadvertent entry of maintenance tools or other material.