

# EVALUATION OF CATEGORY III MLS DESIGNS

Rick Cassell, Kelly R. Markin, Alex E. Smith

## ABSTRACT

This paper evaluates three different implementations of a design architecture for Microwave Landing System (MLS) ground equipment that are intended to achieve United States Federal Aviation Administration (FAA) and International Civil Aviation Organization (ICAO) requirements for Category III landing operations. Each of the designs is evaluated for compliance with Category III continuity of service and integrity requirements. In addition, tradeoffs between the designs and several alternatives are analyzed.

## I. INTRODUCTION

The Microwave Landing System (MLS) is in the process of being implemented worldwide as the new all-weather instrument landing system. It will replace the current Instrument Landing System (ILS). A key aspect of MLS implementation will be its ability to satisfy the requirements for providing guidance to aircraft under low visibility landing conditions when visual guidance is not available to the pilot. The lowest visibility operation is termed Category III. In Category III conditions aircraft guidance depends solely on the landing system. During these operations the safety of the landing system is most critical. Category III ILS equipments have been installed and utilized by aircraft for Category III operations for a number of years. As of this writing there have not been any MLS ground equipments manufactured and certified for Category III operations.

Since the landing system is used in Category III operations as the sole means of guidance, safety is the primary consideration. The safety of the landing system is related to two different terms, continuity of service (COS) and integrity. The COS quantifies the probability of maintaining guidance throughout the critical phase of the landing operation. Integrity quantifies the probability of not transmitting potentially hazardous guidance to the aircraft.

There are several design features that typically are built into landing systems in order to satisfy the integrity and COS requirements. This paper

examines several different implementations of a basic design architecture and evaluates how well each design satisfies the Category III requirements. The requirements against which the designs are analyzed are those developed by the International Civil Aviation Organization (ICAO) [1] and the United States Federal Aviation Administration (FAA) [2]. Included is an analysis of several design tradeoffs and a comparison of the impact on the calculated integrity and COS. The angle equipment (Azimuth and Elevation) only is addressed. However the design concepts are similar and the analysis performed here is equally applicable to the Precision Distance Measuring Equipment (DME/P).

The FAA Category III ground equipment requirements were developed in Wroblewski [3] and Markin [4]. A discussion of design considerations in achieving Category III operational performance is contained in Everett, et al [5]. A detailed analysis of software issues for Category III operations is contained in Houston & Vickers [6]. This paper presents and analyzes specific hardware design approaches.

## II. CATEGORY III REQUIREMENTS

### *Integrity*

Integrity is defined by ICAO [7] as "the probability of not radiating false guidance signals." The ICAO MLS operational requirement [8] for system integrity is that "the probability of a failure, malfunction, or generated environmental effect that will jeopardize flight safety during an approach and landing shall be infinitesimal." The operational requirements are quantified as system requirements in the ICAO technical standards [1] and FAA MLS specification [2], and are summarized in Table 1.

The ICAO requirements, given as classification levels of the ground equipment, allow the government agency to set additional requirements for Category II and III operations.

**Table 1. Integrity Requirements**

ICAO	FAA	Azimuth/Elevation	DME/P
Level 3	Cat II	$1-0.5 \times 10^{-9}$	$1-1 \times 10^{-7}$
Level 4	Cat III	$1-0.5 \times 10^{-9}$	$1-1 \times 10^{-7}$

The method used to specify the integrity requirements given in Table 1 has been used with ILS for many years [7]. The specified value for Cat III Azimuth of  $1-0.5 \times 10^{-9}$  means that the probability of a failure resulting in erroneous or hazardous guidance is  $0.5 \times 10^{-9}$  or 1 in 2,000,000,000. The probability of success (no hazardous guidance) is 1 minus this very small number.

### ***Hazardous Parameters***

Before a system can be designed to meet the above integrity requirements the potentially hazardous parameters must be defined. ICAO defined certain conditions which might constitute a hazard in Cat II and III operations as [1]:

1. An undetected fault causing a significant increase in Path Following Error (PFE) as seen by an approaching aircraft.
2. An undetected error in the minimum glide path, transmitted in basic data word 2.
3. An undetected error in the Time Division Multiplex (TDM) synchronization resulting in function overlap.
4. Loss of power that increases Control Motion Noise to unacceptable limits.

In the analysis that follows only the first two parameters (PFE and Data) are considered hazardous. Reference to undetected errors implies that failure of the monitor is a key consideration. The radiation of hazardous guidance requires both a transmitter failure and a monitor/control failure that disables the monitor detection of the fault or renders the transmitter control inoperative. It is therefore of primary concern that the monitor and control functions are fully operative. In order to verify proper operation of the monitor a technique called monitor verification is used.

### ***Monitor Verification***

The purpose of monitor verification is to detect hidden failures in the monitor system and is accomplished by periodic checks. The two types of periodic checks are End-to-End Integrity Checks and Automatic Integrity Checks.

*End-to-End Integrity Check.* The ideal test to ensure proper operation of the monitor is to intentionally radiate out of tolerance guidance information and to verify that the monitor response is appropriate and the system is shutdown. Such a test verifies correct operation of all of the relevant components in the monitor. However, this type of check can be performed only when the system is not in service and therefore its periodicity is limited. The End-to-End Check is not unique to MLS and is performed today with ILS, in some cases manually, e.g. by changing alignment and observing that the equipment shuts down.

*Automatic Integrity Checks.* The Automatic Integrity Check is an on-line simulation of out of tolerance guidance which is performed continually between MLS TDM function frames during system operation. It is a more limited version of the End-to-End Check as it checks many of the components in the monitor but does not actually cause a system shutdown.

*Continuity of Service.* Continuity of Service is defined by ICAO [7] as “the probability of not losing the radiated guidance signals.” Basically whereas integrity is a measure of the validity of the signal in space, the COS is a measure that the system will continue to radiate during a short time interval. This time interval, sometimes defined as the critical time period, begins at a point in the approach beyond which loss of guidance could result in a hazard. Continuous guidance is required over the time interval when the aircraft is highly dependent on the landing system. The time interval ends when visual guidance is obtained in order to complete the landing operation. A summary of the ICAO and FAA requirements for COS is given in Table 2.

**Table 2. ICAO and FAA COS Requirements**

	<b>Cat.</b>	<b>ICAO</b>	<b>FAA</b>
AZ/EL	II	$1-2 \times 10^{-6}$ (15s)	$1-4.2 \times 10^{-7}$ (15s)
AZ	III	$1-2 \times 10^{-6}$ (30s)	$1-3.3 \times 10^{-7}$ (60s)
EL	III	$1-2 \times 10^{-6}$ (15s)	$1-8.3 \times 10^{-8}$ (15s)
DME/P	II	$1-4 \times 10^{-6}$ (15s)	$1-4.2 \times 10^{-7}$ (15s)
DME/P	III	$1-4 \times 10^{-6}$ (15s)	$1-8.3 \times 10^{-8}$ (15s)

Notes:

- 1) The numbers in parenthesis indicate the critical time periods in seconds.
- 2) Categories II and III are equivalent to Levels 3 and 4 in ICAO terminology.

Consider the ICAO entry for Cat III Azimuth. Annex 10 Requires a probability that the Azimuth will continue to radiate of  $1-2 \times 10^{-6}$ , which equals 0.999998 over a 30 second time interval. This can be defined as the probability of an Azimuth outage of  $2 \times 10^{-6}$  in any 30 second interval, which is equivalent to a Mean Time Between Outages (MTBO) of 4166 hours.

It should be noted that Annex 10 COS requirements are minimum values. The design COS should exceed these by as large a margin as is feasible for the following reasons [1]:

1. The MTBO experienced in an operational environment is often worse than that determined by the design calculations due to the impact of operational factors.
2. ICAO COS objectives are minimum values to be achieved in an operational environment. Any improvement in performance above these values enhances the overall safety of the landing operations.
3. A margin between the COS objective and that achieved is required in order to reduce the chance of falsely rejecting the suitability of an equipment for a particular level of service due to statistical uncertainty.

A comparison of Annex 10 and FAA MTBO requirements leads to the conclusion that the FAA

requirements are significantly more stringent than the ICAO minimum values, e.g., for Cat III Azimuth the FAA requires an MTBO of 50,000 hours, whereas ICAO requires a minimum of 4,000 hours. The reasons [3] for the FAA's choice of MTBO and COS requirements are based on the values specified for FAA ILS equipment. In the 1970s, the FAA specified requirements for CAT III ILS to achieve COS values higher than the ICAO requirements and, in addition, the COS was required over critical time intervals shorter than currently used. The higher COS and shorter time intervals resulted in MTBO requirements on the order of 20 outages per million hours (OPMH). Field data collected from these systems showed that MTBO values significantly higher than the ICAO requirements were achievable, although the achieved values were somewhat lower than the design goals. FAA decided to maintain the more stringent requirement (20 OPMH) for the MLS, with the COS value resulting from the desired critical time interval. The FAA has specified certain design features [2,3] to assist in achieving the higher MTBO requirements, including: redundant transmitters and executive monitors; pre-alarm limits to warn of parameters nearing their tolerance limits; warnings of failure of critical parts of the system, e.g., if the standby transmitter is inoperative, and provision of an uninterruptible power supply.

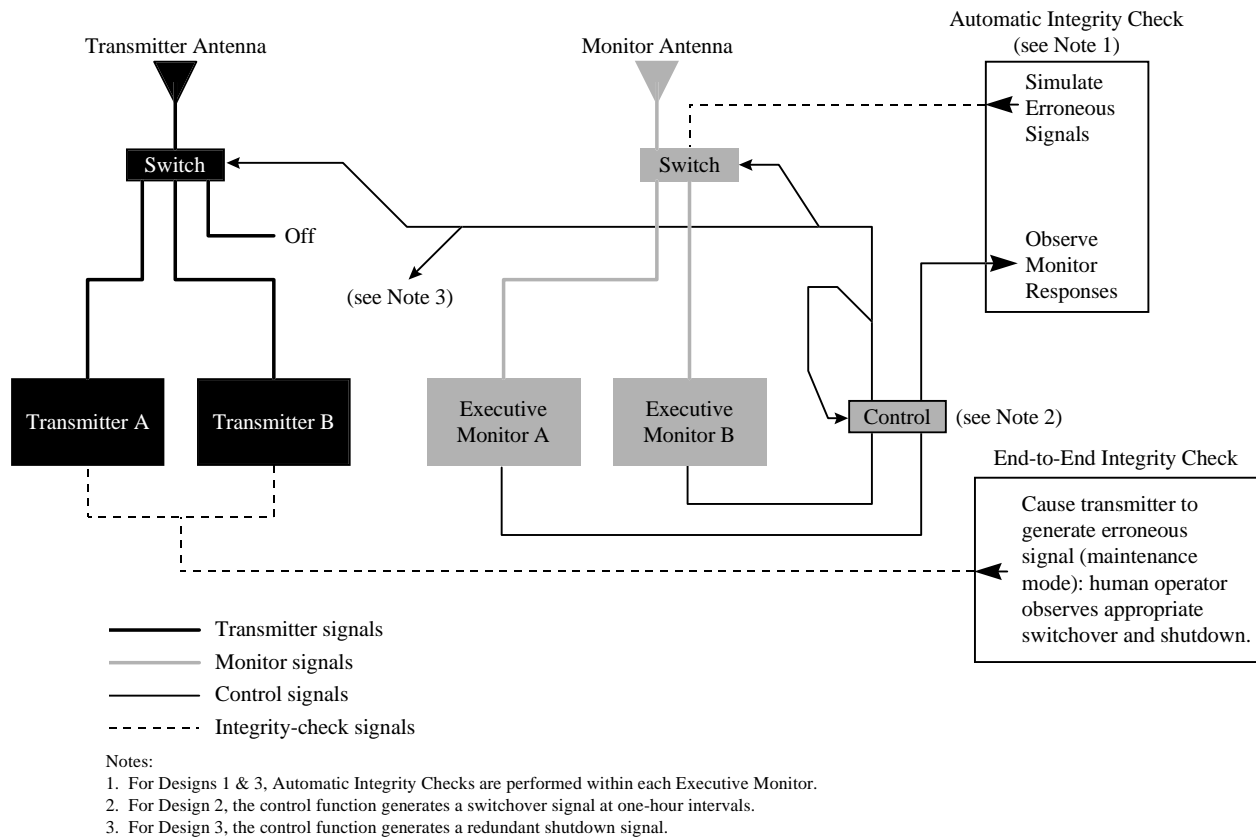
### III. DESCRIPTION OF THREE DESIGNS

Three basic designs are described and evaluated for their ability to meet the Category III COS and integrity requirements. Figure 1 shows the basic design, which consists of redundant transmitters and monitors. Only one of the executive monitors actively monitors the signal in space at any time. When a failure in either the transmitter or executive monitor occurs the control circuit initiates a switchover to the standby transmitter (which is in "hot standby"), and the redundant monitor also becomes active. A second failure causes the control circuit to initiate a complete shutdown. The design uses both Automatic Integrity Checks and End-to-End Checks. The End-to-End Check will cause the primary transmitter to radiate out of tolerance signals which are detected by the monitor, the control circuit will initiate a switchover to the standby transmitter and monitor, verify that they are operating correctly, and then do a complete shutdown. The time between Automatic Integrity Checks is 1 hour. The time between End-to-End Checks is 24 hours. These periodicities were chosen as typical values for Category III MLS equipments.

Design #2 utilizes the same architecture as design #1. The only difference is that the control circuit causes a periodic switchover between the two transmitters and executive monitors. The switchover rate is once per hour. One benefit of this approach is ease of implementation of the Automatic Integrity Checks. For design #1 they must be performed on the active monitor. For design #2 they can be performed on the off-line monitor. The primary benefit, in terms of integrity, is that the switchover circuitry is checked at a rate of once per hour rather than every 24 hours through the End-to-End Check. The End-to-End Check primarily needs to only check a small part of the transmitter switch, basically a few gates, that would cause complete shutdown.

There is also a slight benefit in the COS because any undetected failures in the switchover circuits will be detected within 1 hour rather than up to 24 hours later with the End-to-End Check.

Design #3 is identical to design #1 except for the addition of a redundant shutdown capability. This function is accomplished by incorporating a circuit that will disable the power supplies if the primary shutdown circuit fails. The redundancy improves integrity by reducing the risk of an inability to shutdown when a failure occurs. The added circuitry has a slightly negative effect on the COS.



**Figure 1. CAT III MLS Design Architecture**

The failure rates used in the calculations of integrity and COS are listed in Table 3. The failure rates are based on a sampling of reliability data from several different MLS ground equipment designs. They are consistent with the reliability required by the FAA Category III equipment specification [2].

**IV. EVALUATION OF EXAMPLE DESIGNS**

The three designs described above are now evaluated in terms of their integrity and COS. Since the designs for azimuth and elevation are similar only the azimuth configuration will be evaluated. The critical time period used will be the FAA requirement of 60 seconds. Since the critical time period for azimuth is

30 seconds with the ICAO standard, the computed COS would be better than that calculated here when a comparison is made with the ICAO requirement.

**Table 3. Equipment Failure Rates**

Item	Calculation Values			
	FPMH (1)	Integ (2)	COS (3)	COS (4)
$\lambda_t$	30.0	3.0	30.0	-
$\lambda_{em}$	15.0	1.5	15.0	-
$\lambda_{ts}$	3.0	0.6	3.0	0.6
$\lambda_{ms}$	3.0	0.6	3.0	0.6
$\lambda_{cc}$	0.2	0.04	0.16	0.04
$\lambda_{rs}$	0.5	0.1	0.4	0.1
$\lambda_{at}$	0.5	0.05	0.5	-
$\lambda_g$	0.006	0.006	-	-

Notes:

- 1) Failure rates are given in Failures Per Million Hours (FPMH).
- 2) The integrity computation uses only a fraction of the total failure rate for the transmitter, monitor, and antenna since not all failures will result in potentially hazardous guidance. Additionally, there are two hazardous parameters (PFE and Data) and the risk is assumed to be equally divided between the two.
- 3) This value is used with the Azimuth 60 second critical time interval, for failures that would immediately result in a shutdown.
- 4) This value is used with the time between End-to-End Check or switchover time interval for case #2, for failures that are only observable by switchover or End-to-End Check.

$\lambda_t$  = transmitter

$\lambda_{em}$  = executive monitor

$\lambda_{ts}$  = transmitter switch

$\lambda_{ms}$  = executive monitor switch

$\lambda_{cc}$  = control circuit

$\lambda_{rs}$  = redundant shutdown circuit

$\lambda_{at}$  = antenna failures (phase shifters, power dividers, cables, and DPSK antenna)

$\lambda_g$  = gate in shutdown circuit that is only checked by the End-to-End Check

### Continuity Of Service Calculations

The probability of experiencing no failures over a given time period is:

$$P = e^{-\lambda t} \quad (1)$$

$\lambda$  = failure rate of the component (per hour)  
 $t$  = time interval (hours)

The computation of COS is different for parallel and series equipments. Since a Category III MLS is a combination of parallel and series equipment the overall value is a product of the two.

$$P_c = P_p P_s \quad (2)$$

$P_c$  = COS of the combination of parallel and series components

$P_p$  = COS of the parallel components

$P_s$  = COS of the series components

Calculation of the COS of the parallel components is given by [3]:

$$P_p = P_1 + P_2 - P_1 P_2 \quad (3)$$

$P_1$  = Path #1 (primary equipment)

$P_2$  = Path #2 (secondary equipment)

$$P_p = e^{-\lambda_1 t_1} + e^{-\lambda_2 t_E} - [(e^{-\lambda_1 t_1})(e^{-\lambda_2 t_E})] \quad (4)$$

$t_1$  = Critical time period (60 seconds for Azimuth)

$t_E$  = Time between End-to-End Checks (or time between switchovers for design #2)

$\lambda_1$  = failure rate of path #1

$$= \lambda_t + \lambda_{em}$$

$\lambda_2$  = failure rate of path #2

$$= \lambda_t + \lambda_{em} + \lambda_{tsE} + \lambda_{msE} + \lambda_{ccE}$$

$\lambda_{tsE}$ : Portion of transmitter switch failures

detected only by End-to-End Check (or the time between switchovers for design #2)

$\lambda_{msE}$ : Portion of monitor switch failures detected only by End-to-End Check (or time between switchovers for design #2)

$\lambda_{ccE}$ : Portion of control circuit failures detected only by End-to-End Check (or time between switchovers for design #2)

Calculation of the COS of the series components is given by:

$$P_s = e^{-\lambda_s t_1} \quad (5)$$

$$\begin{aligned} \lambda_s &= \text{Failure rate of series components} \\ &= \lambda_{ts} + \lambda_{ms} + \lambda_{cc} + \lambda_{at} + \lambda_{rs} \end{aligned}$$

Note: The redundant shutdown circuit ( $\lambda_{rs}$ ) is included in the COS calculation for design #3 only.

The results of the continuity of service calculations are given in Table 4.

**Table 4. Continuity of Service Results**

Design	$P_p$ (parallel)	$P_s$ (series)	$P_c$ (total)
#1	$1-8.32 \times 10^{-10}$	$1-1.11 \times 10^{-7}$	$1-1.12 \times 10^{-7}$
#2	$1-3.47 \times 10^{-11}$	$1-1.11 \times 10^{-7}$	$1-1.11 \times 10^{-7}$
#3	$1-8.32 \times 10^{-10}$	$1-1.18 \times 10^{-7}$	$1-1.18 \times 10^{-7}$

### Integrity Calculations

The basic equation for computing integrity is:

$$\text{Integrity} = 1 - R \quad (6)$$

R is the risk of radiating potentially hazardous guidance. Risk is calculated according to the following equation:

$$R = P_t P_{em} \quad (7)$$

$P_t$  = Probability of a transmitter failure

$P_{em}$  = Probability of an executive monitor failure

The equations used in the following analysis were developed using the approach described by Markin

[4]. The calculated value ( $R_{av}$ ) is the average risk over the applicable time interval (e.g. the time between End-to-End Checks). An assumption is made that there are no common failure modes between the transmitter and the monitor. Generally the existence of such failure modes results in significantly higher risk than would be predicted by these equations.

For design #1, the baseline, the risk equation is:

$$R_{av} = 2[1/6(\lambda_t + \lambda_{at})\lambda_{em}t_A^2 + 1/6(\lambda_t + \lambda_{at})(\lambda_{cc} + \lambda_{ts})t_E^2] \quad (8)$$

$t_A$  = Time between Automatic Integrity Checks

$t_E$  = Time between End-to-End Checks

Design #2, Periodic Switchover:

$$R_{av} = 2[1/6(\lambda_t + \lambda_{at})(\lambda_{em} + \lambda_{cc} + \lambda_{ts} - \lambda_g)t_A^2 + 1/6(\lambda_t + \lambda_{at})\lambda_g t_E^2] \quad (9)$$

Design #3, Redundant Shutdown:

$$R_{av} = 2[1/6(\lambda_t + \lambda_{at})\lambda_{em}t_A^2 + 1/12(\lambda_t + \lambda_{at})(\lambda_{cc} + \lambda_{ts})\lambda_{rs}t_E^3] \quad (10)$$

The first term in each equation represents those failure modes protected against by the Automatic Integrity Checks. The second term represents the failure modes protected against by the End-to-End Check. The sum of the two is multiplied by a factor of 2 because there are 2 hazardous parameters that for this evaluation contribute equally to the risk. A summary of the calculated results is contained in Table 5.

**Table 5. Risk Calculation Results**

Design	Automatic Check Term	End-to-End Check Term	$R_{av}$ (total)
#1	$7.63 \times 10^{-13}$	$1.87 \times 10^{-10}$	$3.76 \times 10^{-10}$
#2	$1.08 \times 10^{-12}$	$1.76 \times 10^{-12}$	$5.68 \times 10^{-12}$
#3	$7.63 \times 10^{-13}$	$2.25 \times 10^{-16}$	$1.53 \times 10^{-12}$

Note:

The total risk ( $R_{av}$ ) is obtained by multiplying the sum of the two terms by a factor of 2.

Table 6 contains a summary of the calculated results for the integrity and continuity of service.

**Table 6. Summary of Calculated Integrity and COS**

Design	Integrity	COS
#1	$1-3.76 \times 10^{-10}$	$1-1.12 \times 10^{-7}$
#2	$1-5.68 \times 10^{-12}$	$1-1.11 \times 10^{-7}$
#3	$1-1.53 \times 10^{-12}$	$1-1.18 \times 10^{-7}$

## V. TRADEOFFS AND DESIGN ALTERNATIVES

From the results, designs #2 and #3 offer the best overall performance. Both have significant improvement in integrity over design #1. This is important since design #1 narrowly meets the integrity requirement. In design #3 the improvement was achieved simply by the addition of a redundant shutdown circuit, which reduced the probability of the system being unable to shutdown when erroneous guidance is detected. Design #2 showed improvement through the addition of the periodic switchover mechanism. The periodic switchover reduces the critical time period for undetected failures in the switching mechanisms.

One could anticipate that design #2 would yield better COS over #1 since the switching mechanisms and redundant transmitter are checked at one hour intervals as opposed to 24 hour intervals. The COS of the parallel components is improved by a factor of approximately 20, however in the overall computation the parallel COS contribution was not significant since the series components still dominate the achieved COS. This is true for all three designs, and will generally be true for designs which have a combination of parallel and series components. Design #3 yielded slightly lower COS due to the addition of the redundant shutdown circuit.

There are other ways in which the performance of the designs may be improved. One way is to add redundant transmitter and monitor switches. For design #1 this would give a COS of  $1.10 \times 10^{-8}$ , an

improvement by a factor of 10. This is obtained by eliminating the transmitter and monitor switch failure rates from the series COS calculation given in equation (5). In the other two designs a similar improvement would result. This is important since the COS for all three designs is only slightly better than the FAA required COS. It should also be noted that these calculations were based on a particular set of failure rates for the equipment components. The results will change with different failure rates. In an actual design more detailed and accurate information would be utilized along with a Failure Modes, Effects and Criticality Analysis to determine more accurately the integrity and continuity of service.

## VI. CONCLUSIONS

Three candidate Category III MLS ground equipment designs have been evaluated for their ability to meet integrity and COS requirements. All of the designs meet both the ICAO and the more stringent FAA requirements. In addition, design alternatives were evaluated for their impact on the calculated integrity and COS. One conclusion that can be reached is that the series components dominate the achieved COS. It can also be concluded that relatively small changes in design architecture and implementation can result in large differences in the calculated integrity and COS. This was shown by the improvement in integrity by adding a redundant shutdown circuit and a periodic switchover mechanism. It also appears possible that with the addition of redundant transmitter and executive monitor switches improved COS can be achieved. This is important since it is desirable to have as much margin over the requirements as possible in the calculated values. Analyses such as those presented in this paper are useful in making such comparisons of design alternatives.

## REFERENCES

1. ICAO All Weather Operations Panel (AWOP), Report of the Twelfth Meeting, Montreal, Canada, November 1987.
2. *Microwave Landing System Specification*, U.S. Department of Transportation/Federal Aviation Administration, FAA-E-2721B, Draft, October 1989.
3. Wroblewski, Peter J., *Development of Continuity of Service Requirements for the Microwave Landing System (MLS)*, The MITRE Corporation, MTR-86W243, McLean, VA, September 1987.
4. Markin, Kelly R., *Development of Integrity Requirements for the Microwave Landing System (MLS)*, The MITRE Corporation, MTR-86W242, McLean, VA, August 1988.
5. Everett, Seymour; Markin, Kelly R.; Wroblewski, Peter J., and Zeltser, Melvin, "Design Considerations for Achieving MLS Category III Requirements," *Proceedings of the IEEE*, Volume 77, Number 11, November 1989.
6. Houston, Susan H., and Vickers, Maryann, "Design and Analysis Techniques for MLS Safety Critical Software," in *Proceedings of Canadian Conference on Electrical and Computer Engineering*, Montreal, Canada, September 17-20, 1989.
7. *International Standards, Recommended Practices and Procedures for Air Navigation Services, Aeronautical Telecommunications, Annex 10*, International Civil Aviation Organization, Fourth Edition, April 1985
8. *ICAO MLS Operational Requirements*, Report of the Seventh Air Navigation Conference, Montreal, Canada, April 1972.

For more information on this paper and/or MLS, visit Rannoch Corporation's web site at <http://www.rannoch.com>, or e-mail us at [info@rannoch.com](mailto:info@rannoch.com).