FAA
Advanced Systems Design Service Team, AJW-121

Allocation Report: Remote Tower (RT) Systems for Non-Federal Applications

Version 1.3
16 September 2021

Table of Contents

List of Tables

List of Figures

1 Purpose

The purpose of this document is to provide a rationale and validation of the final continuity and integrity technical requirements presented in the Remote Tower (RT) Systems Minimum Functional and Performance Requirements for Non-Federal Applications, Version 2.0[1]. This document also explains the analysis that was conducted on pilot and controller runway incursion intervention and their success rates as they relate to major severity Operational Safety Assessment (OSA) hazards and the detection and mitigation of potential runway incursions.

2 Remote Tower Background

Initial safety work was completed for the Remote Tower Pilot Program at JYO (Leesburg, VA) Facility. This safety work drove several Safety Risk Management (SRM) documents and created an initial set of Operational Visual Requirements (OVRs). These requirements were drafted and reviewed by FAA SMEs working with the NextGen Remote Towers Pilot Project. The OVRs are considered a living document and will be provided as an appendix to the technical requirements. The JYO evaluations also resulted in identifying ATC responses to RT equipment outages that drove OSA hazards.

In preparation for the OSA Safety Panel the Remote Tower Safety Team performed an initial review of each system function. These functions were allocated as follows: Required Visual Presentation (RVP), Signal Light Gun (SLG), Maintenance Data Terminal (MDT), Ambient Airfield Audio (AAA) and Data Recording Function (DR). Three classifications of failures have been identified to evaluate all hazards: Loss of Function (LoF), Partial Loss of Function (PLoF), and Malfunction (MALF).

3 Remote Tower Operational Safety Assessment (OSA)

The OSA identified and assessed hazards associated with a RT system using only visual sensors (i.e., cameras) at an airport which are used to provide a visual reproduction of the airport environment at a separate location for Air Traffic Control (ATC) purposes. The OSA addressed RT systems that are intended to be used at single runway airports in Class D airspace to provide VFR tower services.

Guidance for the development of the OSA[2] (signed and approved July 2, 2021) was provided by the *ATO Safety Risk Management Guidance for Acquisition Management (SRMGSA, March 2020)* and the *Safety Management System Manual (SMS, April 2019).* This assessment provides safety objectives and requirements that are independent of any particular vendors' RT system design. The OSA does not consider overall safety risk; it is used to assess only a hazard's severity and determine the target level of likelihood required to achieve an acceptable level of safety.

3.1 OSA Results

The OSA Panel met several times from March 2020 to September 2020. There were several working groups convened during the OSA process to help assist with the final OSA Panel. The OSA panel was comprised of various stakeholders, including Subject Matter Experts (SMEs), Pilots, Air Traffic Control,

[1] This version of requirements is limited to single runway airports, under VFR conditions and without radar surveillance. See requirements document for details of scope.

[2] Remote Tower (RT) Systems Operational Safety Assessment (OSA) for Non-Federal Applications, Version 2.7, April 1, 2021.

Engineering, and Safety Experts. See Table 3-1 for a list of the major severity OSA hazards (only the major severity hazards are listed as they were the only ones relevant to this analysis).

Table 3-1 OSA Major Severity Hazards

Hazard ID	Hazard Description	Severity
RVP-LoF-1	Partial or total loss of the capability to detect and identify/observe spatial relationships objects in the area of jurisdiction (i.e., runways, short finals, and base turns).	Major
RVP-MALF-1	Hazardously Misleading Information (HMI) provided to ATCT controller: Presented visual information is not real-time; asynchronous time lag between presentations/displays. The relative spatial relationship between objects on different physical presentations will be incorrect (i.e., asynchronous presentations/displays).	Major
RVP-MALF-2	HMI provided to ATCT controller: Presented visual information is not real-time: consistent time lag in all monitors.	Major
RVP-MALF-3	HMI provided to ATCT controller: Presented visual information is not real-time: presentation of frozen visual information.	Major
MDT-MALF-2	Loss of system integrity during operations due to a malfunction or error during the installation, setup, or checkout process.	Major

4 Remote Tower Hazards Identified for Further Review

In the OSA functional hazard assessment, the OSA did not qualify the impact of any existing barriers or mitigations when determining the hazard severity classifications for the loss of function and malfunctions hazards. One implication of the assigned OSA major hazard severities is that the Design Assurance Levels (DALs) associated with the RVP (Loss of Function and Malfunction) and MDT (Malfunction) would be assigned based on major (e.g., RTCA/DO-278A DAL 3, RTCA/DO-254 Level C).

At the request of FAA management, the Remote Tower Safety Team was directed to review additional data associated with existing barriers and mitigations for major severity hazards. These barriers and mitigations potentially reduce Remote Tower System design assurance and integrity requirements.

4.1 Pilot Working Group Meeting

Based on the request from FAA management to conduct a further review of the OSA results, several additional working group meetings were held. The decision was made to focus the analysis on the hazards identified with the RVP Loss of Function and RVP Malfunction. Since the primary event associated with both of these hazards was a Category B runway incursion, it was decided to conduct an analysis of how RT systems could contribute to a runway incursion as well as mitigate Category B runway incursions.

The working group meetings included pilots, and other SMEs. The analysis included a review of Runway Incursion data and pilot and controller intervention statistics.

5 Data Assessment Review

When selecting what data to analyze, Runway Incursions (RIs) were specifically chosen because they present the ATCS with an unknown situation when (and if) the Remote Tower system malfunctioned (HMI) or failed (LOF) at that time. The assessment targets of opportunity are (for hypothetical RTS operations):

- ATCS loss of capability to intervene during a Category C RI at risk of elevating to a Category B RI
- RT System misleading information resulting in a controller operational incident causing a Category C RI, and at risk of elevating to a Category B RI

RIs are defined as "any occurrence at an aerodrome involving the incorrect presence of an aircraft, vehicle or person on the protected area of a surface designated for the landing and takeoff of aircraft."[3] It was determined one goal of the analysis is to estimate the likelihood of Category C runway incursions becoming Cat B. It was also determined that by definition Cat D runway incursions are not a risk of becoming Cat Bs.

5.1 Data Sources

Two sources of data were used in the assessment. The all-inclusive RI data containing all reported RI events on or near a runway came from the FAA's AJI-3 CEDAR Database. The Airport Operations data was obtained from the Air Traffic Activity System (ATADS)[4] to establish RI rates.

The Runway Incursion Assessment Team, as defined in FAA JO 7050.1, collects information and performed an assessment on each RI event. As part of the assessment, the FAA Runway Incursion Assessment Team provides amplifying information regarding the event which includes items such as the incident type, severity category (see Figure 5-1 below), event code, and weather conditions.

Incident Types as defined in FAA Order 7050.1B include Operational Incidents, Pilot Deviations, and Vehicle/Pedestrian Deviations:

- Operational Incidents are defined as a surface event attributed to ATCT action or inaction.
- Pilot Deviations are defined as a surface event caused by a pilot or other person operating an aircraft under its own power.
- Vehicle/Pedestrian Deviations are defined as a surface event caused by a vehicle driver or pedestrian.

[3] FAA Order 7050.1B, Runway Safety.
[4] www.aspm.faa.gov

Runway Incursion Severity

Available Reaction Time	Evasive of Corrective Action	Environmental Conditions	Speed of Aircraft and/or Vehicle	Proximity of Aircraft and/or Vehicle

Category D	Category C	Category B	Category A	Accident
Incident that meets the definition of runway incursion such as incorrect presence of a single vehicle/person/aircraft on the protected area of a surface designated for the landing and take-off of aircraft but with no immediate safety consequences.	An incident characterized by ample time and/or distance to avoid a collision.	An incident in which separation decreases and there is a significant potential for collision, which may result in a time critical corrective/ evasive response to avoid a collision.	A serious incident in which a collision was narrowly avoided.	An incursion that resulted in a collision

Figure 5-1: Runway Incursion Severity[5]

5.2 Data Filters

The all-inclusive RI data set contains all incursions from all towered airports, airport configurations, and meteorological conditions. The all-inclusive RI data set is more extensive than the intended environment for the Remote Tower installation and therefore needs to be filtered for applicability. It was determined that the applicable data set was airports that do not have ASDE surveillance and operations in VMC (Visual Meteorological Conditions). In all cases, the filters were applied to both the all-inclusive RI data

[5] https://www.faa.gov/airports/runway_safety/resources/runway_incursions/

set and the Airport Operations data set. The following filters were applied for creating the Non-ASDE Airports; VMC Operations data set used in the assessment [6]:

- Instrument Meteorological Conditions (IMC) RIs entries were removed from the all-inclusive RI data, leaving only the Visual Meteorological Conditions (VMC) data. The RI data set does not delineate Instrument Flight Rules (IFR) and Visual Flight Rules (VFR) flights. However, Airport Operations data includes IFR (along with VFR) flights. IFR can be flown in IMC or VMC and the Airport Operations data does not segregate the actual weather conditions.
- Non-ASDE airports: This filter was applied to view the incursions that occurred where airport runway surveillance monitoring is not available. The ASDE airports were removed from both the all-inclusive RI data and the Airport Operations data.
- Airports with Class B airspace were removed from the data sets by consulting airspace charts.[7]
- Dates: The initial AJI-3 CEDAR data set began in October of 2016 and went through the end of 2020. COVID-19 severely affected the aviation industry, so 2020 was removed from some of the data sets, including the set used for further analyses.

5.3 Data Narrative and Categorization

The Runway Incursion Assessment Team created reports and provided a standardized narrative based on the reported event. ATCT personnel submit the runway safety occurrence reports, which is then screened by AJI Quality Assurance. The Runway Incursion Assessment Team (RIAT) determines the runway incursion severity, type of surface event, and identifies factors affecting severity. The report contains the RIAT team's best guess of the root cause of the event. The mitigation success or failure realization is already accounted for in the text of the root causes in the reports. The reports do not:

- Contain assessment regarding whether the mitigations or interventions were successful.
- Estimate if the hazard severity is reduced due to the mitigations or interventions (e.g., A Cat-D RI is recorded as being caused by the controller, but the intervention by the controller or pilot that prevents it from becoming a Cat-C/B/A is not captured).

5.4 Intervention Assessment

The intervention assessment conducted by a subgroup of the Remote Tower Safety Team focused on CAT C (Minor severity) RIs that could potentially lead to CAT B RI events (major severity) as the target of opportunity. Cat C RIs were specifically chosen because there was a reasonably sized data set (1227 Cat C RIs). Cat C RI narratives for the Non-ASDE Airports; VMC Operations data set were analyzed for this paper to determine if interventions were documented. The goal of this was to ascertain if there was something that potentially kept the incident from escalating (from Cat C to Cat B) and if so, what it was, controller intervention, pilot intervention, or geometry/timing (critical system state, see section 7.1).

[6] Data set was provided by ATADS

[7] The Airport Data and Information Portal also provides runway information. It was used to determine airports with only one runway. Due to the lack of RI data for single runway, Class D airports, the decision was made to eliminate the filter for one runway. It was determined that the statistical significance was insufficient to use that data set.

6 Runway Incursion Rates by Category

Table 6-1 lists the number of events and calculated rate (per operation) in the Non-ASDE Airports; VMC Operations data set of the various categories of runway incursions used in the assessment. These represent the "status quo" data used in the fault tree allocations.

Table 6-1 Runway Incursion Data Summary

Runway Incursion Category	# Events	Rate
Category A	9	9.05E-08
Category B	15	1.51E-07
Category C	1227	1.23E-05
Category D	2310	2.32E-05
Category A/B/C/D	3561	3.58E-05

The runway incursion rates were also compared in the various subsets of data, shown in Table 6-2. The various data sets are used to corroborate the reasonableness of the data set used in the assessment and Remote Tower (RT) system allocations (Non-ASDE Airports; VMC Operations). As can be seen, there is very little difference in the runway incursion rates in the four different datasets. That is despite the different airport types, different time periods, and significantly different total number of operations.

Table 6-2 Comparison of Runway Incursion Rates

	All Towered Airorts: VMC Operations		Non-ASDE Airports; VMC Operations		Class D Airports: VMC Operations		ASDE Airports; VMC Operations	
Runway Incursion Categories	# Events	Rate	# Events	Rate	# Events	Rate	# Events	Rate
Category A/B	28	1.95E-07	24	2.41E-07	20	1.82E-07	7	1.24E-07
Category C	1955	1.36E-05	1227	1.23E-05	1090	9.94E-06	977	1.74E-05
Category A/B/C	1983	1.38E-05	1251	1.26E-05	1110	1.01E-05	984	1.75E-05
Category A/B/C/D	4698	3.28E-05	3561	3.58E-05	3333	3.04E-05	1552	2.76E-05
Number of Operations	143,276,561		99,488,810		109,669,232		56,304,157	
Time Period	2017 - 2019		2017 - 2019		Oct 2016 - Sep 2020		Oct 2016 - Dec 2020	

6.1 Causal Event Rates for Runway Incursions

Assessment of the Non-ASDE Airports; VMC Operations data set was done to determine the causal event status quo rates, based on the runway incursion incident types categorized in the data set. The number of events and causal event rate for runway incursion causes leading to Category C runway incursions is shown in Table 6-3.

Table 6-3 Causal Events for Category C Runway Incursions

Runway Incursion Cause	# Events	Rate
Controller Operational Incident	326	3.28E-06
Pilot Deviation	773	7.77E-06
Vehicle/Pedestrian Deviation	128	1.29E-06

7 Fault Trees

7.1 Remote Tower Loss of Function

Figure 7-1 is a generic fault tree for a Category B Runway Incursion Hazard, which includes a Loss of Function event associated with the Remote Tower. The fault tree shows two possible causes leading to a top-level event of a Cat B Runway Incursion. The left side represents the nominal rate of incursions that occur in "fault-free" RT system operations, meaning the RT system is operating normally. This is identified as the Cat B Status Quo branch of the fault tree. It is assumed that the nominal rate of runway incursions with RT systems will be the same as for brick and mortar towers.

On the right-side fault of the tree in Figure 7-1, for the Cat B Runway Incursion Related to RT system Loss of Function event to occur, three independent events are required:

- Cat C Runway Incursion
- Critical System State event
- Intervention Failure

The Nominal Cat C Runway Incursions (identified as the Cat Status Quo branch of the fault tree) is influenced by three events that are treated as independent:

- Pilot Deviation,
- Vehicle Deviation[8]
- Controller Operational Incident

The Critical System state event represents conditions such as relative separation and/or timing that prevent a Cat C runway incursion from becoming a Cat B runway incursion, whether or not there is an intervention. See section 7.2 for derivation of critical system state.

The Intervention Failure event is influenced by the contribution from the Remote Tower Failure (identified as the Remote Tower Allocations branch of the fault tree). For the Intervention Failure event to occur, three independent events are required:

- A Remote Tower Failure event resulting in loss of function.
- A Pilot Intervention Failure event is where a pilot must fail to avoid the hazard by means of see-and-avoid.
- A Controller Intervention Failure event where ATCS must be unable to intervene to avoid the hazard.

[8] The pedestrian numbers are included in the data set, linked with the vehicle deviations

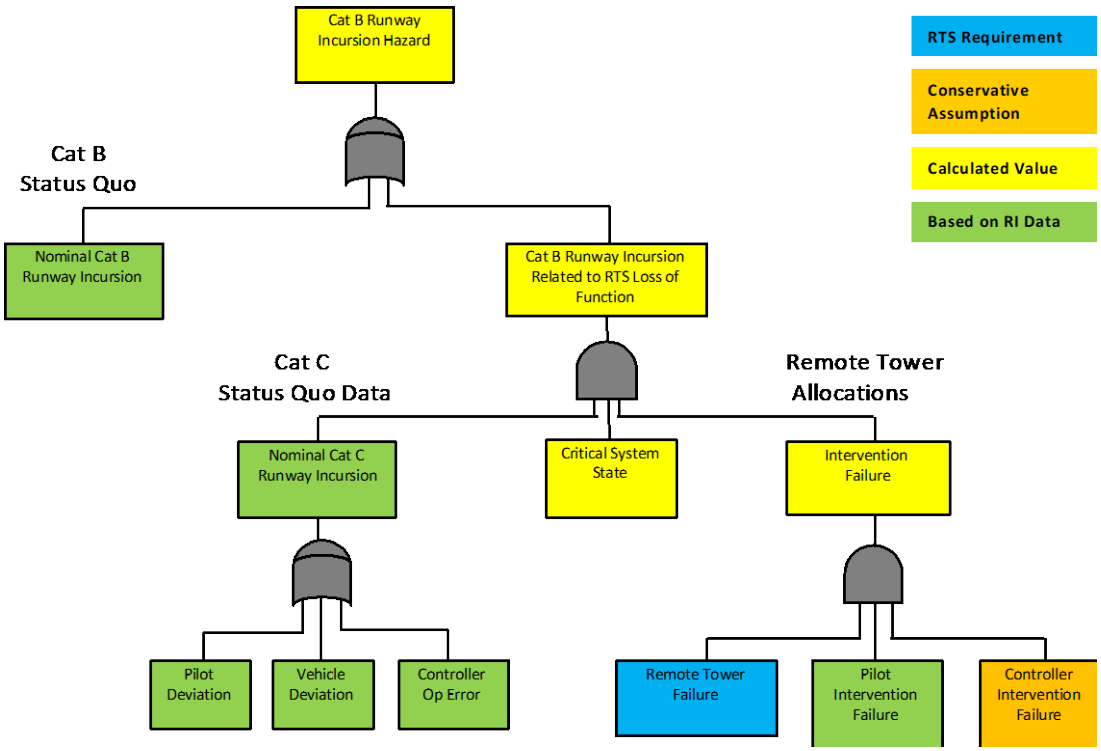

Figure 7-1: Generic Loss of Function Fault Tree

The generic fault tree from Figure 7-1 will now be populated with known or derived quantities to determine an allocation for the Remote Tower Failure event rate. Table 7-1 identifies the values and rationale for the derived quantities, based on the most stringent requirement defined in the SMS for a Cat B RI (10^{-7}). Figure 7-2 shows the results of the Remote Tower Failure event rate in meeting the most stringent requirement.

Table 7-1 RT System LOF Event Rates

Event	Rate	Rationale
Cat B Runway Incursion Related to RT system Loss of Function	$1.0x10^{-7}$	Category B runway incursions are a major hazard severity and therefore, the range of allowable event probabilities is between 10^{-5} and 10^{-7}. The most stringent (conservative) value in the range of probabilities is chosen.
Nominal Cat C Runway Incursions	$1.23x10^{-5}$	Table 6-1 Individual causal event rates
Critical System event rate	0.38	Derivation in Section 7.2
Pilot Intervention Failure	0.86	Derivation in Section 7.2
Controller Intervention Failure	1.0	In the event of an RT system LOF, the ability for ATCS to intervene is significantly compromised
Intervention Failure	0.215	= $1.0x10^{-7}$/(1.23E-5 * 0.038)
Nominal Cat B Runway Incursion	$1.51x10^{-7}$	Table 6-1
Cat B Runway Incursion Hazard	$2.51x10^{-7}$	=$1.51x10^{-7}$ + $1.0x10^{-7}$
Remote Tower Failure	0.25	=0.215/0.86

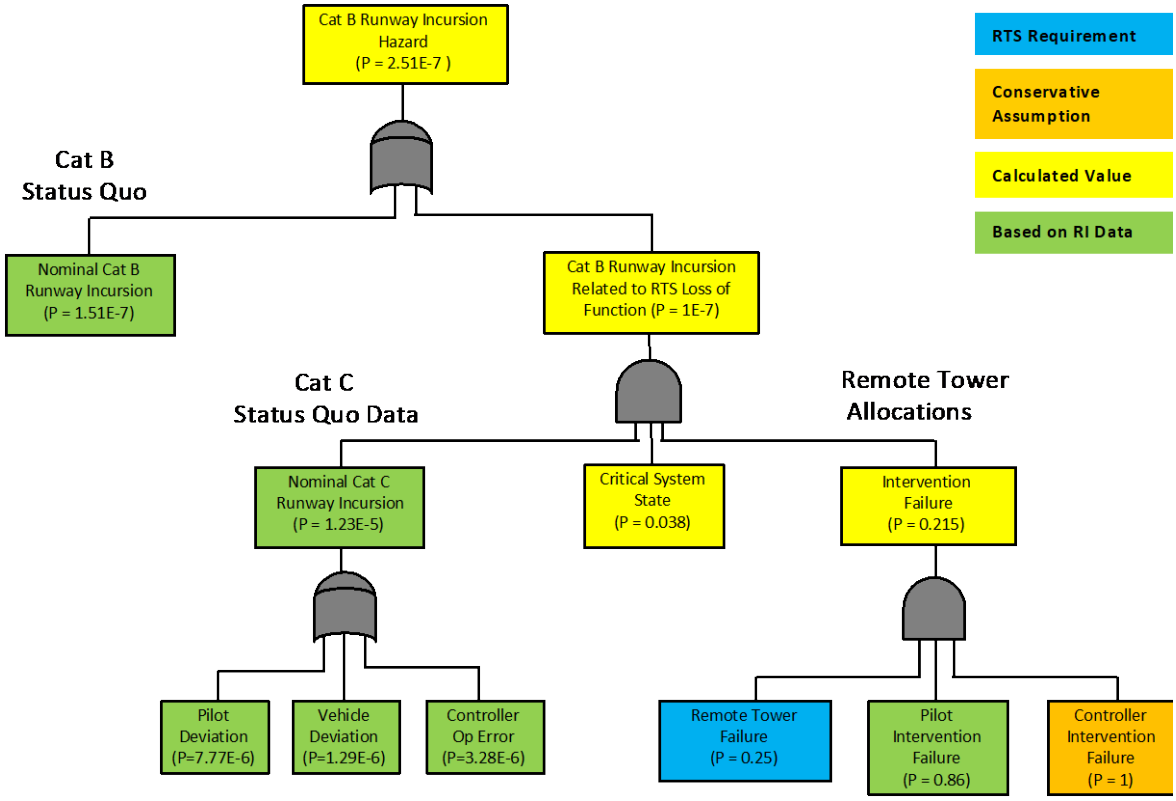

Figure 7-2: Loss of Function Fault Tree Minimum RT System Allocation

Because the Cat B Runway Incursion event related to RT system Loss of Function event includes the *a priori* likelihood of a Cat C incursion, the allocation to the Remote Tower Failure works out to be minimal, a maximum probability of 0.25. As this probability level would result in an operationally unacceptable level of reliability it was decided to allocate a minimum acceptable reliability requirement to the Remote Tower based on engineering judgment and subject matter expertise. The value chosen for the MTBCF was 2190 hours, which is equivalent to one failure per quarter (3 months). This is likely the maximum acceptable rate of failures for the RT system. In the fault tree (Figure 7-3) the MTBCF is converted to a probability by factoring in the exposure time (see discussion later) of 120 seconds resulting in a Remote Tower Loss of Function probability of 1.5×10^{-5} per operation. The contribution of a Remote Tower Failure event resulting in a Cat B Incursion (6.1×10^{-12}) compared to the overall likelihood of a Cat B incursion Hazard (1.5×10^{-7}) is negligible. Therefore, the MTBCF of 2190 hours is deemed as an acceptable RT Loss of Function requirement.

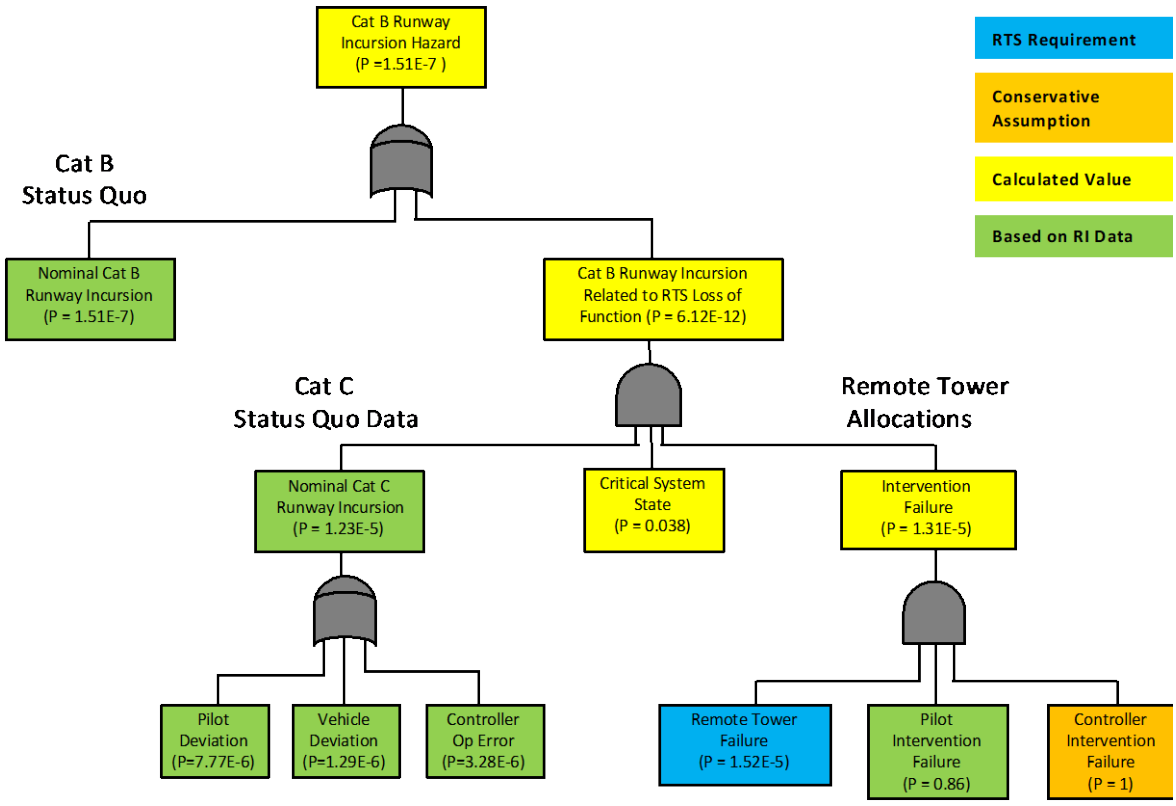

Figure 7-3: Loss of Function Fault Tree Final Allocations

7.2 Remote Tower Malfunction

Figure 7-4 is the generic fault tree for the Remote Tower malfunction hazard. The malfunction hazard was defined by the OSA to be a Category B runway incursion. The data assessment was used to quantify events that through fault tree analysis techniques can be used to determine the RT system allocation. It was determined one goal of the assessment is to estimate the likelihood of Category C runway incursions becoming Cat B. It was also determined that by definition Cat D runway incursions are not a meaningful risk of becoming Cat Bs.

The left side represents the nominal rate of incursions that occur in "fault-free" RT system operations, meaning the RT system is operating normally. This is identified as the Cat B Status Quo Data branch of the fault tree. The assumption is that given the known rate of Cat B and Cat C runway incursions, the difference between these two rates is due to various barriers. Three specific barriers were identified: controller intervention, pilot intervention, and the "critical system state." The critical system state represents conditions that prevent a Cat C runway incursion from becoming a Cat B, primarily based on the relative relationship (geometry and timing) between two aircraft or an aircraft and ground vehicle. More specifically, the critical system state includes cases where no intervention was required (by pilot or controller) to mitigate the conflict. The formula used to compute critical system state is shown later in Equation 1.

The right side of the fault tree represents a Cat B runway incursion due to a Remote Tower malfunction. The Remote Tower malfunction is primarily manifested in the ability of the controller to make proper

decisions in giving instructions to pilots and vehicle drivers resulting in reduced spatial separations. It is assumed that the malfunction results in Hazardously Misleading Information (HMI) being presented to the controller. The HMI then can lead to the controller making an operational incident, leading to a Cat C runway incursion. As in the case of the status quo portion of the fault tree, there are three potential barriers to mitigating the conflict: controller intervention, pilot intervention (see-and-avoid), and critical system state.

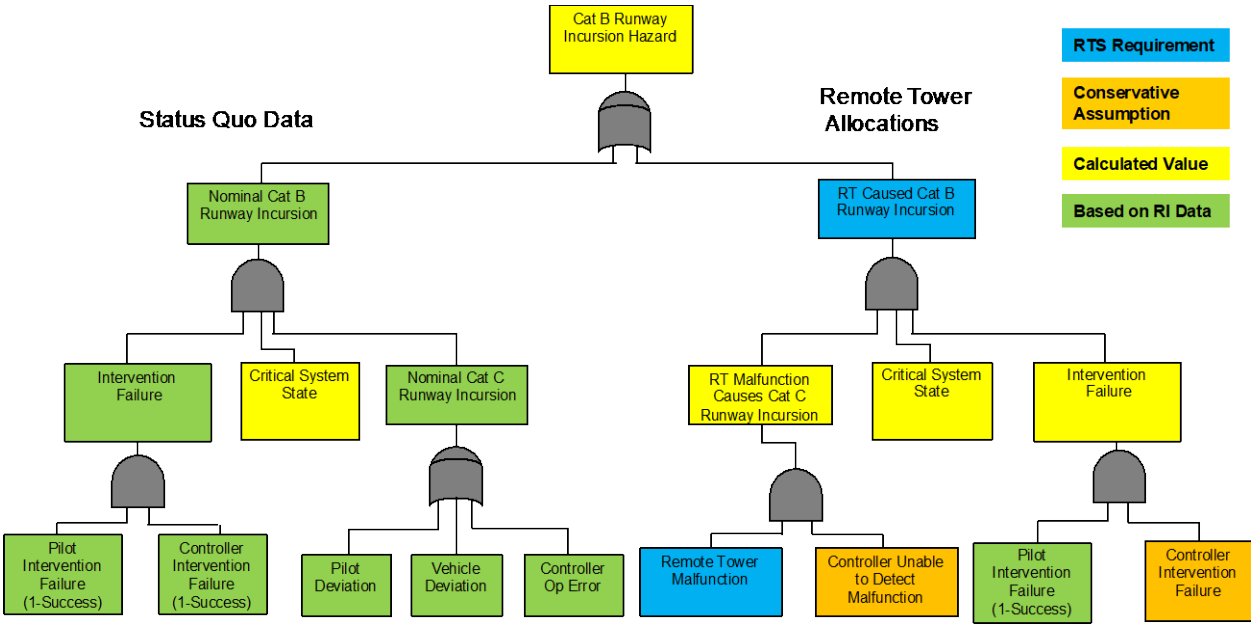

Figure 7-4: Generic Malfunction Fault Tree

Figure 7-5 includes the allocations for the malfunction hazard. A key decision made concerned the goal (target level of safety) for the overall probability of a Cat B runway incursion influenced by a Remote Tower malfunction. There were two primary factors considered in the determination of this allocation. One is that the hazard severity assigned in the OSA which is major severity. The other is that the nominal rate of Cat B runway incursions for the relevant class of airports and operations in the NAS, which is 1.5×10^{-7} per operation. Hazards with a major severity are normally allocated (i.e., per SMS guidance) a probability between 10^{-5} and 10^{-7}. It was established that the acceptable rate of Category B RIs for operations utilizing RT systems was 1.0×10^{-6}.

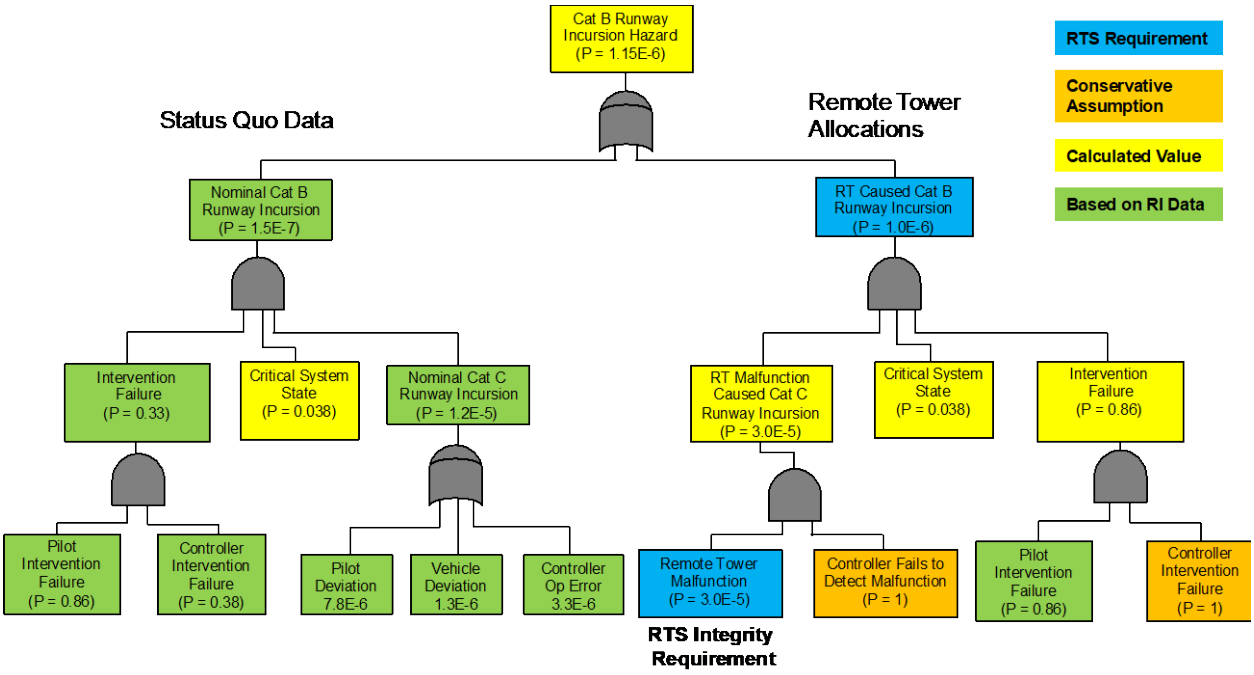

Figure 7-5: Malfunction Hazard Allocations

The status quo Cat C runway incursion rates are derived from the runway incursion event data for Non-ASDE Airports: VMC Operations and summarized in Table 6-1**.** The pilot see-and-avoid success rate and the controller intervention success rate were estimated by examining the narrative descriptions of the runway incursion events. The narratives were used to assign credit to controller intervention or pilot intervention (Section 5.4). When the controller intervened and instructed one (or both) of the pilots (or vehicle driver) to take evasive action, the controller was credited with success. When one or both pilots initiated evasive action, the pilot was credited with success. The values and rates (based on 1227 Cat C runway incursions) are shown in Table 7-2.

Table 7-2 Intervention Success and Failure Rates by Controllers and Pilots

	# Successes	Success Rate	Failure Rate
Controller	760	61.9%	38.1%
Pilot	169	13.8%	86.2%
Combined			32.8%

The intervention failure rate is computed by subtracting the success rate from 1 (1 – Success). The last value that can be computed from the assessment of collected data is the Critical System State event rate, which is computed in Equation 1:

P(Critical System State) = (Nominal Cat B Rate)/[(Combined Intervention Failure Rate)*(Nominal Cat C Rate)] (Eq. 1)

$P(\text{Critical System State}) = (1.5\times10^{-7})/(0.33*1.2\times10^{-5}) = 0.038$

It is assumed that the Critical System State event likelihood will be the same for Remote Tower operations as with brick-and-mortar towers. Therefore, the same value is applied to the Remote Tower Allocation branch of the fault tree. Similarly, the pilot see-and-avoid intervention Failure event probability is assumed to be the same value (0.86) on the Remote Tower Allocation branch of the fault tree. Controller intervention failure rate is assumed to be one since there is an RT system malfunction. Because the malfunction results in HMI being displayed to the controller it is conservatively assumed that controller intervention will not be possible. The Remote Tower Malfunction allocation can now be computed since there are estimates for all of the other allocations on the Remote Tower Allocation branch, including the goal for Cat B runway incursions caused by Remote Tower malfunctions equal to $1x10^{-6}$ (RT Caused CAT B Runway Incursion event). The allocation is computed in Equation 2:

P(Remote Tower Malfunction) = (RT Caused Cat B Rate)/[(Pilot Intervention Failure Rate)*(Critical System State)] (Eq. 2)

P(Remote Tower Malfunction) = $(1x10^{-6})/(0.038*0.86) = 3.06x10^{-5}$ in any operation

7.3 Average Risk and Specific Risk

An important aspect regarding the allocation of risk concerns whether to treat it as "average risk" or "specific risk." An Aviation Rulemaking Advisory Committee for Transport Airplane and Engine Issues Area reported that an FAA/EASA consensus definition for "specific risk" is as follows:

> *"The risk on an aircraft on a specific flight due to a condition that deviates from the fleet's average risk."*[9]

An example of the difference and how that is applied can be found in aircraft navigation systems. Loss of continuity for navigation systems is generally considered to be an average risk. Loss of integrity is generally treated as a specific risk, where the assumption is that the aircraft is in a critical phase of the flight operation (e.g., Category I or Category III landing). ICAO Annex 10 contains the following guidance material concerning the application of specific risk to GPS navigation systems:

> *"The approach integrity requirements apply in any one landing and require a fail-safe design. If the specific risk on a given approach is known to exceed this requirement, the operation should not be conducted. One of the objectives of the design process is to identify specific risks that could cause misleading information and to mitigate those risks through redundancy or monitoring to achieve a fail-safe design. For example, the ground system may need redundant correction processors and to be capable of shutting down automatically if that redundancy is not available due to a processor fault."*[10]

Another example of the difference and how it is applied can be found in the application of the continuity risk to precision approach navigation. For a CAT I GBAS Landing System (GLS) precision approach the loss of continuity is defined as "an average probability per 15-second period". ICAO SARPS Annex 10 guidance material states the following:

> *"For GNSS-based APV and Category I approaches, missed approach is considered a normal operation since it occurs whenever the aircraft descends to the decision altitude for the approach*

[9] TAE.Meeting.Notice.10.14.04 (faa.gov)

[10] ICAO Annex 10, Aeronautical Telecommunications, Volume 1, July 2018, Attachment D, 3.3.11.

> *and the pilot is unable to continue with a visual reference. The continuity requirement for these operations applies to the (over time) of loss of service, normalized to a 15-second exposure time. Therefore, the specific risk of loss of continuity for a given approach could exceed the average requirement without necessarily affecting the safety of the service provided or the approach."*[11]

Unlike the above CAT I example, the continuity requirement for a ground system supporting a CAT III precision approach is defined as "during any 15-second interval" indicating that specific risk rules apply. The specific risk rules apply due to the aircraft's proximity to the ground, e.g., GLS CAT III supports guidance through touchdown and rollout. Specific approach conditions may generate higher risks than the average and degrade the safety of the operation to unacceptable levels.

The question then is how do average risk and specific risk apply to Remote Tower Systems. Computing under average risk rules protects the user on average during the nominal operational rate of traffic levels. However, it does not protect every user during peak operations and traffic density at all airports. Some users will experience higher risk during operations where traffic levels are higher. Under specific risk, all users are protected with acceptable (required) risk since it applies to each operation.

The RT system continuity requirement allocation associated with loss of function is based on average risk. Though the derived RT System continuity probability is 1.52×10^{-5} per operation (see Figure 7-3), the minimum allocation shown in Figure 7-2 demonstrates that an increase in RT system continuity risk will not cause Category B runway incursion risk to be unacceptably high. Therefore, estimation of loss of continuity can account for system operation over all relevant conditions (traffic density, environmental, etc.).

The RT system integrity requirement allocation associated with a malfunction is based on specific risk. Since the malfunction can contribute to the hazard it should account for the risk under worst-case conditions. In the case of the RT system, this means peak traffic density. Thus, it is assumed that the RT system malfunction and peak aircraft operations are concurrent and potentially contribute to a major severity hazard (e.g., Cat B runway incursion). Therefore, no credit has been taken for averaging the traffic density.

A convention is applied to numerical probability values to denote where average vs. specific risk rules apply. The use of "per operation" or "per 120 sec exposure time" will be used to indicate where average risk rules apply and "in any operation" or "per any 120 sec exposure time" to indicate where specific risk rules apply.

8 Development and Allocation of Technical Requirements

8.1 Integrity

The allocated probability of Remote Tower malfunction (Figure 7-5) is 3×10^{-5} for any operation. An issue here is the definition of a malfunction. A malfunction is defined as a failure that results in Hazardously Misleading Information (HMI). Initially, HMI was defined in the Technical Requirements (Remote Tower (RT) Systems Minimum Functional and Performance Requirements for Non-Federal Applications) to be a failure to meet the RVP latency requirement. Subsequent review determined that HMI could occur through other types of failures in the Remote Tower system. Since the OSA hazard is a Cat B runway

[11] ICAO Annex 10, Aeronautical Telecommunications, Volume 1, July 2018, Attachment D, 3.4.

incursion, the definition of HMI was revised to be "a failure contributing to a major severity hazard (e.g., Category B runway incursion or rejected landing near runway threshold), as defined in the FAA Safety Management System Manual."

A second issue with the allocation is that the probability is "for any operation." In order to determine the technical requirement, the operation needs to be specifically defined and an associated exposure time defined. The event associated with the hazard is a runway incursion. Therefore, the exposure time should be the time that an aircraft can potentially be exposed to a Cat C runway incursion. An assessment of typical operations determined that this time is nominally 60 seconds. This accounts for the time between when the landing aircraft is at 200 ft altitude (Category I Decision Altitude) through the touchdown and rollout segments. Another scenario that was identified concerns the Line Up And Wait (LUAW) procedure. FAA Order 7110.65, Section 3-9-4 defines LUAW as follows:

> *The intent of LUAW[12] is to position aircraft for an imminent departure. Authorize an aircraft to line up and wait, except as restricted in subparagraph g, when takeoff clearances cannot be issued because of traffic. Issue traffic information to any aircraft so authorized. Traffic information may be omitted when the traffic is another aircraft which has landed on or is taking off the runway and is clearly visible to the holding aircraft. Do not use conditional phrases such as "behind landing traffic" or "after the departing aircraft".*

An examination of the runway incursion database found a significant number of events that involved the use of LUAW for at least one of the aircraft involved, as shown below:

- 3 of 15 Cat B events (20%)
- 60 of 1227 Cat C events (4.9%)
- 46 of 2310 Cat D events (2%)

Since the LUAW procedure allows the aircraft to be holding on the runway for up to 90 seconds, this time should be taken into account in the determination of the exposure time. It is understood that in typical operations the aircraft do not hold for that long. However, since the malfunction case involves an integrity requirement it should account for the worst-case (specific risk). In addition to an aircraft holding on the runway for up to 90 seconds, the exposure should also account for the time for a landing or takeoff aircraft to be on the runway. That is typically 30 seconds. Therefore, the total exposure time could be 120 seconds. The resulting Remote Tower malfunction requirement is the following:

> *"The probability of an undetected malfunction of the RVP resulting in Hazardously Misleading Information (HMI) shall be less than or equal to $3.0x10^{-5}$ in any 120 seconds[13]. HMI is defined as any failure contributing to a major* severity *hazard (e.g., Category B runway incursion or rejected landing near runway threshold), as defined in the FAA Safety Management System Manual."*

[12] NOTE- When using LUAW, an imminent departure is one that will not be delayed beyond the time that is required to ensure a safe operation. An aircraft should not be in LUAW status for more than 90 seconds without additional instructions.

[13] Note that the requirement in the current draft of the Technical Requirements is "$3.0x10^{-5}$ per 120 seconds." That will be changed to be the same as above.

8.2 Continuity

As described in section 7.1 the defined MTBCF was chosen as 2,190 Hours. The MTBCF can be converted to a failure probability with the approximation in Equation 3:

P(Failure) = 1/[(MTBCF)*(Exposure Time)] [Eq. 3]

The exposure time is allocated to be 120 seconds (2 minutes). That is based on a nominal time between aircraft operations during operations at a single runway.

P(Failure) = 1/[(2190 Hrs)*(60 min/Hr/2 min)] = 1.52×10^{-5} per 120 seconds

Since the Loss of Function is a safety-related hazard the Remote Tower allocation is specified as a continuity requirement as follows:

> *"The probability of the loss of continuity of operation shall be less than or equal to 1.5×10^{-5} per 120 seconds, where loss of continuity of operation is defined as a critical failure."*

8.3 Design Assurance Level Assignment

The purpose of this section is to describe how requirements for DALs were determined following consideration for existing barriers and mitigations at the NAS operational level. These barriers and mitigations were incorporated into the LoF, and malfunction fault trees contained in section 7.

Design assurance levels are defined at different levels, consistent with the RT system-requirements. These levels as well as the applicable industry standard are identified as follows:

- A functional level DAL is identified for each function within the RT system based on the application of ARP-4754A.
- A software DAL is identified for each RT system function which applies to any software contained within the function based on the application of DO-278A.
- A complex hardware DAL is identified for each RT system function which applies to any complex hardware contained within the function based on the application of DO-254.

8.3.1 Background

The Remote Tower (RT) Systems Operational Safety Assessment (OSA) for Non-Federal Applications conclusions are summarized in Table 8-1.

Table 8-1 OSA Functional Hazard Severities

Function	Loss of Function (LoF) Hazard Severity	Malfunction Hazard Severity
RVP	Major	Major
SLG	Minimal	Minimal
AA	Minimal	Minimal
MDT	Minor	Major

The following functions/hazards trace from the OSA to the Design Assurance Level (DAL) requirements without further mitigation or barrier considerations:

- SLG Loss of Function
- SLG Malfunction
- AA Loss of Function
- AA Malfunction
- MDT Loss of Function

Mitigations and barriers for the RVP LoF and malfunction as well as MDT malfunction will be evaluated further in this document to derive applicable design assurance level requirements. These remaining hazards are described as follows:

- Loss-of-Function (LoF) is the loss of capability to detect and identify/observe spatial relationships objects in the area of jurisdiction (i.e., runways, short finals, and base turns).
- Malfunction is where Hazardously Misleading Information (HMI) is provided to ATCT controller e.g., presented visual information is not real-time or relative spatial relationship between objects are incorrect.

The OSA categorized both the LoF and malfunction hazards as major severity hazards. The worst-case credible effects were identified as category B incursion, rejected takeoff, or rejected landing at or near the threshold.

- The LoF hazard contributes to this effect due to the ATCS losing the ability to intervene in the prevention of a runway incursion if a conflict arises.
- The malfunction hazard contributes to this effect in one of two ways:
    - The malfunction may mask the ability of ATCS to intervene in the prevention of a runway incursion.
    - Provide visual information to ATCS in such a manner as it leads to faulty instructions leading to a runway incursion.

In the assessment of the LoF and malfunction hazards, the OSA did not consider the impact of any barriers or mitigation strategies when determining the hazard severity classifications.

8.3.2 Process Consideration

The process followed to assign software and complex hardware DAL's is described here, with applicable references to the SRMGSA and the Safety Management System Manual (SMS). The process steps are:

Step 1: Initial Functional-Level DAL Assignment
Step 2: Functional-Level DAL After Barriers/Mitigation Considerations
Step 3: Software and Complex Hardware DAL Selection

These steps, which are described in the following sections, are consistent with the SRMGSA. Section 2.3.2.1.4 states:

> *"New or modified FAA CNS/ATM systems should impose a system development process such as that outlined in SAE ARP4754A. Using this methodology, system-level DALs would be assigned to each function based on the highest severity level within each function. Software DALs using RTCA*

DO-278A and hardware DALs using RTCA DO-254 could then be allocated to each component and better aligned with system-level DALs. The assignment of DALs is architecture dependent, and the PO should work with ANG to consider designs that not only ensure safety, but also satisfy business goals."

8.3.2.1 Step 1 – Initial Functional Level DAL Assignment

The functional-level DAL is assigned based on the worst-case credible effect that hazards at the functional level could contribute to.

This step has largely been performed within the OSA, as the hazards for each function have been identified along with their worst-case credible effect. Per section 3.2 of the OSA, mitigation strategies within the CNS/ATM system are not used to lower the resulting functional level hazard classifications.

The remaining action for this step is to translate the OSA's hazard classification to DAL, per ARP-4754A.

8.3.2.2 Step 2 – Final Functional Level DAL After Barriers/Mitigation Considerations

Barriers and mitigation strategies are used to assess the impact on hazard severity and considered for possible reductions in the FDALs (Functional Design Assurance Level) assigned to each of the functions and hazards identified in Step 1.

This is accomplished using section 5.2.3.2 of ARP-4754A as guidance. The ARP guidance provides a process that allows for reductions in FDAL under certain conditions. These conditions are shown in Table 3 of ARP-4754A and are described as follows, for the major severity hazard classification only:

- If the RT system functional hazard can solely lead to the hazardous effect (Category B Incursion) then no reduction of DAL is permitted.
- If multiple independent events are required to cause the hazardous effect (Category B Incursion), then either of the following may apply:
    - One of the independent events inherits the Major hazard class DAL and other events DALs are set based on the remaining most severe hazards for that event.
    - Two or more independent events are at the Minor hazard class DAL (one step below Major) and DALs for other events are set based on the remaining most severe hazards for that event.

ARP-4754A was specifically written to address aircraft level functions and their associated risks and does not specifically address operational risks associated with processes and procedural mitigations. In this step the process is adapted to consider credit for operational barriers and operational mitigations. This is consistent with section 2.2.1.1 of the SMS Manual, which when referencing the traditional Swiss cheese hazard model states:

"Developing a safe procedure, hardware, or software system requires that the procedure/system contain multiple defenses, ensuring that no single event or sequence of events results in an incident or accident."

Section 3.5.2 of the SMS goes on to describe controls that reduce a hazard's causes or effects. Examples of controls (SMS Table 3.2) include systems that can provide mitigations or barriers for hazards such as Traffic Collision Avoidance System and Ground Proximity Warning System, but also include operational control methods such as use of checklists, pilot intervention, and controller intervention.

8.3.2.3 Step 3 – Software and Complex Hardware DAL Selection

The FDAL from step 2 is used to determine the software and complex hardware DALs based on DO-278A and DO-254 respectively. The correlation between DO-278A and DO-254 DALs and ARP-4754A FDALs is shown in Table 8-2.

Table 8-2 Functional, Software, Hardware DAL Correlation

Failure Condition Category	Functional DAL's (ARP-4754A)	Software DAL's (DO-278A)	Complex Hardware DAL's (DO-254)
Catastrophic	FDAL A	AL1	Level A
Hazardous	FDAL B	AL2	Level B
Major	FDAL C	AL3	Level C
Between Major & Minor	No Equivalent	AL4	No Equivalent
Minor	FDAL D	AL5	Level D
No Effect	FDAL E	AL6	Level E

There is a direct one-for-one correlation between the functional DAL's and the Hardware DAL's. Likewise, there is a one-for-one correlation between FDAL's A, B, and E with software DAL's. These direct correlations make the software and complex hardware DAL's unambiguous in terms of selection.

The DO-278A software design assurance categories have three levels, Major (AL3), Minor (AL5), and Less than Major, more than Minor (AL4).

> *As cited in DO-278 (but removed from DO-278A), assurance level 4 (or AL-4) was developed to account for "certain CNS/ATM systems where AL-3 was too stringent and AL-5 was too lenient".*[14]

Section 6.1 of the SRMGSA states:

> *"AL4 applies to CNS/ATM software that satisfies objectives less stringent than AL3 but more stringent that AL5. AL4 is not consistent with or equivalent to any RTCA DO-178C airborne software levels." account for "certain CNS/ATM systems where AL-3 was too stringent, and AL-5 was too lenient".*

To resolve the ambiguity associated with selecting the software DALs associated with Major and Minor fault condition categories consideration will be given to the barriers and mitigation strategies (quantitative and qualitative) external from the device containing the software.

8.3.3 Loss of Function (LoF) Design Assurance Level

The most severe credible hazard associated with a LoF for the RVP was determined by the OSA to be a category B runway incursion, which has a hazard category of major severity, which would correspond to an occurrence probability in the range of 1.0×10^{-5} to 1.0×10^{-7} per operation. This represents a Functional DAL (FDAL) of C consistent with ARP-4754A.

[14] RTCA DO-278, Section 2.1.

The Category B incursion is a result of an unmitigated Category C runway incursion. The Category C incursion could be caused by a pilot deviation, a vehicle deviation, or an operational incident by the controller. Historical data for these events show they have a probability of occurrence of approximately 10^{-5} per operation. Once the Category C incursion has occurred there are three mitigation barriers to prevent it from escalating to a Category B incursion. These are:

- Critical System State – Conditions such as a relationship (geometry and timing) between the vehicles prevent a Cat C incursion from escalating to a Cat B incursion.
- Pilot see-and-avoid – Pilots are to continuously scan for other aircraft, vehicles, or other objects when operating at an airport.
- ATC intervention - ATC is responsible for preventing collisions involving aircraft operating in the system and apply separation standards.

As described in Section 7.1, a Remote Tower Failure probability of 0.25 is sufficient to support compliance with the tighter requirement of 1.0×10^{-7} per operation for a Category B incursion related to an RT system LoF. Therefore, the final FDAL, after consideration of barriers and mitigations, can be classified as Minor (FDAL D).

The FDAL of D (Minor) corresponds to a software DAL of AL4 or AL5 and a complex hardware DAL of level D. Since Minor is typically associated with frequency of occurrence between 10^{-3} and 10^{-5}, and we are only needing a 0.25 LoF failure probability for the RT system (see Figure 7.1-2), there is more than enough margin to select the software DAL of AL5.

The proposed minimum requirements for the RVP loss of function are shown in Table 8-3[15].

Table 8-3 Minimum Requirements for RVP Loss of Function Hazard

Function	Failure	ARP 4754A DAL	DO 278A DAL	DO-254 DAL
RVP	Loss of Function	FDAL D	AL5	Level D

8.3.4 Malfunction Design Assurance Level

The effects of a malfunction can vary depending on the specifics of the malfunction being presented. In general, the malfunction represents the presentation of Hazardously Misleading Information (HMI) to the ATCS which can include incorrect temporal and spatial relationships. Malfunction for both the RVP and MDT functions were identified as potential contributors to HMI.

The most severe credible hazards associated with a malfunction failure that causes HMI included:

- ATC makes an incorrect decision based on the HMI, leading to a category B incursion.
- Flight crew rejects landing at or near the runway threshold.
- Flight crew rejects takeoff.

Based on the above hazards, the OSA assigned the RT system malfunction with a hazard severity of major, which would normally correspond to an occurrence probability in the range of 1.0×10^{-5} to 1.0×10^{-7} for any operation. This represents a functional DAL of C consistent with ARP-4754A.

[15] Note that applicants may incorporate additional architectural mitigations to further reduce the above DAL's. The applicant may also incorporate additional functionality within the RT system whose safety impact will need to be evaluated to determine the appropriate DAL for the functionality.

As described in sections 5 and 6, data was analyzed to identify that the current risk for a category B runway incursion, without the RT system, is 1.5×10^{-7} for any operation. The introduction of the RT system will result in new failure modes that can independently lead to a category B incursion. A target of 1.0×10^{-6} was determined to be an acceptable rate for the increase of Cat B incursions caused by the malfunction of the RVP. This means that the overall category B incursion risk can be 1.15×10^{-6} for any operation ($1.5 \times 10^{-7} + 1.0 \times 10^{-6}$), which is near the mid-point for the acceptable range for a major severity category hazard.

Using the target of 1.0×10^{-6} for any operation, the fault tree shown in Figure 8.2-2 was constructed to determine the allocated RT malfunction probability. This fault tree was used to derive the required Remote Tower Malfunction probability of 3.0×10^{-5} for any operation by consideration of mitigations. The derived RT system malfunction probability requirement was computed using several conservative measures, which are described as follows:

Conservative Measure #1 – Controller Fails to Detect Malfunction

A malfunction for the RT system that produces HMI may be readily apparent to the controller such as inconsistency between displays, or inconsistency between pilot reported information and visual presentations. A controller's capability to detect HMI is limited and difficult to quantify. Additionally, there are not procedures defined for ATCS to monitor for HMI. For these reasons, no credit is taken for this in deriving the RT system malfunction probability.

Conservative Measure #2 – Controller Intervention Failure

A Category C RI attributed to RT systems HMI may be prevented from escalating to a Category B incursion by ATCS intervention (e.g., interventions supported by aircraft and controller communications). The original RT system HMI that produced the Category C incursion could also mask information the controller would need to prevent the escalation to a Category B incursion. For this reason, no credit is taken for this potential mitigation. For these reasons, no credit is taken for the need for RT system malfunction and operational scenarios to correlate to produce a CAT B RI.

Conservative Measure #3 – Correlation of RT System HMI with Operational Scenario

It is conservatively assumed that any RT system malfunction causing HMI will result in a Category C incursion. This is not the case in operational practice as the positions and movements of aircraft and vehicles need to coincide with the specific HMI scenario that is occurring. For example, a frozen screen in a location where no aircraft or vehicle movements are taking place could not produce a Category C incursion. In addition to the obvious difficulty in quantifying this conservative measure, there is concern that its quantification is inconsistent with specific risk rules.

Conservative Measure #4 – Application of specific risk rules

As described in Section 7.3 specific risk rules were applied to the malfunction hazard. One implication of this decision was that no credit was taken for traffic density, i.e., an RT system malfunction cannot contribute to a Category B runway incursion if there is not a second aircraft or a vehicle present.

ARP-4754A contains a process by which the assignment of a Functional Design Assurance Level (FDAL) can take credit for external events, see section 5.2.4 of ARP-4754A. The example used in the standard is the external event of a cargo fire as it relates to the FDAL for the monitoring system. Though the risk of an undetected cargo fire may be an FDAL of A, the FDAL of the monitors may be reduced to an FDAL of B

or C depending on the probability of the external event (cargo fire). Though specifics are not contained for applying this principle when the initial FDAL is C, the standard does not exclude this application.

The numerical requirement for an RT system malfunction leading to HMI producing a Category C incursion has been identified as 3.0×10^{-5} for any operation. This event could conservatively inherit the FDAL of C based on its contribution to a Category B incursion which is classified as a major severity hazard. Instead, this assessment concludes that the FDAL should be level D for the following reasons:

- The Category C incursion event is in-and-of-itself a Minor hazard. The severity table in the SMS (Table 3.3) defines a Category C runway incursion as having a Minor hazard severity classification.
- Application of the ARP-4754A process for taking credit for external events permits the reduction of FDAL for external events. The external events currently contained in the fault tree are 3.27×10^{-2} (0.038 x 0.86) but as described above are conservative such that in operational practice could be expected to be lower by an order of magnitude or more.

The FDAL of D corresponds to a software DAL of AL4 or AL5 and a complex hardware DAL of level D. The small margin between the requirement ($3x10^{-5}$) and upper range for Minor hazards (10^{-5}) led to the selection of software DAL AL4.

The proposed minimum requirements for the malfunction hazards are shown in Table 8-4[16].

Table 8-4 Minimum Requirements for RVP & MDT Malfunction Hazard

Function	Failure	ARP 4754A DAL	DO 278A DAL	DO-254 DAL
RVP	Malfunction	FDAL D	AL4	Level D
MDT	Malfunction leads to loss of integrity	FDAL D	AL4	Level D

9 Summary

The purpose of this report was to provide the rationale for the final safety related technical requirements for the Remote Tower (RT) Systems Minimum Functional and Performance Requirements for Non-Federal Applications. The assessment concentrated on assessing the barriers that mitigate Category C runway incursions from becoming Category B incursions, since those are the most severe hazards identified in the OSA classified as having major hazard severity. The assessment included reviewing runway incursion statistics and an assessment of pilot and controller runway incursion intervention and success rates in the mitigation of runway incursion severity. The assessment also determined that in addition to controller and pilot intervention that the occurrence of Category B runway incursions required the presence of a critical system state, such that two aircraft (or vehicle) are in a proximity that could potentially lead to the Category B incursion.

The results of the assessment allowed the derivation of allocations to the Remote Tower system for Loss of Function and Malfunction events. The resulting allocations are less stringent than those that would be

[16] Note that applicants may incorporate additional architectural mitigations to further reduce the above DAL's. The applicant may also incorporate additional functionality within the RT system whose safety impact will need to be evaluated to determine the appropriate DAL for the functionality.

based on the OSA (per Table 8-2, the RVP DALs would have been: FDAL C, AL3, Level C). The numerical allocations are the following:

Malfunction Integrity Requirement: $\leq 3x10^{-5}$ in any 120 seconds

Loss of Function Continuity Requirement: $\leq 1.5x10^{-5}$ per 120 seconds

The allocations also resulted in new Design Assurance Levels as shown in Table 9-1.

Table 9-1 Design Assurance Level Summary

Function	**Failure**	**ARP 4754A DAL**	**DO 278A DAL**	**DO-254 DAL**
RVP	Malfunction	FDAL D	AL4	Level D
MDT	Malfunction leads to loss of integrity	FDAL D	AL4	Level D
RVP	Loss of Function	FDAL D	AL5	Level D