Advanced System Design Services
FAA NAS Modernization Group
ATO Technical Operations - Operations Support

Remote Tower (RT) Systems Operational Safety Assessment (OSA) for Non-Federal Applications

For Use in Class D Airspace

Version 2.7

April 1, 2021

Executive Summary

Remote Tower (RT) systems use visual sensors at an airport, and visual display systems at a separate location, to provide a visual reproduction of an airport environment for Air Traffic Control (ATC) purposes without the construction of a brick-and-mortar tower. Remote Tower systems as defined in this OSA are intended to be used in Class D airspace to provide VFR Tower Services. These Remote Tower is "visual-only" with no integrated surveillance source allowed, and no stand-alone surveillance source assumed. The use of a RT system is intended to be transparent to tower customers (pilots).

Air traffic facilities using an RT system are intended to offer the same set of 24 services that a traditional brick-and-mortar tower would. The Remote Tower system is not responsible for provision of all services, as some services are partially or completely the responsibility of MEL items, including communication devices. Procedures and procedural mitigations are to be considered as a mitigation to hazards resulting from use of the RT system.

According to the ATO Safety Risk Management Guidance for Acquisition Management (SRMGSA), this analysis should provide an early identification and documentation of safety requirements that could improve safety product integration, lower developmental costs, increase product performance, and increase the probability of the program's success. As RT systems are planned to be implemented as non-federal systems, this OSA focuses on identifying safety requirements.

During this exercise, the OSA Safety Risk Management Panel identified the following 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-PLoF-1	Partial loss of the capability to detect and identify objects and observe spatial relationships in non-essential / non-critical areas.	Minimal
RVP-MALF-1	HMI provided to ATCT controller: Presented visual information is not real-time; asynchronous time lag between presentations/displays. 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
SLG-LoF-1	Inability to provide visual signals to aircraft, vehicles, and personnel (NORDO present).	Minimal
SLG-MALF-1	SLG visual signal is unable to point/track accurately.	Minimal
SLG-MALF-2	Incorrect visual signal (i.e., incorrect color pattern / sequence) provided to at least one aircraft, vehicles, or personnel.	Minimal
AAA-LoF-1	Total loss of ability of ATCS to hear AAA.	Minimal
AAA-PLoF-1	Failure of individual audio microphone and/or speaker. This results in inability of ATCT to hear AAA from section of airfield.	Minimal
AAA-MALF-1	AAA isn't provided in "near real time" (e.g. delayed, out of synchronization with correct visual information, etc.). This results in misleading information provided to ATCT.	Minimal
AAA-MALF-2	AAA is not spatially representative of reality (e.g. engine noise from the south appears to be coming from the north). This results in misleading information provided to ATCT.	Minimal
AAA-MALF-3	AAA quality or volume creates a distraction (e.g. volume stuck high, excessive noise, etc.).	Minimal
MDT-MALF-1	Loss of system availability (System State: Nominal).	Minor
MDT-MALF-2	Loss of system integrity during operations due to a malfunction or error during the installation, setup, or checkout process.	Major

According to the current SRMGSA, an OSA does not consider overall safety risk, rather, it is used to assess a hazard's severity and determine the target level of likelihood required to achieve an acceptable level of safety. This is not a typical OSA in that the Remote Tower program specifically led by the FAA will not conduct other aspects the FAA Acquisition Management System (AMS) lifecycle. This OSA is intended to be used to identify functional hazards, identify safety critical functions, and determine requirements which will have to be met by all Remote Tower vendors to achieve system approval for use in the NAS.

Signature Page One of Six

Title: Remote Tower Operational Safety Assessment (OSA)

Initiator: Shelly Beauchamp Project Lead
Initiator's Organization: Remote Tower Program
Initiator's Phone Number: (609) 569-2624
Submission Date: 04/01/2021
SRMD Revision Number: 2.7
SRMD Revision Date: 04/01/2021

Submitted By:	Shelly A. Beauchamp	4/26/2021
	Shelly Beauchamp Manager, Advanced Systems Design Service Team, AJW-121	Date

Signature Page Two of Six

Title: Remote Tower Operational Safety Assessment (OSA)

Initiator: Shelly Beauchamp Project Lead
Initiator's Organization: Remote Tower Program
Initiator's Phone Number: (609) 569-2624
Submission Date: 04/01/2021
SRMD Revision Number: 2.7
SRMD Revision Date: 04/01/2021

Reviewed By: James D. Linney
Director, Operations Support, AJW-1

5/1/21
Date

Signature Page Three of Six

Title: Remote Tower Operational Safety Assessment (OSA)

Initiator: Shelly Beauchamp Project Lead
Initiator's Organization: Remote Tower Program
Initiator's Phone Number: (609) 569-2624
Submission Date: 04/01/2021
SRMD Revision Number: 2.7
SRMD Revision Date: 04/01/2021

Reviewed By: PAUL FONTAINE Digitally signed by PAUL FONTAINE Date: 2021.04.29 13:16:21 -04'00'

Paul Fontaine
Director, Portfolio Management and Technology Development, ANG-C

Date

Signature Page Four of Six

Title: Remote Tower Operational Safety Assessment (OSA)

Initiator: Shelly Beauchamp Project Lead
Initiator's Organization: Remote Tower Program
Initiator's Phone Number: (609) 569-2624
Submission Date: 04/01/2021
SRMD Revision Number: 2.7
SRMD Revision Date: 04/01/2021

Approved By: REBECCA ELLEN GUY Digitally signed by REBECCA ELLEN GUY Date: 2021.06.11 18:03:26 -04'00'

Rebecca Guy
Director of Strategy, Mission Support Services, AJV-S

Date

Signature Page Five of Six

Title: Remote Tower Operational Safety Assessment (OSA)

Initiator: Shelly Beauchamp Project Lead
Initiator's Organization: Remote Tower Program
Initiator's Phone Number: (609) 569-2624
Submission Date: 04/01/2021
SRMD Revision Number: 2.7
SRMD Revision Date: 04/01/2021

Approved By: JEFFREY S SZCZYGIELSKI Digitally signed by JEFFREY S SZCZYGIELSKI Date: 2021.05.21 08:27:29 -04'00' 5/21/21

Jeffrey Szczygielski
Director, Operations Policy and Implementation
Directorate, AJT-2

Date

Signature Page Six of Six

Title: Remote Tower Operational Safety Assessment (OSA)

Initiator: Shelly Beauchamp Project Lead
Initiator's Organization: Remote Tower Program
Initiator's Phone Number: (609) 569-2624
Submission Date: 04/01/2021
SRMD Revision Number: 2.7
SRMD Revision Date: 04/01/2021

Approved By: GREGORY A PRAY Digitally signed by GREGORY A PRAY Date: 2021.07.02 08:55:16 -04'00'

Kimberly Pyle
Director, Policy and Performance, AJI-3

Date

TABLE OF CONTENTS

1. Introduction

The Operational Safety Assessment (OSA) is a process used to assess hazard severity. It establishes how safety requirements are to be allocated between air and ground components and how performance and interoperability requirements might be influenced. The OSA provides a disciplined method of objectively assessing the safety requirements of new National Airspace System (NAS) concepts and systems, typically for Communication, Navigation, and Surveillance (CNS) and Air Traffic Management (ATM) systems. The process used in developing this OSA is defined in *Safety Risk Management Guidance for System Acquisition* (SRMGSA) [Ref: *SRMGSA* and *Federal Aviation Administration (FAA) Safety Management System (SMS)*].

1.1. Operational Approval

The results of the OSA will allow the FAA to define safety requirements and objectives based upon the identified RT system functions, operational hazards, and the associated hazard severity classifications. During Type Certification, non-Federal system applicants must show that submitted designs have adequately accounted for all system safety hazards and that the design can meet or exceed the top-level safety requirements and objectives.

The Advisory Circular (AC) for Remote Tower (RT) Systems for Non-Federal applications will contain the FAA's Type Certification process, Air Traffic site approval process, commissioning process, and any requirements that the system owner will be responsible for, such as physical security and site-specific procedures. Some of these requirements will be determined based on safety requirements defined in this OSA. Technical requirements that the vendor is responsible to meet at a system level will be located in the Non-Federal Remote Tower Requirements document. The AC applies to all entities associated with the design, manufacture, procurement, installation, or maintenance of an RT system to provide Airport Traffic Control Tower (ATCT) services in Class D airspace in the NAS.

1.2. Background

An RT system may consist of one or more types of sensors and displays to provide the necessary visual information to Air Traffic Control Specialists (ATCS) to provide remote ATCT services. Sensors may include, but are not limited to, optical surveillance such as day/night cameras or infrared/thermal cameras. These sensors will be used to replace the information controllers presently gather by looking out the ATCT windows. The RT system, in conjunction with tower equipment listed in AC 90-93B, or the tower Minimum Equipment List (MEL) in Appendix A of JO 7210.78, is used to allow ATCS to provide for safe and efficient operations. Operations will be conducted as dictated by FAA Order JO 7110.65, *Air Traffic Control (ATC),* FAA Order JO 7210.3, *Facility Operation and Administration, FAA* Order JO 7210.78, *FAA Contract Tower (FCT) New Start and Replacement Tower Process* and AC 90-93B, *Operating Procedures for Airport Traffic Control Towers (ATCT) that are not operated by, or under the Contract with, The United States (non-Federal).*. Potentially, other supplementary non-required tower equipment may be present alongside the RT system.

1.3. Remote Tower OSA Panel List

The Operational Safety Assessment 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. Below is the list of panel members, stakeholders, and Subject Matter Experts (SMEs).

Table 1-1. OSA Panel Members

Name	Organization
Change Proponent	
Shelly Beauchamp	AJW-121
Randy Key	AJW-121
Panel Members	
Mitchell Bernstein	ANG-C52
Kimberly Brooks	AJV-S22
Lisa Caldwell	AJT-22
Jerry Crutchfield	AAM-500
Kurt Donnelly	PASS
Joe Foresto	AFS-800
Michael Poisson	AJV-P31
Adam Rhodes	NATCA
David Waudby	AJI-151
Subject Matter Experts	
Katie Berry	ANG-C52/Fort Hill Group
Shawn Casler	ANG-C32
Rick Cassell	ANG-C32/SEI
Kim Class	ANG-C32/SEI
Rebecca Collins	ANG-C52/Fort Hill Group
Alan Davis	AOV-250
John Dutton	ANG-C52
Gary Fiske	AJV-P31
Dave Ford	ANG-C52/CTR
Damien Gutberlet	ANG-C52/CTR
Rob Higginbotham	ANG-C52
Natashia Jones	AJW-121
Sabrina Karniej	ANG-C32/SEI
Amelia Kinsella	ANG-C52/Fort Hill Group
Andras Kovacs	ANG-C52
Rich Morrison	ANG-C52/CTR
Ricky Munoz	AOV-220
Dana Orr	AOV-120
Danielle Pagan	ANG-C5/CTR
Bianca Pickings	AJV-P31
Matthew Richardson	ANG-C52
Lori Smith	ANG-C52/Fort Hill Group
AnnMarie Taggio	AJV-P31
Ruben Velez	ANG-C32

Nathaniel Shumacker	AJT-221
Steve Young	AOV-140
Sarah Zak	AJV-P31
Facilitation Team	
Steven Barksdale	AJI-314
Charlotte Boyd	AJI-314 / GGTI
Martino Dennis	AJI-314
Rune Duke	AJI-314
Tara Scully	AJI-314 / GGTI

2. Operational Services and Environment Description (OSED)

The OSED captures elements that comprise a CNS/ATM system (e.g., aircraft equipage, air traffic service provider technical systems, communication service provider systems, and procedural requirements), and it includes the operational performance expectations, functions, and selected technologies of the CNS/ATM system. The OSED facilitates the formulation of technical and procedural requirements based on operational expectations and needs. Elements that comprise the OSED for RT Systems include the 5M Model, description of services reliant on RT Systems, description of the environment, assumptions, concept constraints, controls, generic architecture, and function definitions.

2.1. 5M Model

The 5M Model is used to capture the information needed to bound and describe the system and aid in the hazard identification process. The components of the 5M Model are: Mission, (hu)Man, Machine, Management, and Media.

Table 2-1. 5M Model

Mission: The clearly defined and detailed purpose of the NAS change proposal or system/operation being assessed	Provide ATCT services in Class D airspace through the use of an RT system in a Visual Flight Rules (VFR) tower environment - Services will be provided by ATCS utilizing the RT system in conjunction with items on the applicable MEL list
(hu)Man: Operators, maintainers, and affected stakeholders	- FAA-certified ATCSs - The flying public - Vehicles and/or pedestrians - Airport management - Non-federal technicians - Non-Federal RT system sponsors - FAA inspectors - ATC and Airspace - Overlying facilities - RT system vendors
Machine: Equipment used in the system	**RT System:**

	- An RT system is used by ATCS to provide ATCT services to an airport from a Remote Tower Center (RTC). The RTC can house multiple Remote Tower Modules (RTM) and may be on airport property or at a remote location. For this assessment, the FAA is not considering multiple RTMs at an RTC - The RTM includes components such as the required visual presentation, signal light gun, maintenance data terminal, data recorder functionalities, and ambient airfield audio transmission - All data transfer provided by a closed network **Other Equipment to be used with RT system:** MEL equipment outlined in AC 90-93B or FAA Order JO 7210.78 Appendix A.
Management: Procedures and policies that govern the system's behavior	- Applicable CFRs - Aeronautical Information Manual - FAA Order JO 7110.65, Air Traffic Control - FAA Order JO 7210.3, Facility Operation and Administration - FAA Order 6700.20, Non-federal Navigational Aids, Air Traffic Control (ATC) Facilities, and Automated Weather Systems - FAA Order 1900.47, Air Traffic Control Operational Contingency Plans - 14 CFR Part 91, General Operating and Flight Rules - Site-specific Standard Operating Procedures (SOPs) - Letters of Agreement (LOAs) - RT training and instruction booklets - FAA AC 90-93B, Operating Procedures for Airport Traffic Control Towers (ATCT) that are not Operated by, or Under Contract with, the United States (Non-Federal) - FAA AC: RT Systems for Non-Federal Applications

Media: The environment in which the system is operated/maintained	- System will be operated in the following environment: Single runway airport; Class D air traffic services; RTC located on or off airport property
	  - All data transfer must be on a closed network
	  - The RT system serves only one airport
	- RT system may be installed at a non-Federal Control Tower (NFCT) or a Federal Contract Tower (FCT)
	- RT system will be owned, operated, and maintained as a non-federal system
	- FAA will inspect the system and oversee the operations and maintenance of the system

2.2. Air Traffic Control Services

The services offered by ATCTs implementing RT systems in Class D airspace are listed below. These services will be made possible by a combination of the RT system, other equipment (e.g., MEL), and procedures in the facility.

Brick-and-mortar ATCTs operating in this environment may provide 1) tower-applied visual separation[1] and 2) opposite direction operations (ODO)[2]. ATCTs implementing RT systems are not currently authorized to provide these. Tower-applied visual separation is outside the scope of this OSA.

ODO may be conducted under non-routine circumstances to accommodate aircraft that have an operational need or are receiving operational priority; otherwise, ODO are outside the scope of this OSA.

Services that are out of scope of this OSA may not be authorized using RT systems without additional safety analysis prior to implementation.

2.2.1. Services to be provided by ATCTs implementing an RT system[3]

a. Ground Movement Services
    1) Manage Ground Movement
    2) Manage Ground Sequencing and Spacing
    3) Manage Runway Separation
    4) Manage Takeoff Information and Instructions
    5) Manage Takeoff Cancellation and Aborted Takeoff
    6) Manage Potential or Actual Ground Conflict
    7) Manage Flow Constraint/Traffic Management Initiative
b. Airborne Services
    1) Manage Overflight
    2) Manage Airborne Departure Including Pattern Airborne Departure
    3) Manage Arrival Including Pattern Arrival
    4) Manage Airborne Sequencing and Spacing[4]
    5) Manage Go Around and Missed Approach
    6) Manage Potential or Actual Airborne Conflict
    7) Manage Potential or Actual Airspace Violation
c. Weather Services
    1) Manage Weather and Severe Weather Condition Information
d. Special Operations, Emergency, and Unusual Situation Services
    1) Manage Unsafe Condition
    2) Manage Special Operation
    3) Manage Response to Uncontrolled Object/Aircraft
    4) Manage Emergency Response
    5) Manage Unusual Situation
e. Air Traffic-Pilot Communication Services
    1) Manage Radio Communication

[1] As defined in FAA Order JO 7110.65, Paragraph 7-2-1
[2] As defined in FAA Order JO 7210.3, Paragraph 2-1-34
[3] Ref: *FAA Order JO 7110.65; FAA Order JO 7210.3; Visual Job Analysis of Airport Traffic Control Towers*
[4] Visual information provided by the RT system cannot be the sole means of enabling this service for arrival/arrival/overflight tasks. Site-specific operating procedures must be defined to augment the RT systems' ability to enable this task (e.g., defined pattern entry procedures).

2) Manage Clearances, Instructions, or Information

f. Flight Plan Services
    1) Manage Flight Plan
    2) Manage Amended Flight Plan Data

2.3. Environment

The items below describe the operational environment in which the services are intended. The current environmental description is based upon where operational testing has taken place.

a. The RT System will be installed at an airport with airspace intended to be classified as Class D when the tower is in operation. The RT system may be operated in Class E or G airspace while the process of changing airspace classifications is underway.
    1) Class D airspace is generally airspace from the surface to 2,500 feet above the airport elevation (charted in Mean Sea Level (MSL)). The configuration of each Class D airspace area is individually tailored and when instrument procedures are published, the airspace will normally be designated to contain the procedures.

b. The RT System will be installed at an airport with a single runway operation.
    1) The runway length serviceable will be constrained by the RT vendor's design and siting criteria.
    2) RT vendors are responsible for defining and validating the environmental constraints in which the system will operate.

c. The RT System will be designed to operate in the following environments [Ref: FAA-G-2100]:
    1) The camera system will be installed in an "Outdoor Operating Environment" [paragraph 3.2.1.1.2].
        i. This can be specific to the intended airport environment.
    2) The display and control equipment will be installed in an "Indoor Operating Environment" [paragraph 3.2.1.1.3].

d. The RT System will serve only one airport.

e. The RT system may have components located on or off airport property (e.g. Required Visual Presentation (RVP)).

f. All RT system data transfer must be provided by a closed network.

2.4. Assumptions

The following assumptions relate the nominal operating conditions for the RT system. This includes equipment from the MEL (7210.78 Appendix A, AC 90-93B) and FAA Orders that dictate the expectations of ATCSs operating the system:

a. Each installed RT System will have an approved local safety case relative to the specific installation.

b. An appropriate RT Center SOP will be developed and in place.

c. Airport markings, signage, lighting, and security at airports providing ATCT services utilizing a RT system will meet or exceed FAA standards.

d. The RTM must permit for control positions to be consolidated to one control position and deconsolidated to multiple appropriate control positions.

e. It is assumed that the MEL equipment is functioning as intended.

2.5. Identified Controls

All of the following controls have been previously identified to exist in the NAS and have already been validated and verified as being effective.

2.5.1. Pilot Responsibilities

a. Abide by CFRs (Title 14 CFR Part 91, Title 14 CFR Part 121, Title 14 CFR Part 125, Title 14 CFR Part 135).

b. Operate aircraft safely, including the following examples:

- Be familiar with the operational requirements for each of the various types or classes of airspace (AIM, Section 3-1-1 and Chapter 3, Section 2).

- Maintain a safe taxi speed (AIM, Section 4-3-20).

- Exit a runway without delay after landing (AIM, Section 4-3-20).

- Taxi completely clear of the landing runway after landing (AIM, Section 4-3-20).

- Exercise vigilance and apply avoidance procedures in situations where responsible for avoiding wake turbulences (AIM, Chapter 7, Section 3).

- Operate so as to preclude disrupting traffic flows or creating conflicting patterns (unexpected maneuvers) (AIM, Section 4-3-5).

- Ensure safe takeoff and landing intervals when operating behind other aircraft (AIM, Section 7-3-8).

c. Maintain basic VFR weather minimums (AIM, Section 3-1-4).

d. Remain alert and in anticipation of all circumstances, situations, and conditions affecting the safe operation of aircraft (AIM, Sections 5-5-1, 5-5-8, and 7-5-1).

e. Continuously scan for other aircraft, vehicles, or other objects when operating on an airport. Apply see-and-avoid procedures as necessary (including on the ground). See and avoid other aircraft on the ground to avoid collision (AIM, Sections 4-3-18, 4 3-21, and 5-5-8).

   - Acceptance of instructions to follow another aircraft or to provide visual separation from it is an acknowledgement that the pilot will maneuver the aircraft as necessary to avoid the other aircraft or to maintain in-trail separation. Pilots are responsible to maintain visual separation until flight paths (altitudes and/or courses) diverge (AIM, Sections 5-5-8 and 5-5-12).

f. Evaluate and refuse ATC clearances that would place the aircraft in jeopardy or deviate from a rule or regulation.

   - Be aware of major bird migratory activity and current Notices to Airmen (NOTAMs) (AIM, Section 7-4-1).

   - Exercise extreme caution when warned of the presence of wildlife on and in the vicinity of airports (AIM, Section 7-4-5).

   - Report observed bird and wildlife hazards on or near a runway (AIM, Sections 7-4-4 and 7-4-5).

g. Maintain two-way radio communication between aircraft and an ATCT and comply with Title 14 CFR Part 91.129(d) in the event of radio failure.

   - Obtain approval prior to moving an aircraft on to the movement area (including the runway) (AIM, Section 4-3-18).

h. Recognize hazards involving debris, obstructions, surface vehicles, other aircraft, or airport personnel and take necessary actions to avoid hazards (AIM, Sections 4-3-17, 4 4-1, 4-4-14, 5-5-1, and 7-5-1).

i. Follow control instructions/clearances, report deviation from control instructions or expected maneuvers, and accurately report position when requested by ATC.

   - Obtain approval prior to moving an aircraft onto the movement area (AIM, Section 4-3-18).

   - Report position on the field when requesting taxi clearance (AIM, Section 4-3-18).

   - Refuse ATC clearance that would place the aircraft in jeopardy or deviate from a rule or regulation (AIM, Sections 4-4-1 and 5-5-1).

- Exercise vigilance and apply avoidance procedures in situations where responsible for avoiding wake turbulence to keep controllers and other pilots informed (AIM, Sections 4 4-14).

j. During emergencies, deviate from any rule in Title 14 CFR Part 91 to the extent required (AIM, Section 6-1-1).

k. Request assistance from ATC immediately if concerned for their safety for any reason (AIM, Sections 6-1-2 and 6-3-1).

l. Be alert for and in anticipation of all circumstances, situations, and conditions affecting the safe operation of the aircraft.

   - Be aware of weather information sources (AIM, Chapter 7, Sections 1 and 2).

   - Maintain awareness of current weather conditions, report current weather conditions and airport conditions to controllers and avoid severe weather (AIM, Sections 4 3 8 and 7-1-20 through 7-1-29).

   - Be familiar with all available information concerning the flight (e.g., pre-briefing including weather information and NOTAMS) (AIM, Chapter 7).

   - Be familiar with weather phenomena, reporting responsibilities, and potential impacts to safe operation of aircraft (AIM, Chapter 7, Sections 1 and 2).

   - Request current runway condition information if not issued by controllers (AIM, Sections 4-3-8 and 4-3-9).

   - Request lighting changes for safety, such as asking for runway edge light intensity to be adjusted (AIM, Section 2-1-8).

   - Report abnormal conditions such as sections of unlit taxiways or an airport rotating beacon out of service (AIM, Section 7-1-20).

m. Recognize and adhere to airport markings and signs (AIM, Section 2-3-1).

2.5.2. Airport Personnel Responsibilities

a. See and avoid vehicles and aircraft (FAA Guide to Ground Vehicle Operations).

b. Operate safely when on the airport, follow ATC instructions, and remain clear of the movement area including runway / runway safety area until receiving a clearance to proceed (FAA Guide to Ground Vehicle Operations).

c. Report any known or observed aviation hazards to air traffic controllers (FAA Guide to Ground Vehicle Operations)

d. Maintain awareness of current airport/runway conditions, including lighting outages, and report those to all concerned parties (FAA Guide to Ground Vehicle Operations, AC 150/5340-26, Maintenance of Airport Visual Aids; FAA Order 5280.5, Airport Certification Program Handbook; and FAA Order 5190.6, FAA Airport Compliance Manual).

e. Maintain published NOTAMs as required and provide airport condition information to all concerned parties (FAA Guide to Ground Vehicle Operations; AC 150/5210-24; AC 150/5370-2G, Operational Safety on Airports During Construction; and AC 150/5200-33C, Hazardous Wildlife Attractants On or Near Airports).

f. Pick up any observed Foreign Object Debris (FOD) on the airport property and avoid tracking mud or rocks on to the movement area (FAA Guide to Ground Vehicle Operations and AC 150/5210-24, Airport FOD Management).

g. Maintain and operate the airport in accordance with 14 CFR Part 139 and AC 150/4200.

2.5.3. ATCT Controller Responsibilities

a. Provide ATC services to prevent collision involving aircraft operating in the system and provide a safe, orderly, expeditious flow of air traffic.

- Operate lights in accordance with sunrise/sunset times and visibility conditions as requested by pilots and as deemed necessary (if not contrary to pilot request) (FAA Order JO 7110.65, Chapter 3, Section 4; and FAA Order JO 7210.3, Chapter 10, Section 6).

- Issue specific instructions in concise, easy-to-understand terms, which approve or disapprove the movement of aircraft, vehicles, equipment, or personnel on the movement area (FAA Order JO 7110.65, Chapter 3, Section 7).

- When needed to accommodate aircraft that have an operational need or are receiving operational priority, adhere to Opposite Direction Operations (ODO) criteria (FAA Order JO 7210.3BB, Paragraph 2-1-34).

b. Monitor radio frequencies (FAA Order JO 7110.65, Paragraph 2-4-2).

c. Be familiar with pertinent weather information and stay aware of current and forecasted weather information (FAA Order JO 7210.3, Paragraph 2-9-2 and FAA Order JO 7210.65, Paragraph 2-6-1).

d. Maintain situational awareness of current airport/runway conditions, planned changes to airport runway conditions, NOTAMs, and special activities (FAA Order JO 7110.65, Paragraphs 2-6-1, 2-6-2, 2-10-3, and 3-3).

e. Solicit and issue PIREPs about airport conditions and weather (FAA Order JO 7110.65, Paragraphs 2-6-2 and 3 3-5).

f. Provide information of use to airport management and pilots. This includes weather and airport conditions observed, known through pilot reports, reports from airport personnel, and NOTAMs (FAA Order JO 7110.65, Paragraphs 2-6-3, 2-6-5, 2 6-6, 3-3-3, and 3-3-4).

g. Apply separation standards for same runway separation (FAA Order JO 7110.65, Paragraphs 3-9-6, 3-10-3, 3-11-3, and 3-11-4).

h. Provide separation between an Instrument Flight Rules (IFR) departing aircraft and an IFR arriving aircraft (FAA Order JO 7110.65, Chapters 3, 5, and 6).

i. Issue advisories of all known traffic and wildlife that may interfere with aircraft operations (FAA Order JO 7110.65, Paragraphs 2-1-21, 2-1-22, 3-3-1, 3-3-3, and 3-3-4).

j. Issue advisories of known FOD to pilots and airport personnel (FAA Order JO 7110.65, Paragraphs 3-3-1 and 3-3-3).

k. Respond to known or observed abnormal aircraft conditions (FAA Order JO 7110.65, Paragraphs 3-1-10 and 3-3-3).

l. Ensure aircraft/vehicles do not cross the runway holding position markings when necessary (FAA Order JO 7110.65, Paragraph 3-7-2).

m. Adhere to the facility operational contingency plan (FAA Order JO 1900.47).

2.5.4. Overlying Facility Radar Controller Responsibilities

a. Provide ATC services to prevent collision involving aircraft operating in the system and provide a safe, orderly, expeditious flow of air traffic.

- Ensure that necessary coordination has been accomplished before allowing an aircraft to enter another controller's area of jurisdiction (FAA Order JO 7110.65, Paragraph 2-1-14).

- Issue specific instructions in concise, easy-to-understand terms (FAA Order JO 7110.65, Chapter 3).

- When needed to accommodate aircraft that have an operational need or are receiving operational priority, adhere to ODO criteria (FAA Order JO 7210.3BB, Paragraph 2-1-34).

b. Provide separation services as applicable. Apply merging target procedures.

- Provide separation services for radar arrivals (FAA Order JO 7110.65, Paragraph 5-9-5).

- Provide separation between an IFR departing aircraft and an IFR arriving aircraft (FAA Order JO 7110.65, Chapter 6).

2.5.5. Other NAS Controls

a. FAA Technical Operations will manage non-fed equipment per FAA Order 6700.20, Non-federal Navigational Aids, ATC Facilities, and Automated Weather Systems

b. FAA Orders mandate that the maintenance and operation of non-federal navigational aids is in accordance with 14 CFR Parts 170 and 171.

2.6. Generic RT System Architecture

An RT system is used by ATCS to provide ATCT services to an airport from an RTC. The RTC can house multiple RTMs and may be on airport property or at a remote location. For this assessment, the FAA is not considering multiple RTMs at an RTC. The RTM includes components such as RT visual presentation, system control functions, and controller working positions. The RTM is connected to equipment located at the airport, including optical sensors and ancillary equipment.

The “RT system” only refers to the equipment described in Figure 2-1 below; it does not include any MEL or other FAA equipment.

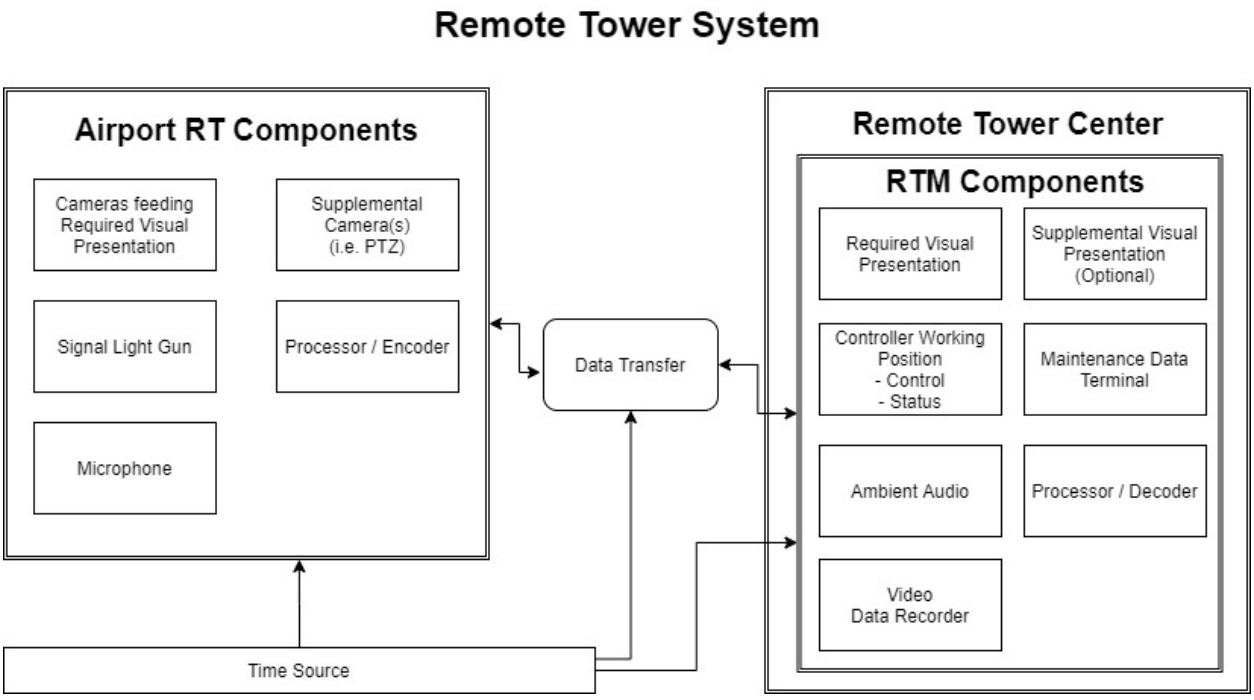

Figure 2-1. Generic RT System Architecture

2.7. RT System Functions

The following subsections define the genericized functions that each RT system is expected to provide. Figure 2-2 illustrates the divide between the functions associated with the RT system, the services it provides, and the external interactions on the system.

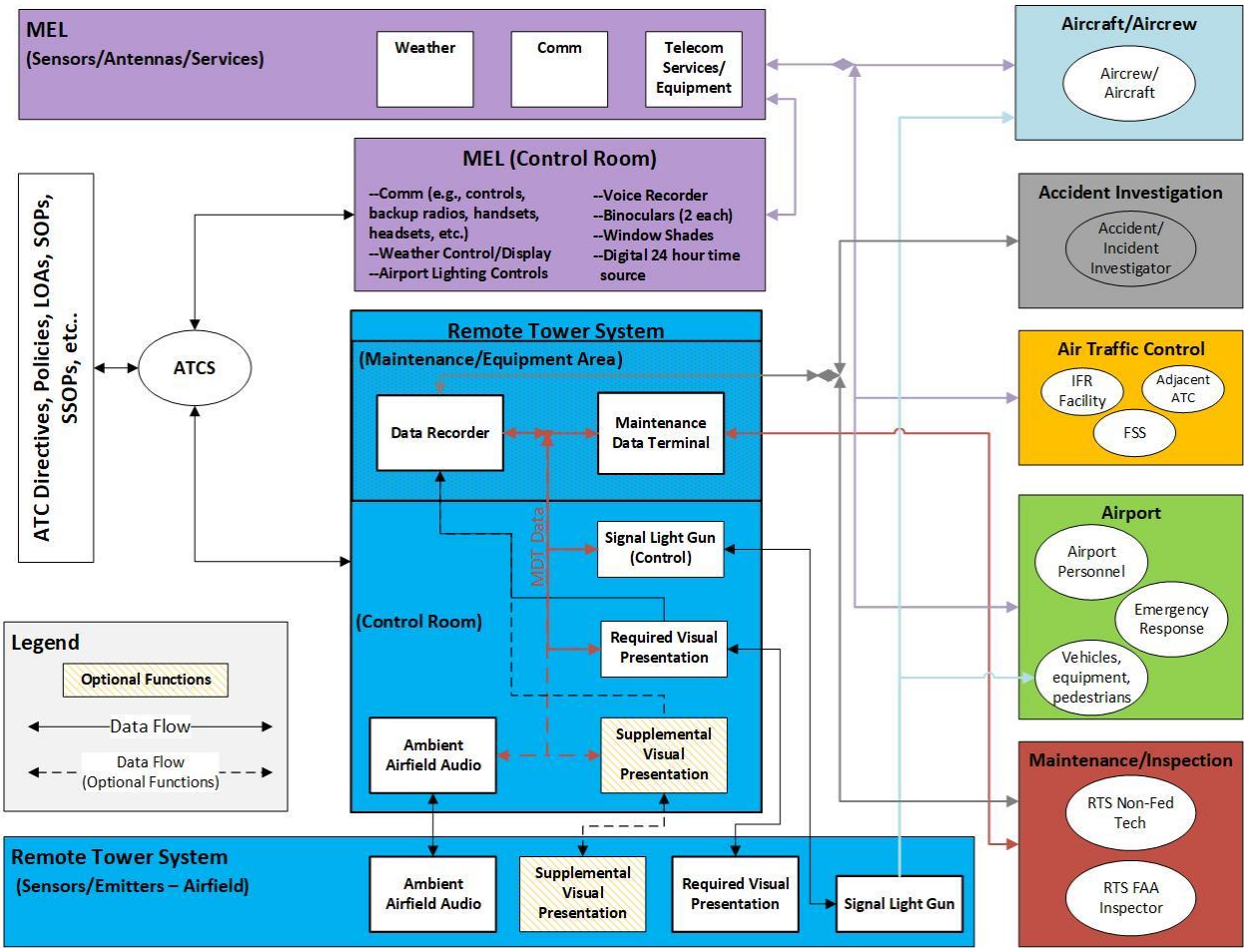

Figure 2-2. Functional Block Diagram

2.7.1. Function Definitions

Table 2-2. Function Definitions

Function	Description
Required Visual Presentation (RVP) (Required)	The RVP function includes all visual presentations necessary to meet V1.0 of the Operational Visual Requirements (OVRs). A continuous fixed 360 degree view of the airfield and surrounding airspace must be provided. Note: OVRs identified as primary must be met on the fixed continuous 360-degree presentation. OVRs identified as secondary can be met either with the fixed continuous 360-degree presentation or with an augmented presentation. Functional chain (sub-functions) also includes:

	- RVP Control Functionality that allows ATCS to control any system components impacting the RVP of the RT system. (Note: This may include environmental controls and redundancy management.) - System Monitoring & Status Functions Functionality built into the system to detect and annunciate failed or degraded components in the RVP chain. (e.g., latency monitoring, redundancy alerts, frozen image alerts, etc.)
Signal Light Gun (SLG) (Required)	Functionality required to visually communicate with aircraft pilot, equipment operator, vehicle operator, or pedestrians. (Note: Equivalent function to SLG on MEL for conventional towers.) This includes: - Aiming at and following an object of concern/interest (e.g., aircraft, vehicle, equipment, or pedestrians) and signaling as appropriate. - Any built-in system functionality (if provided) to monitor/detect and annunciate failure or degradation of components in the SLG functional chain.
Maintenance Data Terminal (MDT) (Required)	Functionality required to facilitate installation and maintenance: This includes functionality to perform: - System configuration setup and updates (e.g., software updates, network configuration updates, configurable parameter setup/modifications, modify/view adaptation data, etc.), - Maintenance activities (i.e., diagnostics, corrective maintenance, calibration, troubleshooting, Built-In-Test, etc.). - Viewing and retrieving of stored system data such as resources, faults, warnings, system errors, event logs, and networking information. Note - Engineers and technicians are the primary users of this function; this function is not intended for ATCS use.
Data Recording (Required)	Functionality required to record visual data for playback (i.e. video, fault/failure annunciations, timestamp). This includes:

	- The functionality to record the information provided on the Required and Supplemental (if provided) Video Presentations. - Controls for the data recording functionality (e.g., configure/setup recording parameters). - System functionality to detect and annunciate failure or degradation of Data Recording components. Note: This functionality is required for accident investigation purposes. This function may also support installation checkout/verification and maintenance activities.
Supplemental Visual Presentation (Optional)	The Supplemental Visual Presentation function includes any and all auxiliary visual presentations or enhancements (e.g., overlays, box-and-track, zoom functionality, additional cameras/views) that are intended to provide additional situational awareness but are NOT required to meet the OVRs (as defined in V1.0). Functional chain (sub-functions) also includes: - Supplemental Visual Presentation Control Functionality that allows ATCS to control any system components impacting the Supplemental Visual Presentation of the RT system. - System Monitoring & Status Functions Functionality built into the system to detect and annunciate failed or degraded components in the Supplemental Visual Presentation chain (e.g., latency monitoring, redundancy alerts, etc.) Binoculars are a MEL item for brick-and-mortar towers. The equivalent functionality can be provided in a RT system in at least three different ways: - Provide physical short focal length binoculars. - An enhanced/augmented presentation provided on the Required Video Presentation or a Supplemental Video Presentation (e.g., a zooming and scanning capability displayed as a video presentation).
Ambient Airfield Audio (AAA) Output (Required)	Functionality to transmit AAA to the ATCS. This includes:

	- Functionality required to install, setup, and confirm the proper operation of the AAA (e.g., view/modify configuration parameters). - Any volume or other controls associated with AAA use. - Functionality built into the system to detect and annunciate failed or degraded components in the Audio Output chain.

3. Operational Hazard Assessment (OHA)

The OHA is a qualitative assessment of the operational hazards associated with the OSED. For the OHA, services are examined to identify and classify hazards that could adversely affect those services. Hazards are classified according to a standardized classification scheme based on hazard severity, taking into account human factors.

Qualitative and/or quantitative safety objectives are established to address the operational hazard classifications.

3.1. Causes of Preliminary Hazards

For the purposes of this OHA, three classifications of failures have been identified to evaluate the hazards listed in section 3.3. Loss of function and malfunction failure categories have been adopted from the ATO SMS Manual in Table 3.4 NAS Equipment Worst Credible Severity Table utilizing the Surveillance Service (e.g., STARS, ARTS, etc.). Although these failures have been adopted from Table 3.4, the associated Worst Credible Severity may or may not be applicable to camera surveillance being used in a VFR tower environment, given the severities in Table 3.4 were based on surveillance sources listed in the ATO SMS (section 3.5.4.2.1). In other words, the hazard severity classifications will be determined by also assessing these failures against the effects in the ATC Services in Table 3.3 Severity Table in the ATO SMS Manual. Partial loss of function was also identified as a failure classification from DO-264. In certain circumstances, the RT system can experience a partial loss of function and still remain useable until the Controller in Charge (CIC) deems it necessary to declare ATC-Zero.

a. Loss of Function (LoF) - The function is no longer provided. Examples would be a total loss of any function such as the required visual presentation, signal light gun, ambient audio, etc.

b. Partial Loss of Function (PLoF) - Failure resulting in the degradation of a function, generating improper output. Examples would include the loss of a portion of the visual presentation, a reduction in the display resolution, etc.

c. Malfunction (MALF) - A malfunction occurs when a function is providing false or misleading information to the user. Examples of a malfunction includes frozen screens, asynchronous rendering of images (e.g., display screens aren't synchronous), a lag in the monitors or audio output, etc.

3.2. Hazard Severity Classification

Each operational hazard is classified according to the severity of its identified effects using an OHA. The OHA is developed as described in the SRMGSA, Table C.1. To determine hazard severity:

a. Assess the effects of the hazard on operations considering the effects on the aircrew, air traffic services, and the aircraft occupants.

b. Shared mitigation strategies within the CNS/ATM system being introduced and assessed should not be used to lower the hazard class at the service level.

c. The severity of each hazard is determined by the worst credible outcome or effect of the hazard on the solution or the NAS [Ref. SRMGSA, 5.2.7].

3.3. Preliminary Hazards

The hazards that have been assessed are only related to required functions. Hazards associated with supplemental or optional functions will be addressed during the Type Certification review process when specific applicant architectures are proposed.

3.3.1. Required Visual Presentation Hazards

These functional hazards relate to the system's ability to provide visual information to the controller, such that the controller can visually detect, verify, and observe traffic or other objects, the relative distance between objects, and recognize and identify further characteristics and details.

This functionality is provided by the RVP function and sub-functions. The minimum functionality of the RVP is described in the draft OVRs (V1.0.).

- **RVP-LoF-1** - Partial or total loss of the capability to detect and identify objects in the area of jurisdiction (i.e., runways, short finals, and base turns).

- **RVP-LoF-2** - Partial or total loss of capability to observe spatial relationships in the area of jurisdiction.

- **RVP-PLoF-1** – Partial loss of the capability to detect and identify objects and observe spatial relationships in non-essential / non-critical areas.

- **RVP-MALF-1** - Hazardously Misleading Information (HMI) provided to ATCT controller: Relative spatial relationship between objects on different physical presentations will be incorrect (i.e., asynchronous presentations/displays).

- **RVP-MALF-2** - HMI provided to ATCT controller: Presented visual information is not real-time: consistent time lag in all monitors.

- **RVP-MALF-3** - HMI provided to ATCT controller: Presented visual information is not real-time: presentation of frozen visual information.

3.3.2. Signal Light Gun Hazards

These hazards relate to the system's ability to provide the same functionality that the MEL Signal Light Gun provides. This functionality is provided by the Signal Light Gun function.

- **SLG-LoF-1** - Inability to provide visual signals to aircraft, vehicles, or personnel (SLG Loss of Function).

- **SLG-MALF-1** – SLG visual signal is unable to point/track.

- **SLG-MALF-2** - Incorrect visual signal (i.e., incorrect color pattern / sequence) provided to at least one aircraft, vehicle, or personnel.

- **SLG-MALF-3** - Unintended visual signal provided to aircraft, vehicles, or personnel during operation (i.e., no visual signal was intended to be transmitted).

- **SLG-MALF-4** - Unintended visual signal provided to aircraft, vehicles, or personnel during system installation, setup, or checkout.

3.3.3. Ambient Airfield Audio Hazards

These hazards relate to the system's ability to provide AAA to the controller for situational awareness.

- **AAA-LoF-1** – Total loss of ability of ATCS to hear AAA.

- **AAA-PLoF-1** - Failure of individual audio microphone and/or speaker. This results in inability of ATCT to hear AAA from section of airfield.

- **AAA-MALF-1** - AAA isn’t provided in "near real time" (e.g. delayed, out of synchronization with correct visual information, etc.). This results in misleading information provided to ATCT.

- **AAA-MALF-2** - AAA is not spatially representative of reality (e.g. engine noise from the south appears to be coming from the north). This results in misleading information provided to ATCT.

- **AAA-MALF-3** - AAA quality or volume creates a distraction (e.g. volume stuck high, excessive noise, etc.).

3.3.4. Maintenance Data Terminal Hazards

These hazards relate to the system’s ability to allow for maintenance activities, including loading of new software, setup of configurable components, and system restarts. This functionality is provided by the MDT Function.

- **MDT-LoF-1** - Inability to view system status information or control system via the MDT interface.

- **MDT-LoF-2** - Loss of system availability due to lack of MDT capability to transition system into operational mode.

- **MDT-MALF-1** - Loss of system availability during operations.

- **MDT-MALF-2** - Loss of system integrity during operations due to a malfunction during system installation, setup, or checkout.

- **MDT-MALF-3** - Loss of system availability due to a malfunction during system installation, setup, or checkout.

- **MDT-MALF-4** - Loss of system integrity during system installation, setup, or checkout.

3.3.5. Data Recorder Hazards

These hazards relate to the system’s ability to record the live video from the RVP and supplementary cameras for replay purposes. This functionality is required for accident investigation purposes and may also be used for maintenance activities.

- **DR-LoF-1** - Loss of the capability to record (and subsequently replay) the required video presentation used by ATC.

- **DR-MALF-1** - Misleading, inaccurate, and/or unusable required video presentation recordings.

3.4. Final Hazards and Deliberation Notes

3.4.1. Required Visual Presentation Hazards

These functional hazards relate to the system's ability to provide visual information to the controller, such that the controller can visually detect, verify, and observe traffic or other objects, the relative distance between objects, and recognize and identify further characteristics and details.

This functionality is provided by the RVP function and sub-functions. The minimum functionality of the RVP is described in the draft OVRs (V1.0.).

- **RVP-LoF-1 -** Partial or total loss of the capability to detect and identify objects / observe spatial relationships in the area of jurisdiction (i.e., runways, short finals, and base turns)

    - **Discussion** – The preliminary hazards RVP-LoF-1 and RVP-LoF-2 were presented to the OSA Panel. The panel determined that these two hazards should be combined, as it was not possible to lose one capability without the other in the event of a loss of RVP function. This resulted in the final version of RVP-LoF-1 that is shown here, and in the HA. RVP-LoF-2 was removed from the final OSA and does not appear in the HA.

      The critical portion of the RVP contains the runway, short final, and base turn sections of the airport. The need to define this area on a site-by-site basis was captured as a safety requirement. The panel determined that the critical exposure time to this hazard was the time it would take to completely transition to an ATC-Zero situation, which was estimated to be 60-120 seconds depending on the specific circumstances present at the time of the LoF. Hazards present after this transition to ATC-Zero was complete were determined to be out of the scope of this OSA, as ATC-Zero is a condition present in the NAS today and not unique to facilities using RT systems.

      Significant discussion occurred around this hazard over the course of multiple workgroup and full panel meetings, with much debate between an assignment of minor or major severity. The hazard severity was assessed based on the effects on ATC Services, NAS Equipment, and Flight Crew listed in the ATO-SMS Table 3.3: Severity Table. The original panel vote results were seven to two for minor severity. After an additional panel meeting held to allow NATCA and PASS to further explain their rationales for believing the hazard severity to be major, the votes shifted to a five to four majority in favor of a major hazard severity.

      Proponents of a minor severity assignment for this hazard pointed out several key interventions and mitigations that would be present in this environment. These included use of a pad of call signs, aircraft types, and flight details, the ability to immediately cancel all landing clearances, and the ability to use radio communications to inform all area traffic of the loss of function and to stop all

ground traffic. A key control sited in the argument for a minor severity assessment was the see-and-avoid responsibility of pilots in a VFR tower environment.

Proponents for a major severity note that this LoF is not equivalent to the transition to ATC-Zero in a brick-and-mortar tower due to the instantaneous total or near total loss of visual information in the remote tower case. Some panelists compared this scenario to the loss of radar in a radar environment, but others felt that this was too stringent a comparison for a VFR tower.

A follow up panel meeting was held on October 14, 2020 to allow the two panelists who had originally believed the severity was major to further make their cases. The proponents for a major severity assessment maintained that the starting points for Table 3.3 and Table 3.4 in the SMS manual fit a major severity, which can result in events such as a large increase in ATC workload, significant reduction in safety margin, a CAT B runway incursion, or a rejected landing at or near the threshold. The use of Table 3.4 (NAS Equipment/Surveillance) was another point of disagreement between the panel members. As RT technology is a new concept, Table 3.4 in the SMS manual does not address RT services explicitly and may be more tailored to IFR/radar services. Some panel members contended Remote Tower Functionality MUST be assessed utilizing the Surveillance service criteria of Table 3.4, until the SMS is updated to definitively capture the service provided by Remote Tower Systems.

The scenario described that led to the major severity assessment is as follows: An aircraft is on final approach and another aircraft is holding short that has been cleared for takeoff. At this time the RVP function is lost. The controller is not able to see if/when the departing aircraft actually begins to move and therefore cannot intervene when the aircraft rolls past the hold short line onto the runway. The lack of controller intervention could contribute to a runway incursion. In this scenario, a Category B Runway Incursion and/or rejected landing at or near the threshold could occur if the approaching pilot does not detect the ground aircraft prior to passing the threshold. Proponents for a Minor severity assessment argued that the remote tower is a VFR tower and pilots practice see-and-avoid procedures Pilots scan the landing runway area, and if they see an aircraft rolling onto their landing runway, they will announce their observation on the tower frequency, and as deemed necessary, execute a go-around. Pilot controls listed in section 2.5.1 are validated and verified controls that reduce the likelihood of this scenario from occurring.

Panel members advocating for a major severity assessment felt that there were no credible examples that can be used in the NAS today where a controller loses all visibility instantaneously. The case was made that many of the suggested controls (for instance, SOPs on controller actions in the event of a LoF) were not assessed in the NAS, and therefore could not be verified as effective. It was suggested that controls listed are unverified requirements of how controllers should react when a loss of function occurs.

Details of the considered effects are shown in the HA table. No dissenting opinions are included in this document, as the panel eventually voted in favor of a Major severity assessment. The final panel votes for this severity assessment were very close, and are summarized in the table below. The five-to-four vote for a Major severity assessment when considering the effects of a loss of function on the flight crew drove the final assessment to be Major. It should be noted that the panel member from Flight Standards voted for a Minor severity.

Table 3-1. SRM Panel Deliberations

Panel Member's Organization	Effects on Flight Crew	Effects on ATC Services	Effects on NAS Equipment
Mitchell Bernstein (ANG-C52)	Minor	Minor	Minor
Kimberly Brooks (AJV-S22)	Minor	Minor	Minor
Lisa Caldwell (AJT-22)	Minor	Minor	Minor
Jerry Crutchfield (AAM-500)	**Major**	Minor	Minor
Kurt Donnelly (PASS)	**Major**	Minor	**Major**
Joe Foresto (AFS-800)	Minor	Minor	Minor
Michael Poisson (AJV-P31)	**Major**	**Major**	**Major**
Adam Rhodes (NATCA)	**Major**	**Major**	**Major**
David Waudby (AJI-151)	**Major**	**Major**	**Major**

- **Severity Assessment** – Major

- **RVP-LoF-2 -** Partial or total loss of capability to observe spatial relationships in the area of jurisdiction.

  - **Discussion –** The preliminary hazard RVP-LoF-2 was combined with RVP-LoF-1 after panel consideration. RVP-LoF-2 is not included in the final OHA.

- **RVP-PLoF-1** – Partial loss of the capability to detect and identify objects and observe spatial relationships in non-essential / non-critical areas.

    - **Discussion -** The panel determined that the partial loss of the capability to detect and identify objects and observe spatial relationships in non-essential / non-critical areas has a severity effect of minimal. This assessment was unanimous, with no dissenting opinions. It was again noted that critical areas of the RVP should be defined during installation on a site-by-site basis; this has been captured as a safety objective, as has the need for developing procedures to follow if "non-critical/non-essential" presentation areas suffer a LoF/PLoF. With these requirements in place, the panel determined there would only be a slight increase in ATC workload. Contributing to this assessment was work done at the JYO Remote Tower test site, which indicated that the system could continue to offer air traffic services during such a failure for a period of up to four hours, which suggests minimal impact of a failure of this nature on operations. (Note: This is not intended to drive a global requirement for all RTs to operate for up to four hours after this failure condition.)

    - **Severity Assessment** – Minimal

- **RVP-MALF-1** - Hazardously Misleading Information (HMI) provided to ATCT controller: Relative spatial relationship between objects on different physical presentations will be incorrect (i.e., asynchronous presentations/displays).

    - **Discussion** – The panel determined that a misinterpretation of visual information should have a severity rating of major. This hazard led to considerable discussion that occurred over several working group and full panel meetings. It was noted that the specific effects of this malfunction case may vary based on the specific malfunction presented, an applicant's design (e.g. the number of presentation screens used, number impacted by the malfunction, the relative amount of lead/lag time), and the system state at the time of the malfunction (e.g. the number of aircraft in the pattern, relative proximity of aircraft to one another, etc). It was noted that an otherwise un-annunciated malfunction may be detectable if ATCS notices the same aircraft/vehicle on multiple screens at the same time. It was recommended that a safety requirement be generated to develop SOPs to establish a predefined ATCS reaction to apparent malfunctions.
      SMEs noted several key concerns regarding this failure mode. These included:
        - The potential to clear someone for landing and/or takeoff when the ATCS thought they had greater separation than actually exists,
        - An aircraft is holding short on a taxiway; lag occurs such that the aircraft has moved onto runway and display does not show this,
        - Various scenarios involving approach end activity when this end is impacted by a screen or set of screens that has malfunctioned.

      Panelists and SMEs did note that the ATCS may be alerted to this malfunction by a pilot over 2-way radio communication, by the unanticipated maneuver of a pilot, or by other human-in-the-loop means. However, there was also concern that pilots

would heed the advice of ATC until the last possible moment before making a different decision, as pilots would generally assume that the ATC tower had integrity in their visualization.

In general, it was agreed that controllers are making decisions and providing instruction based on what they see, and that a loss of separation due to misleading information of this nature was possible. Details of the anticipated effects of this malfunction are included in the HA.

- **Severity Assessment** – Major

- **RVP-MALF-2 -** HMI provided to ATCT controller: Presented visual information is not real-time: consistent time lag in all monitors.

  - **Discussion -** The panel determined that this hazard should have a severity rating of major; this decision was unanimous. Discussions occurred over the span of several work groups, with key discussion points mirroring those noted under RVP-MALF-1. Details of determined effects are included in the HA table.

  - **Severity Assessment** – Major

- **RVP-MALF-3 -** HMI provided to ATCT controller: Presented visual information is not real-time: presentation of frozen visual information.

  Discussion - The majority of panel assessed the severity associated with this hazard as Major; the ANG-C5 panel member dissented, stating the severity should be assessed as Minor. In general, panelists and SMEs felt that this malfunction would be detectable by the ATCS within a relatively short period of time based on visual cues. These might include discrepancies between airfield audio and the presentation, discrepancies between two-way radio communications and the presentation, and non-continuous presentations (e.g. discrepancies between adjacent presentation screens). It was also noted that these discrepancies may be less noticeable by the ATCS when there was less ambient light. Additionally, it was noted that this malfunction would be more noticeable at busier airports, or at airports adjacent to busy airports, due to the near continuous stream of traffic appearing on the RVP. Depending when and where the screen freezes ATC can potentially place two aircraft on the runway at the same time.

  The panel discussed the following scenario which would lead to a potential Category B runway incursion: There is an aircraft on final approach and an aircraft holding short that was cleared for takeoff. The RVP (partial or total) freezes and the controller does not notice the screen is frozen, causing the departing aircraft to appear to still be holding short. By the time the situation is observed by the controller and cancels the takeoff clearance, a Category B Runway Incursion could occur.

Due to the presumed detectability of this malfunction case by the ATCS, during workgroup discussion several panelists and SMEs initially felt that the severity of this hazard should be assessed to be equivalent to the RVP-LoF-1 case. However, after further discussion at the full panel level, the consensus was for an assessment of Major severity, consistent with other RVP malfunction cases, with the single dissenting vote noted.

- **Severity Assessment** – Major

- **Dissenting Opinion** – See Appendix E

3.4.2. Signal Light Gun Hazards

These hazards relate to the system's ability to provide the same functionality that the MEL Signal Light Gun provides in a brick and mortar tower. This functionality is provided by the Signal Light Gun function.

- **SLG-LoF-1** - Inability to provide visual signals to aircraft, vehicles, and personnel (NORDO present).

    - **Discussion** - The panel determined that the effect of this LoF would be a slight increase in ATC workload, as ATC will need to conduct extra coordination with other traffic to accommodate the NORDO aircraft that cannot be communicated with via the SLG. A need for requirements for the ATCS to be able to confirm that the SLG was operating properly (e.g. see/test the emitted signal) and determine the on/off status of the SLG was noted; these were captured as Safety Objectives. The panel unanimously assessed this hazard as having a minimal severity.

    - **Severity Assessment** – Minimal

- **SLG-MALF-1** – SLG visual signal is unable to point/track accurately.

    - **Discussion** - The panel considered this malfunction case to be equivalent in effect to SLG-LoF-1. They unanimously assessed the severity of this hazard as Minimal.

    - **Severity Assessment** – Minimal

- **SLG-MALF-2** - Incorrect visual signal (i.e., incorrect color pattern / sequence) provided to at least one aircraft, vehicle, or personnel.

    - **Discussion** – Panel discussion on this hazard noted the increased attention the ATCS places on the target of the SLG, such that a reaction to an incorrect signal would be quickly observed. The panel unanimously determined the outcome of this

hazard has a Minimal severity, due to the slight increase in ATC workload associated with this malfunction.

- **Severity Assessment** – Minimal

- **SLG-MALF-3** - Unintended visual signal provided to aircraft, vehicles, or personnel during operation (i.e., no visual signal was intended to be transmitted).

    - **Discussion** – The panel did not believe that an unintended SLG signal would go unnoticed and/or unreported for long enough to drive effects that would lead to an operational hazard. SLG-MALF-3 was removed from the final OHA.

- **SLG-MALF-4** - Unintended visual signal provided to aircraft, vehicles, or personnel during system installation, setup, or checkout.

    - **Discussion** – The panel did not believe that an unintended SLG signal would go unnoticed and/or unreported for long enough to drive effects that would lead to an operational hazard. SLG-MALF-4 was removed from the final OHA.

3.4.3. Ambient Airfield Audio Hazards

These hazards relate to the system's ability to provide AAA to the controller for situational awareness.

- **AAA-LoF-1** – Total loss of ability of ATCS to hear Ambient Airfield Audio (AAA).

    - **Discussion** – The panel discussed the use of ambient audio in brick-and-mortar towers. The OSA Panel felt that AAA function provided additional situational awareness, but is not essential to provide ATC service. Ambient Audio is not a requirement in today's NAS; there are no requirements associated with siting a brick-and-mortar tower to ensure adequate ambient audio to the ATCS. The panel determined that Ambient Audio does provide additional situational awareness to ATC that aircraft on the field may be starting up, taxiing, taking off/landing or in the traffic pattern, but that this is not an essential element to provide Air Traffic Services. The panel unanimously determined that the loss of AAA would cause a slight decrease in ATC Situational Awareness, leading to a Minimal severity assessment. This determination is in line with findings from the JYO remote tower test site that indicated that air traffic services could continue to be offered indefinitely after a failure of the ambient audio component.

    - **Severity Assessment** – Minimal

- **AAA-PLoF-1** - Failure of individual audio microphone and/or speaker. This results in inability of ATCT to hear ambient audio from a section of airfield.

- **Discussion** – The panel determined that a partial loss of function of the AAA would be no worse than the full loss assessed under AAA-LoF-1. The panel unanimously determined this hazard to have a Minimal severity due to the slight decrease in ATC Situational Awareness.

- **Severity Assessment** – Minimal

- **AAA-MALF-1** – Ambient Airfield Audio (AAA) isn't provided in "near real time" (e.g. delayed, out of synchronization with correct visual information, etc.). This results in misleading information provided to ATCT.

    - **Discussion** - The panel unanimously determined this hazard to have a Minimal severity. This assessment was based on the "slight increase in ATC workload" as controllers react to lagging or otherwise asynchronous audio and most likely move to disable/reduce the sound.

    - **Severity Assessment** – Minimal

- **AAA-MALF-2** – Ambient Airfield Audio (AAA) is not spatially representative of reality (e.g. engine noise from the south appears to be coming from the north). This results in misleading information provided to ATCT.

    - **Discussion** - The malfunction of AAA will result in a "slight increase in ATC workload" as controllers become aware of and react to spatially misleading audio and most likely move to disable/reduce the sound. The panel unanimously determined that this hazard is of a Minimal severity.

    - **Severity Assessment** – Minimal

- **AAA-MALF-3** – Ambient Airfield Audio (AAA) quality or volume creates a distraction (e.g. volume stuck high, excessive noise, etc.).

    - **Discussion** - This malfunction of AAA will result in a "slight increase in ATC workload" as controllers react to the distraction and most likely move to disable/reduce the sound. The panel unanimously determined that this hazard is of Minimal severity.

    - **Severity Assessment** – Minimal

3.4.4. Maintenance Data Terminal Hazards

These hazards relate to the system's ability to allow for maintenance activities, including loading of new software, setup of configurable components, and system restarts. This functionality is provided by the MDT Function.

- **MDT-LoF-1** - Inability to view system status information or control system via the MDT interface.

    - **Discussion** - This LoF case was determined to have no operational impact. MDT-LoF-1 was removed from the final OHA.

- **MDT-LoF-2** - Loss of system availability due to lack of MDT capability to transition system into operational mode.

    - **Discussion** – The effect of this LoF case is an inability to transition the system into operation, from a previously non-operational state. This may lead to an inability to return the RT to service, but will not lead to the loss of existing service. This LoF was determined to have no operational impact. MDT-LoF-2 was removed from the final OHA.

- **MDT-MALF-1** - Loss of system availability during operations.

    - **Discussion** - Subject matter experts were used to assist the OSA panel in their deliberations for this hazard. The impact of this malfunction case is an inadvertent transition to a non-operational state when the system is operating. The panel determined that this malfunction case is of the same severity (Major) as the RVP LoF case (see RVP-LoF-1), although other functions including SLG and AAA may be lost simultaneously.

    - **Severity Assessment** – Major

- **MDT-MALF-2** - Loss of system integrity during operations due to a malfunction or error during the installation, setup, or checkout process.

    - **Discussion** – Subject matter experts were used to assist the panel in their deliberations of this hazard. The effect of this malfunction case is that the RT system may provide misleading information to the ATCS. The panel determined that this malfunction case is of the same severity (Major) as RVP malfunction cases (see RVP-MALF-1, 2, and 3), although other functions including SLG and AAA may also be impacted.

    - **Severity Assessment** – Major

- **MDT-MALF-3** - Loss of system availability due to a malfunction during system installation, setup, or checkout.

- **Discussion** – It was agreed upon that this hazard is redundant with MDT-LoF-2. MDT-MALF-3 was removed from the final OHA.

- **MDT-MALF-4 -** Loss of system integrity during system installation, setup, or checkout.

    - **Discussion** - It was agreed upon that this hazard is redundant with RVP-MALF-2. MDT-MALF-4 was removed from the final OHA.

3.4.5. Data Recorder Hazards

These hazards relate to the system's ability to record the live video from the RVP and supplementary cameras for replay purposes. This functionality is required for accident investigation purposes and may also be used for maintenance activities.

- **DR-LoF-1** - Loss of the capability to record (and subsequently replay) the required video presentation used by ATC.

    - **Discussion** – Information from the National Airspace System (NAS) Voice Recorder (NVR) Preliminary Hazard Analysis (PHA) was provided to the panel for reference when discussing this hazard, and the findings are in line with what was provided in that document. It was determined that this failure mode does not have an impact on operational safety. DR-LoF-1 was removed from the final OHA.

- **DR-MALF-1** - Misleading, inaccurate, and/or unusable required video presentation recordings.

    - **Discussion -** Information from the National Airspace System (NAS) Voice Recorder (NVR) Preliminary Hazard Analysis (PHA) was provided to the panel for reference when discussing this hazard, and the findings are in line with what was provided in that document. It was determined that this failure mode does not have an impact on operational safety. DR-MALF-1 was removed from the final OHA.

3.5. Remote Tower OHA Worksheet

Table 3-2. OHA Worksheet RVP-LoF-1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
RVP-LoF-1	Partial or total loss of the capability to detect and identify objects / observe spatial relationships in the area of jurisdiction (i.e., runways, short finals, and base turns).	Equipment failure; Hardware design error; Software/Firmware design error; Installation, Setup/ Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: - Controller intervention. - SOPs - Pilot training / intervention o Pilot see and avoid procedure - Pilot-reported positions - Published flight advisories - Controller system experience. - Airport Personnel FOD prevention, detection, removal, evaluation, and reporting (Ref AC 150/5210-24). - Operational contingency plan (OCP) for transitioning to ATC-Zero
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- Loss of all required ATC visual presentation - ATC loss of situational awareness - Large increase in ATC workload	Major	**Flight crew:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification	SO1 - Define site-specific presentation areas that correspond to the area of jurisdiction. These critical areas need to be defined at each installation site.

	- Loss of ATC services requiring visual information - Transition to ATC-Zero in 60-120 seconds (estimate) - Aircraft under the direction of the RT will need to switch to uncontrolled tower procedures (e.g., Increase in flight crew workload) - Potential for CAT B runway incursion		- Significant reduction in safety margin - Rejected landing at or near threshold - Four panel members voted that the severity should be defined as Minor **ATC:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - CAT C runway incursion - Three panel members voted that the severity should be defined as Major **NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Significant increase in ATC workload - Four panel members voted that the severity should be defined as Major	SO2 - Define appropriate site-specific ATCS reaction to this failure (i.e., transition to ATC- Zero) as required by FAA JO 1900.47. SO3 – Define a reliability requirement for the RVP based on NAS equivalent equipment performance or based on a derived allocation for the Loss of RVP Function.

			For more details see Section 3.4 Final Hazards and Deliberation Notes	

Table 3-3. OHA Worksheet RVP-PLoF-1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
RVP-PLoF-1	Partial loss of the capability to detect and identify objects and observe spatial relationships in non-essential / non-critical areas.	Equipment failure; Hardware design error; Software/Firmware design error; Installation, Setup/ Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls - Controller Intervention. - SOPs. - Published flight advisories - Airport Personnel FOD prevention, detection, removal, and reporting (Ref AC 150/5210-24). - Tower is staffed per 7210.3 - Pilot intervention - Pilot-reported positions - Pilots are trained to fly in non-towered airspace
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 -	- Slight increase in ATC workload.	Minimal	**NAS Equipment:** - Assessed effects are consistent with effects	SO1 - Define site-specific presentation areas that correspond to the area of

Identified Controls			defined in SMS Table 3.3 for the stated severity classification - Slight increase in ATC workload For more details see Section 3.4 Final Hazards and Deliberation Notes	jurisdiction. These critical areas need to be defined at each installation site. SO2- Develop procedures (OCP) to follow if "non-critical/non-essential" presentation areas suffer a LoF/PLoF.

Table 3-4. OHA Worksheet RVP-MALF-1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
RVP-MALF-1	HMI provided to ATCT controller: Presented visual information is not real-time; asynchronous time lag between presentations/displays. Relative spatial relationship between objects on different physical presentations will be incorrect (i.e., asynchronous presentations/ displays).	Equipment failure; Hardware design error; Software/Firmware design error; Installation, Setup/ Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- ATC makes decisions based on HMI - Large increase in ATC workload - Significant reduction in safety margin - Potential for a flight crew to reject landing at or near the runway threshold - Potential for flight crew to abort a takeoff; the act of aborting takeoff	Major	**Flight crew:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Circumstances requiring a flight crew to abort takeoff (i.e., rejected	Define synchronization monitoring requirement for all presentations: SO1 - Define latency requirement between the occurrence of an event in the real world and the presentation on the display.

	degrades the aircraft performance capability - Potential for Category B or C runway incursion (RI)		takeoff); the act of aborting takeoff degrades the aircraft performance capability - Potential for a flight crew to reject landing at or near the runway threshold **ATC:** - Assessed effects are consistent with effects defined in SMS Table 3.3 and Table 3.4 for the stated severity classification - CAT B runway incursion **NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Large increase in ATC workload - Significant reduction in safety margin For more details see Section 3.4 Final Hazards and Deliberation Notes	SO2 - Define a requirement for the probability of an undetected malfunction. SO3 - Define failure alerting notification requirement S04 - Define synchronization monitoring requirement for all presentations

Table 3-5. OHA Worksheet RVP-MALF-2

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
RVP-MALF-2	HMI provided to ATCT controller: Presented visual information is not real-time: consistent time lag in all monitors.	Equipment failure; Hardware design error; Software/Firmware design error; Installation, Setup/ Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**

See Section 2.5 - Identified Controls	- ATC makes decisions based on HMI
	- Large increase in ATC workload
	- Significant reduction in safety margin
	- Potential for a flight crew to reject landing at or near the runway threshold
	- Potential for flight crew to abort a takeoff; the act of aborting takeoff degrades the aircraft performance capability
	- Potential for Category B or C runway incursion (RI)
		Major	**Flight crew:**
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - Circumstances requiring a flight crew to reject landing (i.e., balked landing) at or near the runway threshold
			
			ATC:
			- Assessed effects are consistent with effects defined in SMS Table 3.3 and Table 3.4 for the stated severity classification
			  - CAT B runway incursion
			
			NAS Equipment:
				SO1 - Define latency requirement between the occurrence of an event in the real world and the presentation on the display.
				
				SO2 - Define a requirement for the probability of an undetected malfunction.
				
				SO3 - Define failure alerting notification requirement

			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Significant reduction in safety margin For more details see Section 3.4 Final Hazards and Deliberation Notes	

Table 3-6. OHA Worksheet RVP-MALF-3

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
RVP-MALF-3	HMI provided to ATCT controller: Presented visual information is not real-time: presentation of frozen visual information.	Equipment failure; Hardware design error; Software/Firmware design error; Installation, Setup/ Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- ATC makes decisions based on HMI - Large increase in ATC workload - Significant reduction in safety margin - Potential for a flight crew to reject landing at or near the runway threshold	Major	**Flight crew:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification	SO1 - Define latency requirement between the occurrence of an event in the real world and the presentation on the display.

	- Potential for flight crew to abort a takeoff; the act of aborting takeoff degrades the aircraft performance capability - Potential for Category B or C runway incursion (RI)		- Circumstances requiring a flight crew to reject landing (i.e., balked landing) at or near the runway threshold **ATC:** - Assessed effects are consistent with effects defined in SMS Table 3.3 and Table 3.4 for the stated severity classification - CAT B runway incursion - One panel member dissented, stating the severity should be defined as Minor **NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Significant reduction in safety margin See Appendix E for Dissenting Opinions For more details see Section 3.4 Final Hazards and Deliberation Notes	SO2 - Define a requirement for the probability of an undetected malfunction. SO3 - Define failure alerting notification requirement

Table 3-7. OHA Worksheet SLG-LoF-1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
SLG-LoF-1	Inability to provide visual signals to aircraft, vehicles, or personnel. (NORDO present)	Equipment failure; Hardware design error; Software/Firmware design error; Installation, Setup/ Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: - 7210.3 requires equipment checks during each watch and duty familiarization checklists when transferring controller position responsibility (Ref: Section 4-6-5 and 2-2-4 respectively).
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- A slight increase in ATC workload – ATC will need extra coordination with other traffic to accommodate the NORDO aircraft that cannot see the SLG	Minimal	**NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Slight increase in ATC workload For more details see Section 3.4 Final Hazards and Deliberation Notes	Need to consider adding SLG requirements to: SO1 - Define a requirement to allow ATCS to test the SLG prior to use. Ref FAA Order 7210.3. SO2 - Define a requirement to determine if the SLG is in an On/Off (i.e., radiating a signal or not) state. Ref FAA Order 7210.3.

Table 3-8. OHA Worksheet SLG-MALF-1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
SLG-MALF-1	SLG visual signal is unable to point/track.	Equipment failure; Design error; Software/Firmware Design Error; Installation, Setup, Configuration Error	non- Nominal: loss or failure of 2-way radio communications between at least one aircraft, vehicle, or personnel and ATC	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - NAS - Overlying Facility - Pilot (at least one a/c has no 2-way radio communications) - ATCT (no 2-way Radio communications with at least one a/c) - Airport Personnel (no 2-way radio communications with ATC)
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- ATC is unable to use the SLG - A slight increase in ATC workload	Minimal	**NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Slight increase in ATC workload	No safety objective

Table 3-9. OHA Worksheet SLG-MALF-2

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
SLG-MALF-2	Incorrect visual signal (i.e., incorrect color pattern / sequence) provided to at least one aircraft, vehicle, or personnel.	SLG Malfunction: Hardware failure, software design	non-Nominal: loss or failure of 2-way radio communications between at	- Pilot (at least one a/c has no 2-way Radio communications)

		error, firmware failure, etc.	least one aircraft, vehicle, or personnel and ATC	- ATCT (no 2-way Radio communications with at least one a/c) - Airport Personnel (no 2-way radio communications with ATC) - NAS - Overlying Facility
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- Slight increase in ATC workload - Increased attention the ATCS places on the target of the SLG, such that a reaction to an incorrect signal would be quickly observed	Minimal	**NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Slight increase in ATC workload For more details see Section 3.4 Final Hazards and Deliberation Notes	SO1 - Define a requirement to allow ATCS to test the SLG prior to use. Ref FAA Order 7210.3. SO2- Require that controllers have some way of verifying the correct color and sequence of light is being used and where it's being pointed. SO3 - Must require that the system can notify controllers of when the SLG is turned on

Table 3-10. OHA Worksheet AAA-LoF-1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
AAA-LoF-1	Total loss of ability of ATCS to hear AAA.	Equipment failure; Design error; Software/Firmware Design Error; Installation, Setup,	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility

		Configuration Error		- NAS Specific controls: - RVP Visual Information
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- Slight decrease in ATC Situational Awareness (i.e., no opportunity for awareness gained from sounds of aircraft on the field starting up, taxiing, taking off/landing or in the traffic pattern).	Minimal	**NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Slight increase in ATC workload For more details see Section 3.4 Final Hazards and Deliberation Notes	No safety objective

Table 3-11. OHA Worksheet AAA-PLoF-1

(1) OHA Hazard ID	**(2) Hazard Description**	**(3) Cause**	**(4) System State**	**(5) Controls**
AAA-PLoF-1	Failure of individual audio microphone and/or speaker. This results in inability of ATCT to hear AAA from section of airfield.	Equipment failure; Design error; Software/Firmware Design Error; Installation, Setup, Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific controls: - RVP Visual Information
(6)	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**

Control Justification				
See Section 2.5 - Identified Controls	- Slight decrease in ATC Situational Awareness - Inability of ATCT to hear AAA from section of airfield.	Minimal	**NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Slight increase in ATC workload For more details see Section 3.4 Final Hazards and Deliberation Notes	No safety objective

Table 3-12. OHA Worksheet AAA-MALF-1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
AAA-MALF-1	AAA isn't provided in "near real time" (e.g. delayed, out of synchronization with correct visual information, etc.). This results in misleading information provided to ATCT.	Equipment failure; Design error; Software/Firmware Design Error; Installation, Setup, Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific controls: - RVP Visual Information
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- Slight increase in ATC workload	Minimal	**NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for	SO1 - Define safety requirements to allow ATCS to disable AAA. This should include the ability to override

	- Controllers react to lagging audio and most likely move to disable/reduce the sound		the stated severity classification - Slight increase in ATC workload For more details see Section 3.4 Final Hazards and Deliberation Notes	applicable installation configurable settings.

Table 3-13. OHA Worksheet AAA-MALF-2

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
AAA-MALF-2	AAA is not spatially representative of reality (e.g. engine noise from the south appears to be coming from the north). This results in misleading information provided to ATCT.	Equipment failure; Design error; Software/Firmware Design Error; Installation, Setup, Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific controls: - RVP Visual Information
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- A slight increase in ATC workload - Controllers become aware of and react to spatially misleading audio and most likely move to disable/reduce the sound	Minimal	**NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Slight increase in ATC workload	SO1 - Define safety requirements to allow ATCS to disable AAA. This should include the ability to override applicable installation configurable settings.

			For more details see Section 3.4 Final Hazards and Deliberation Notes	

Table 3-14. OHA Worksheet AAA-MALF-3

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
AAA-MALF-3	AAA quality or volume creates a distraction (e.g. volume stuck high, excessive noise, etc.).	Equipment failure; Design error; Software/Firmware Design Error; Installation, Setup, Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific controls: - RVP Visual Information
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**
See Section 2.5 - Identified Controls	- A slight increase in ATC workload - Controllers react to the distraction and most likely move to disable/reduce the sound	Minimal	**NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Slight increase in ATC workload For more details see Section 3.4 Final Hazards and Deliberation Notes	SO1 - Define safety requirements to allow ATCS to disable AAA. This should include the ability to override applicable installation configurable settings.

Table 3-15. OHA Worksheet MDT-MALF-1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
MDT-MALF-1	Loss of system availability during operations.	MDT Malfunction: Hardware failure, software design error, firmware failure, etc.	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**

See Section 2.5 - Identified Controls	- MDT Malfunction: inadvertent transition to non-operational state
	- Operational effect equivalent to RVP-LoF-1 (directly below)
	  - Loss of all required ATC visual presentation
	  o ATC loss of situational awareness
	  o Significant increase in ATC workload
	  o Loss of ATC services requiring visual information
	  - Transition to ATC-Zero in 60-120 seconds (estimate)
	  - Aircraft under the direction of the RT will need to switch to uncontrolled tower procedures (e.g., Increase in flight crew workload)
	  - Potential for CAT C runway incursion
		Major	**Flight crew:**
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - Circumstances requiring a flight crew to reject landing (i.e., balked landing) at or near the runway threshold
			- Four panel members voted that the severity should be defined as Minor
			
			ATC:
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - CAT C runway incursion
				SO1 - Define a requirement for fail-safe system status changes (e.g., Operational-to-Non-Operational, Non-Operational-to-Operational, Operational-to-Test, etc.).
				
				SO2 - Mitigation(s) should be developed to prevent MDT malfunctions from causing other system functions to fail. The level of assurance for the chosen mitigation strategy (e.g., design architecture, functional design assurance levels, procedural, etc., or a combination thereof) should be commensurate with the failure effects of the impacted function(s).

	- Potential for additional functional losses (e.g., AAA, SLG, etc.)		- Three panel members voted that the severity should be defined as Major **NAS Equipment:** - Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification - Significant reduction in safety margin - Four panel members voted that the severity should be defined as Major For more details see Section 3.4 Final Hazards and Deliberation Notes	

Table 3-16. OHA Worksheet MDT-MALF-2

(1) **OHA Hazard ID**	**(2)** **Hazard Description**	**(3)** **Cause**	**(4)** **System State**	**(5)** **Controls**
MDT-MALF-2	Loss of system integrity during operations due to a malfunction or error during the installation, setup, or checkout process.	MDT Malfunction: Hardware failure, software design error, firmware failure, etc.	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS
(6) **Control Justification**	**(7)** **Effect**	**(8)** **Severity**	**(9)** **Severity Rationale**	**(10)** **Safety Objectives**

See Section 2.5 - Identified Controls	- Operational effect equivalent to RVP-MALF-1/2/3 (directly below)
	  - ATC makes decisions based on HMI
	  - Large increase in ATC workload
	  - Significant reduction in safety margin
	  - Potential for a flight crew to reject landing at or near the runway threshold
	  - Potential for flight crew to abort a takeoff; the act of aborting takeoff degrades the aircraft performance capability
	  - Potential for Category B or C runway incursion (RI)
	- Potential for additional malfunctions (e.g., AAA, SLG, etc.)
		Major	**Flight crew:**
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - Circumstances requiring a flight crew to reject landing (i.e., balked landing) at or near the runway threshold
			
			ATC:
			- Assessed effects are consistent with effects defined in SMS Table 3.3 and Table 3.4 for the stated severity classification
			  - CAT B runway incursion
			
			NAS Equipment:
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - Significant reduction in safety margin
			
			For more details see Section 3.4 Final Hazards and Deliberation Notes
				SO1 - Define a requirement for defined system modes (e.g., Operational, non-Operational, Maintenance/Test, OFF).
				
				SO2 - Define a requirement to disable the MDT ability to alter system status and configuration parameters when the system is an OPERATIONAL state.
				
				SO3 - Define a requirement for fail-safe system status changes (e.g., Operational-to-Non-Operational, Non-Operational-to-Operational, Operational-to-Test, etc.).
				
				SO4 - Mitigation(s) should be developed to prevent MDT malfunctions from causing other system functions to fail. The level of assurance for the chosen mitigation strategy (e.g., design architecture, functional design assurance levels, procedural, etc., or a combination thereof) should be commensurate with the failure effects of the impacted function(s).
				
				SO5 - Define a requirement to confirm configuration settings have been loaded into the system appropriately prior to the system being placed in an Operational state.

4. Allocation of Safety Objectives and Requirements (ASOR)

4.1. Introduction and Scope

An ASOR is an analysis of operational hazard causes and safety requirements related to operational services that are documented in the OSED. The purpose and scope of this ASOR is to allocate the safety objectives and requirements related to the RT system. This ASOR was developed using the guidance provided in the latest versions of the ATO SMS Manual and SRMGSA.

Based on the OHA results, the ASOR allocates safety objectives and requirements, and identifies safety risk mitigation strategies in attaining those objectives and requirements. Objectives, requirements, and mitigation strategies are allocated to the system elements that provide the functional capability to perform the service.

The ASOR was developed using information from Section 3 as input. From the OHA, each operational hazard cause was analyzed further. Safety objectives and recommended safety requirements from the OHA were then allocated to systems on a "per function" basis.

The system's functional Design Assurance Levels (DAL) will be based on the hazard severity and later work to determine the portion of the hazard allocated to the remote tower system. Guidance for relating the functional severities to the specific DALs for software and hardware are provided in RTCA DO-278 - *Guidelines for Communication, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) Systems Software Integrity Assurance* and RTCA DO-254 - *Design Assurance Guidance for Airborne Electronic Hardware*.

Table 4-1. Hazard List with Severity Levels

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-PLoF-1	Partial loss of the capability to detect and identify objects and observe spatial relationships in non-essential / non-critical areas.	Minimal
RVP-MALF-1	HMI provided to ATCT controller: Presented visual information is not real-time; asynchronous time lag between presentations/displays. 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
SLG-LoF-1	Inability to provide visual signals to aircraft, vehicles, and personnel (NORDO present).	Minimal
SLG-MALF-1	SLG visual signal is unable to point/track accurately.	Minimal
SLG-MALF-2	Incorrect visual signal (i.e., incorrect color pattern / sequence) provided to at least one aircraft, vehicles, or personnel.	Minimal
AAA-LoF-1	Total loss of ability of ATCS to hear AAA.	Minimal
AAA-PLoF-1	Failure of individual audio microphone and/or speaker. This results in inability of ATCT to hear AAA from section of airfield.	Minimal
AAA-MALF-1	AAA isn't provided in "near real time" (e.g. delayed, out of synchronization with correct visual information, etc.). This results in misleading information provided to ATCT.	Minimal
AAA-MALF-2	AAA is not spatially representative of reality (e.g. engine noise from the south appears to be coming from the north). This results in misleading information provided to ATCT.	Minimal
AAA-MALF-3	AAA quality or volume creates a distraction (e.g. volume stuck high, excessive noise, etc.).	Minimal
MDT-MALF-1	Loss of system availability (System State: Nominal).	Minor
MDT-MALF-2	Loss of system integrity during operations due to a malfunction or error during the installation, setup, or checkout process.	Major

4.2. Allocation of Safety Objectives and Requirements

The safety objectives were identified during the Remote Towner SRM Panel (Table 4-2). The safety objectives were used to derive the recommended safety requirements (Table 4-3). These requirements will need to be validated and verified.

Table 4-2. Safety Objectives

Objective Number	Objectives
RVP-LoF-1 SO1	Define site-specific presentation areas that correspond to the area of jurisdiction. These critical areas need to be defined at each installation site.

Objective Number	Objectives
RVP-LoF-1 SO2	Define appropriate site-specific ATCS reaction to this failure (i.e., transition to ATC- Zero) as required by FAA JO 1900.47.
RVP-LoF-1 SO3	Define a reliability requirement for the RVP based on NAS equivalent equipment performance or based on a derived allocation for the Loss of RVP Function.
RVP-PLoF-1 SO1	See recommended safety objective for RVP-LoF-1 SO1.
RVP-PLoF-1 SO2	Develop procedures (OCP) to follow if "non-critical/non-essential" presentation areas suffer a LoF/PLoF.
RVP-MALF-1 SO1	Define latency requirement between the occurrence of an event in the real world and the presentation on the display.
RVP-MALF-1 SO2	Define a requirement for the probability of an undetected malfunction.
RVP-MALF-1 SO3	Define failure alerting notification requirement.
RVP-MALF-1 SO4	Define synchronization monitoring requirement for all presentations
RVP-MALF-2 SO1	See recommended safety objective for RVP-MALF-1 SO1.
RVP-MALF-2 SO2	See recommended safety objective for RVP -MALF-1 SO2.
RVP-MALF-2 SO3	See recommended safety objective for RVP -MALF-1 SO3.
RVP-MALF-3 SO1	See recommended safety objective for RVP -MALF-1 SO1.
RVP-MALF-3 SO2	See recommended safety objective for RVP -MALF-1 SO2.
RVP-MALF-3 SO3	See recommended safety objective for RVP -MALF-1 SO3.
SLG-LoF-1 SO1	Define a requirement to allow ATCS to test the SLG prior to use. Ref FAA Order 7210.3.
SLG-LoF-1 SO2	Define a requirement to determine if the SLG is in an On/Off (i.e., radiating a signal or not) state. Ref FAA Order 7210.3.
SLG-MALF-2 SO1	See recommended safety objective for SLG-LoF-1 SO1.
SLG-MALF-2 SO2	Require that controllers have a way of verifying the correct color and sequence of light is being projected, and where it's being pointed.
SLG-MALF-2 SO3	See recommended safety objective for SLG-LoF-1 SO2.
AAA-MALF-1 SO1	Define safety requirements to allow ATCS to disable AAA in the event of malfunction. This should include the ability to override applicable installation configurable settings.
AAA-MALF-2 SO1	See recommended safety objective for AAA-MALF-1 SO1.

Objective Number	Objectives
AAA-MALF-3 SO1	See recommended safety objective for AAA-MALF-1 SO1.
MDT-MALF-1 SO1	Define a requirement for fail-safe system status changes (e.g., Operational-to-Non-Operational, Non-Operational-to-Operational, Operational-to-Test, etc.).
MDT-MALF-1 SO2	Mitigation(s) should be developed to prevent MDT malfunctions from causing other system functions to fail. The level of assurance for the chosen mitigation strategy (e.g., design architecture, functional design assurance levels, procedural, etc., or a combination thereof) should be commensurate with the failure effects of the impacted function(s).
MDT-MALF-2 SO1	Define a requirement for defined system modes (e.g., Operational, non-Operational, Maintenance/Test, OFF).
MDT-MALF-2 SO2	Define a requirement to disable the MDT ability to alter system status and configuration parameters when the system is an OPERATIONAL state.
MDT-MALF-2 SO3	See recommended safety objective for MDT-MALF-1 SO1
MDT-MALF-2 SO4	Mitigation(s) should be developed to prevent MDT malfunctions from causing other system functions to fail. The level of assurance for the chosen mitigation strategy (e.g., design architecture, functional design assurance levels, procedural, etc., or a combination thereof) should be commensurate with the failure effects of the impacted function(s).
MDT-MALF-2 SO5	Define a requirement to confirm configuration settings have been loaded into the system appropriately prior to the system being placed in an Operational state.

Table 4-3. Recommended Safety Requirements

Requirement Number	Requirements
RVP-LoF-1 SR1	The vendor should have a procedure that defines the portion of the RVP that contains views of the area of jurisdiction. The area of jurisdiction should be included in the OCP.
RVP-LoF-1 SR2	The airport specific Memorandum of Agreement (MOA) / Operations and Maintenance Manual (OMM) / OCP must define a procedural requirement for the transition to ATC- Zero, following loss of function of the RVP. [Advisory Circular (AC)]

Requirement Number	Requirements
RVP-LoF-1 SR3	A reliability related requirement should be defined. The requirement will take the form of 1) An MTBCF equal to or greater than TBD hours or 2) a continuity allocation with a TBD exposure time. Note - Critical failures include those resulting in the loss of the RVP, and related sub-function failures, including control, monitoring and status. The loss of the RVP function can account for any built-in redundancy
RVP-PLoF-1 SR1	See recommended safety requirement for RVP-LoF-1 SR1
RVP-PLoF-1 SR2	The airport specific Memorandum of Agreement (MOA) / Operations and Maintenance Manual (OMM) / OCP must define a procedural requirement to follow in the event "non-critical/non-essential" presentation areas suffer a LoF/PLoF. [Advisory Circular (AC)]
RVP-MALF-1 SR1	There should be no greater than a 1 second time delay between the occurrence of an event in the real world and the presentation on the display [Technical Requirement (TR)]. [ED-240A, *Minimum Aviation System Performance Standards (MASPS) for Remote Tower Optical Systems*, EUROCAE, 12 November 2018].
RVP-MALF-1 SR2	The probability of an undetected malfunction of the RVP resulting in HMI should be less than or equal to 1E-6 (per 60 seconds). HMI is defined any failure resulting in exceedance of the latency requirement. Note- This probability can account for the presence of monitor(s) designed to detect malfunctions. [TR]
RVP-MALF-1 SR3	Video Failure Notification is the elapsed time between a failure affecting the operational usability of the video images presented to the operator and notification thereof to the operator. The video failure notification time should not exceed 2 seconds. [TR]
RVP-MALF-1 SR4	Define synchronization monitoring requirement for all presentations.
RVP-MALF-2 SR1	See recommended safety requirement for RVP-MALF-1 SR1.
RVP-MALF-2 SR2	See recommended safety requirement for RVP-MALF-1 SR2.
RVP-MALF-2 SR3	See recommended safety requirement for RVP-MALF-1 SR3.
RVP-MALF-3 SR1	See recommended safety requirement for RVP-MALF-1 SR1.
RVP-MALF-3 SR2	See recommended safety requirement for RVP-MALF-1 SR2.
RVP-MALF-3 SR3	See recommended safety requirement for RVP-MALF-1 SR3.
SLG-LoF-1 SR1	The SLG function must be able to be tested manually prior to use [TR] Ref FAA Order 7210.3.
SLG-LoF-1 SR2	The system shall provide notification of the SLG's On/Off (i.e., radiating a signal or not) state. Ref FAA Order 7210.3.
SLG-MALF-2 SR1	See recommended safety requirement for SLG-LoF-1 SR1
SLG-MALF-2 SR2	The system shall provide a means for controllers to verify the correct color and sequence of light is being projected and where it's being pointed.

Requirement Number	Requirements
SLG-MALF-2 SR3	See recommended safety requirement for SLG-LoF-1 SR2
AAA-MALF-1 SR1	Ambient airfield audio must be able to be disabled by the controller in the event of malfunction. This should include the ability to overide any installation configurable settings. [TR]
AAA-MALF-2 SR1	See recommended safety requirement for AAA-MALF-1 SR1
AAA-MALF-3 SR1	See recommended safety requirement for AAA-MALF-1 SR1
MDT-MALF-1 SR1	The system shall enable fail-safe system status changes (e.g., Operational-to-Non-Operational, Non-Operational-to-Operational, Operational-to-Test, etc.).
MDT-MALF-1 SR2	Mitigation(s) should be developed to prevent MDT malfunctions from causing other system functions to fail. The level of assurance for the chosen mitigation strategy (e.g., design architecture, functional design assurance levels, procedural, etc., or a combination thereof) should be commensurate with the failure effects of the impacted function(s).
MDT-MALF-2 SR1	The RT system installation and maintenance procedures shall include a requirement to confirm configuration settings have been loaded into the system appropriately prior to the system being placed in an Operational state. [AC]
MDT-MALF-2 SR2	The system shall disable the MDT from allowing alterations to system status and configuration parameters when the system is an OPERATIONAL state.
MDT-MALF-2 SR3	See recommended safety requirement for MDT-MALF-1 SR1.
MDT-MALF-2 SR4	See recommended safety requirement for MDT-MALF-1 SR2.
MDT-MALF-2 SR5	The vendor must develop procedures to confirm configuration settings have been loaded into the system appropriately prior to the system being placed in an Operational state.

Table 4-4 below provides the distribution of the recommended safety requirements from the OHA Table in Section 3.4 to Remote Tower functions. The requirements were reviewed internally and distributed among the RT System Functions.

Table 4-4. Allocation of Safety Requirements by Function

Related Functions (From the OSED)	Safety Requirements Allocation

Required Visual Presentation	RVP-LoF-1 SR1 RVP-LoF-1 SR2 RVP-LoF-1 SR3 RVP-PLoF-1 SR2 RVP-MALF-1 SR1 RVP-MALF-1 SR2 RVP-MALF-1 SR3 RVP-MALF-1 SR4
Signal Light Gun	SLG-LoF-1 SR1 SLG-LoF-1 SR2 SLG-MALF-2 SR2
Ambient Audio	AAA-MALF-1 SR1
MDT	MDT-MALF-1 SR1 MDT-MALF-1 SR2 MDT-MALF-2 SR1 MDT-MALF-2 SR2 MDT-MALF-2 SR5

5. Remote Towers Assessment and Conclusions

The Remote Towers OSA was conducted in accordance with reference documents listed in Appendix F.

Per Table 4-1, 15 “RT hazards” were identified resulting in worst case credible hazard severities. Based upon these severities, safety objectives and requirements were established to mitigate the associated risk to an acceptable level.

Existing safety controls and requirements have been developed for a design that addresses the minimum functional requirements described in this OSA. Addition safety objectives and requirements will be addressed in applicant specific safety assessments (e.g., Functional Hazard Assessments and Preliminary System Safety Assessments). These additional safety objectives and requirements will address the applicant’s specific architecture (e.g., supplemental functions that are not addressed in the OSA).

Subsequently, safety hazard assessments will continue throughout each applicant’s program lifecycle in response to changes in system architecture or concept of use.

Appendix A - Functional Analysis (FA)

This FA[5] identifies and assesses the system functions required to meet the RT system functional requirements. The identified functions are required to make a non-Federal RT system a viable alternative in the NAS. This analysis is intended be included in the overall RT system operational safety process, and in particular, to be an input into the non-Federal RT system OSA development. The inputs for this assessment are based on a review of several RT systems installed (or being reviewed for installation) throughout the world, systems being used for the FAA RT system demonstration/pilot programs, and various non-Federally approved systems currently installed in the NAS. There are two general classes of functions considered:

RT System Functional Requirements Capture

As there is currently no approved set of system requirements or standards for an RT system, multiple sources (see examples below) were used to capture RT system functional requirements. It is asserted that this set of preliminary functional requirements is sufficient to perform the initial safety assessment (i.e., OSA) of an RT system. The sources used to capture RT system functional requirements are listed below:

1) A direct or implied traceability[6] from the RT system OVRs V1.0, dated July 15, 2019.
2) EUROCAE/ED-240A, *Minimum Aviation System Performance Standard for Remote Tower Optical Systems*
3) Typical NAS equipment functional requirements to configure, maintain, or provide operational monitoring and status, derived during the development and review of this analysis, and information gained from the FAA Remote Tower Pilot Program.

Optional/Supplemental Functions

Although not required for non-Federal Type Certification, some common optional functions are considered in this analysis to review their potential to adversely affect tower operations. Potential adverse impacts could include the optional function(s) corrupting a required function, optional function(s) providing misleading information to the ATCS, etc.

---

[5] . An FA examines the functions and sub-functions of a solution that accomplish the operation or mission. An FA describes what the solution does, rather than how it does it, and is conducted at a level needed to support later synthesis efforts. Products from the FA such as the Functional Flow Block Diagram (FFBD) and N-Squared (N_2) diagram [4] may be used as inputs in developing the OSA. [*Reference Safety Risk Management Guidance for System Acquisitions (SRMGSA), Appendix C: Guidance for Conducting and Documenting an Operational Safety Assessment (OSA), Section 4.2.4 Functional Analysis*]

[6] In general, OVRs provide a direct traceability for the necessity of a visual presentation function. In some cases, the OVRs imply the need for other functionality like an SLG (i.e., there are no SLG requirements listed, but the existence of the SLG is assumed/implied).

Functional Description

Several required and optional functions have been identified from this analysis. These functions have been accumulated through the review of the preliminary RT system functional requirements. It is the assertion of the review team that these functions adequately describe the required functionality for a minimally acceptable RT system. The specific functions identified for further review are listed below:

Required Functions

1. Required Visual Presentation - The RVP function includes all visual presentations necessary to meet the OVRs (as defined in OVR, v 1.0, dated July 5, 2019). A continuous fixed 360-degree view of the airfield and surrounding airspace must be provided.

   Note: Primary OVRs must be met on the fixed continuous 360-degree presentation. Secondary OVRs can be met either with the fixed continuous 360-degree presentation view or with an augmented presentation.

   a. Includes the functionality that allows the ATCS to control any system components relating to the RVP of the RT system. (Note: This may include environmental controls and redundancy management.)

   b. Includes the functionality that performs RVP monitoring and indicates the overall RT system status. Reports any faults, system events, and / or other information necessary for the controllers.

2. Maintenance Data Terminal

   Functionality required to facilitate installation, check-out/verification, and maintenance activities. This includes the functionality required to:

   a. Perform system configuration updates (e.g., software updates, network configuration updates, configurable parameter setup/modifications, modify/view adaptation data, etc.)

   b. Perform maintenance activities (i.e., diagnostics, corrective maintenance, calibration, troubleshooting, Built-In-Test, etc.).

   c. View stored system data such as resource status, faults, warnings, system errors, event logs, and network information.

   Engineers and technicians are the primary users of this function; this function is not intended for use by ATCS.

3. Data Recording

   Functionality required to record visual data for playback (i.e. video, fault/failure annunciations, timestamp, etc.). Includes the functionality required to:

a. Record the information provided on the Required and Supplemental (if provided) Video Presentations.

b. Control the data recording functionality (e.g., configure / setup recording parameters).

c. Detect and annunciate failure or degradation of Data Recording components.

Note – There is no current order or policy requiring this functionality; however, examples of recent FAA programs were used as trending examples of the FAA direction regarding video recording. The functionality is included to support accident investigations, installation checkout/verification, and maintenance activities.

4. Signal Light Gun

Functionality required to communicate visually with aircraft, equipment, vehicles, and pedestrians. The SLG used in an RT system application must be physically located on the airfield and be controllable by ATCS located in the RTC (i.e., the SLG visual signal source and the SLG control are not collocated). (Note: Equivalent function to SLG on MEL for conventional towers.). This includes the functionality required to:

a. Aim at an object of concern/interest (e.g., aircraft, vehicle, equipment, or pedestrians) and signal as appropriate.

b. Monitor, detect, and annunciate failure or degradation of components in the SLG functional chain.

5. Ambient Airfield Audio Function

Functionality to transmit AAA to the controllers. This includes the functionality to:

a. Functionality required to install, setup, and confirm the proper operation of the AAA (e.g., view/modify configuration parameters).

b. Any volume or other controls associated with AAA use.

Functionality built into the system to detect and annunciate failed or degraded components in the AAA chain.

Optional functions

6. Binocular Function

Binoculars are a Minimum Equipment List (MEL) item for brick-and-mortar towers. The equivalent functionality can be provided in a RT system in at least three different ways:

a. A remote tower system MEL could be developed to, among other things, require physical short focal length binoculars.

b. The RT system applicants as a part of the Type Certified system could provide physical short focal length binoculars as part of the RT system.

c. An enhanced/augmented presentation provided on the Required Video Presentation or a Supplemental Video Presentation (e.g., a zooming and scanning capability displayed as a video presentation).

For the purposes of this assessment, the functionality described in option 6c can only be addressed in a general sense. The applicants intended use and specific implementation will need to be evaluated during the Type Certification System Safety Review process. General safety requirements will be developed later in this assessment to address this and other optional functions (e.g., optional functions shall not adversely affect required functionality; optional functions shall not provide hazardous/misleading information to the ATCS, etc.).

7. Supplemental Visual Presentation Function

The supplemental visual presentation function includes any and all auxiliary visual presentations or enhancements that are intended to provide additional situational awareness but are NOT required to meet the OVRs (as defined in V1.0). Example Supplemental Visual Presentations include:

a. Supplemental Visual Presentation Control

Functionality that allows ATCS to control any system components relating to the Supplemental Visual Presentation of the RT system.

b. System Monitoring & Status Functions

Functionality built into the system to detect and annunciate failed or degraded components in the Supplemental Visual Presentation chain (e.g., latency monitoring, redundancy alerts, etc.)

c. Fixed overlays presented on the Required Visual Presentation (e.g., highlighted an area of the airfield, distant object of known distance, etc.).

d. Moving overlays presented on the RVP (e.g., any method used to highlight a moving aircraft on the RVP).

e. Pre-configured scans of airfield areas of interest (e.g., programmed scans from a Pan-Tilt-Zoom (PTZ) camera).

f. Fixed video presentations of a particular area of interest (e.g., fixed video presentation of the primary approach end of the runway).

Functional Interface Description

The table on the following page was generated to identify the functional interfaces between each of the RT system required and optional functions. All possible functional combinations were considered. The review team considered each interface while considering standard failure modes classes (e.g., data coupling corruption, inadvertent control coupling, errors denial of service/functionality, corruption of data, etc.). Each cell of the table contains one of the following values:

Table A-1. Functional Interface Description

Legend Value	Description
X	Required Functional Connection/Interface
IS (n)	Implementation Specific Interface - The interface is subject to the applicant's design choices. - The interface is allowable. - The index "(n)" was used to identify notes specific to the applicable table cell. The notes are shown on the page following the table.
N/A	Not Applicable (Not Allowable) — This analysis concluded that an interface between these functional areas was not allowable. These conclusions will be captured as functional requirements.

Note: The table is intended to be symmetric around the diagonal. To avoid duplicate work, only the lower diagonal portion contains note references (i.e., the references to the upper diagonal would be redundant).

Table A-2. Functional Interfaces

	Required Visual Presentation	Maintenance Data Terminal	Recording	Signal Light Gun	Supplemental Visual Presentation (Optional)	Ambient Airfield Audio	Binocular
Required Visual Presentation	**Required**						
Maintenance Data Terminal	X, IS(12)	**Required**					
Recording	X, IS (10)	X, IS(12)	**Required**				
Signal Light Gun	IS (1)	IS(1), IS(12)	IS (2)	**Required**			
Supplemental Visual Presentation (Optional)	IS (3)	X, IS(12)	X, IS (4)	IS (1)	**Optional**		
Ambient Airfield Audio	IS (11)	IS(11), IS(12)	IS (7)	N/A	IS (11)	**Required**	
Binocular (A specific Supplemental Example)	IS (8)	X, IS(12)	X, IS (9)	N/A	IS (8)	N/A	**Optional**

Table A-3. Functional Interface Descriptions

Interface Notes	Description
IS (1)	(FA-1) The Signal Light Gun (SLG) may be implemented as an independent function, or it may rely on other functions (e.g., for aiming, transmitted signal selections, etc.). Note: If the SLG is dependent of other system functions, design assurance levels for some of the involved functions may be affected (i.e., some functions may be held to a higher standard if they can contribute to a more severe failure condition).
IS (2)	(FA-2) SLG control parameters (i.e., aiming, transmitted signal selection, etc.) shall be captured and stored in system event logs accessible to the MDT function.
IS (3)	Applicants may choose to present visual information from the Required Visual Presentation to the Supplemental Visual Display (e.g., a specific area of the Required Visual Display on a Supplemental Device); likewise, applicant may choose to provide Supplemental Visual Presentation information on the Required Visual Presentation Display (e.g., an overlay of supplemental information). Note: If the Required Visual Display is not independent from other system functions, design assurance levels for some of the involved functions may be affected (i.e., some functions may be held to a higher standard if they can contribute to a more severe failure condition).
IS (4)	If an applicant provides a Supplemental Visual Presentation, does it have to be recorded (X) or is it an option (IS)? (FA-3) Supplemental Visual Presentation data shall be recorded, stored, and available for playback. (FA-4) Recording function shall be capable of retrieval and playback of all recorded visual data.
IS (5)	The Signal Light Gun may be a standalone (i.e., encapsulated) function, or it may rely on other functions for aiming, transmitted signal selections, etc.
IS (6)	If provided, the Ambient Airfield Audio may be a standalone (i.e., encapsulated) function, or it may rely on other supplemental functions for muting, volume control, etc.
IS (7)	If the Ambient Airfield Audio control selections have to be recorded, applicants may choose to record Supplemental Visual Presentation control selections as a part of the normal visual presentation recording if the control functions are selectable/viewable from the Supplemental Visual Presentation; otherwise, the Ambient Airfield Audio control selections should be captured in event logs available on the MDT function.
IS (8)	If provided, the Binocular Function may be a standalone (i.e., encapsulated) function, or it may rely on other Required or Supplemental Visual Presentation functions for aiming, zooming, scanning, display, display control, etc.

IS (9)	If the Binocular Function has to be recorded (i.e., the enhanced presentation), applicants may choose to record the Visual Presentation and the Visual Presentation Control selections as a part of the normal visual presentation recording (i.e., if the control functions are selectable/viewable from the Required Visual Presentation); otherwise, the Binocular Functional parameters should be captured in event logs available on the MDT function.
IS (10)	(FA-5) Control of the Recording function shall not be allowed from the Required Visual Presentation function. (FA-6) The ability to establish/setup recording parameters, modify recording parameters, and delete recorded information shall be limited to authorized personnel with the proper login credentials. (FA-8) The normal operation or failure of the Recording function shall not contribute to the failure (e.g., loss of function or malfunction) of any other system function.
IS (11)	(FA-7) The Ambient Airfield Audio function may be implemented as an independent function, or it may rely on other functions (e.g., for control on a graphical user interface). Note: If the AAA is dependent of other system functions, design assurance levels for some of the involved functions may be affected (i.e., some functions may be held to a higher standard if they can contribute to a more severe failure condition).

Functional Block Diagram

The functional block diagram depicted on the following page was generated after reviewing the Functional Interface Description presented in the previous section.

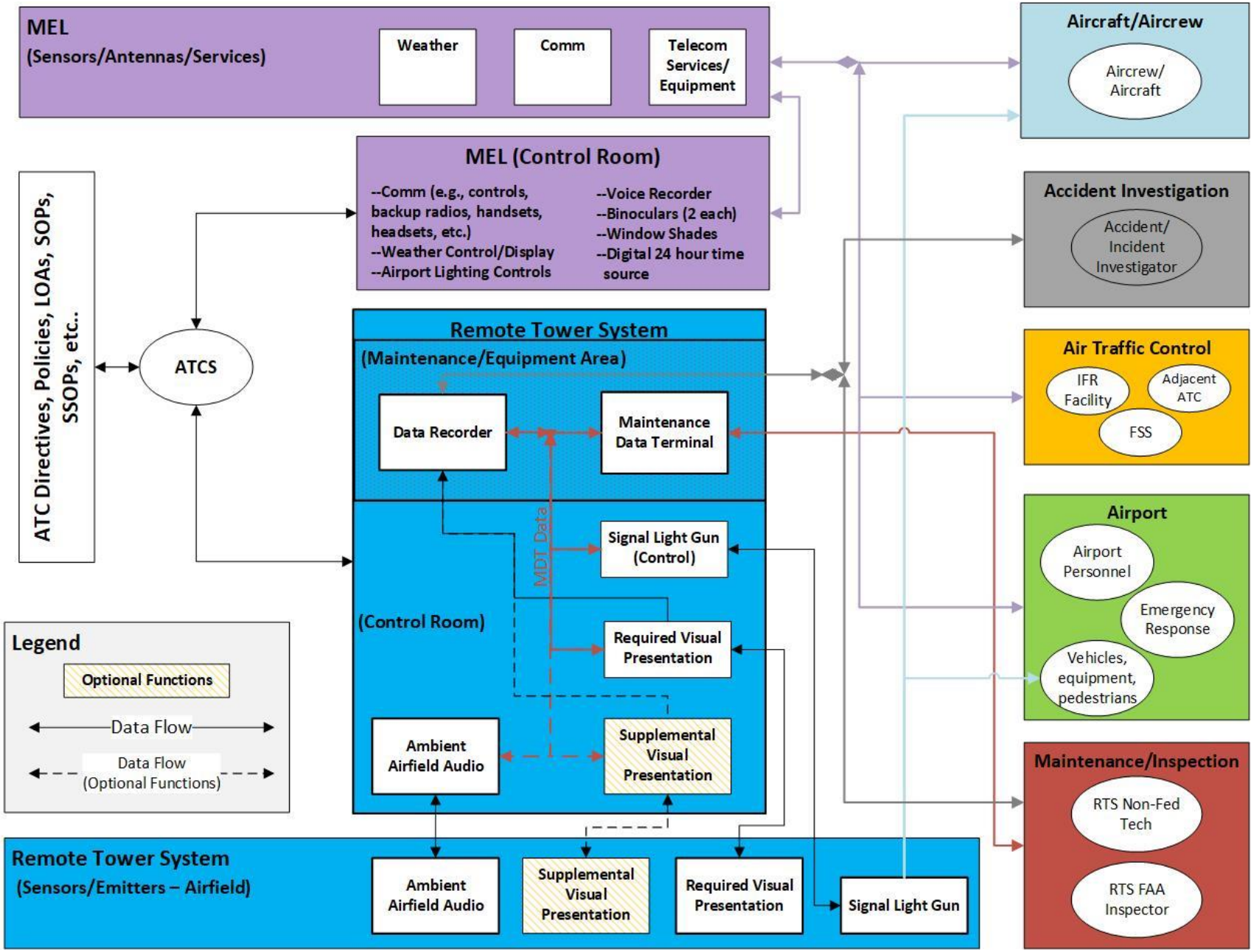

Figure A-1. Functional Block Diagram

System Functional Objectives and Requirements

The preliminary system functional requirements are listed in the table below.

Table A-4. System Functional Requirements

Req't Tag	Requirement and Objectives	Source	Function Block Assignment
FA-1	Acceptable means of implementing the SLG function may be as an independent function, or it may rely on other functions (e.g., for aiming, transmitted signal selections, etc.). Note: If the SLG is dependent of other system functions, DALs for some of the involved functions may be affected (i.e., some functions may be held to a higher standard if they can contribute to a more severe failure condition).	Functional Analysis	SLG
FA-2	SLG control parameters (i.e., aiming, transmitted signal selection, etc.) shall be captured and stored in system event logs accessible to the MDT function.	Functional Analysis	SLG
FA-3	Supplemental Visual Presentation data shall be recorded, stored, and retrievable for playback.	Functional Analysis	Recording
FA-4	Recording function shall be capable of retrieval and playback of all recorded visual data.	Functional Analysis	Recording
FA-5	Control of the recording function shall not be allowed from the RVP function.	Functional Analysis	RVP
FA-6	The ability to establish/setup recording parameters, modify recording parameters, and delete recorded information shall be limited to authorized personnel with the proper login credentials.	Functional Analysis	Recording
FA-7	The Ambient Airfield Audio function may be implemented as an independent function, or it may rely on other functions (e.g., for control on a graphical user interface). Note: If the Ambient Airfield Audio is dependent of other system functions, design assurance levels for some of the involved functions may be affected (i.e., some functions may be held to a higher standard if they can contribute to a more severe failure condition).	Functional Analysis	AAA

Req't Tag	Requirement and Objectives	Source	Function Block Assignment
FA-8	The normal operation or failure of the Recording function shall not contribute to the failure (e.g., loss of function or malfunction) of any other system function.	Functional Analysis	Recording
FA-9	A failure of the MDT function shall not cause a failure of any other function.	Functional Analysis	MDT

Appendix B - Functional Hazard Assessment (FHA)

The table on the following pages capture the FHA of the remote tower system. This FHA considers the required functions identified in the Functional Analysis (ref: Appendix A of this document).

For readers not familiar with FHAs, relevant excerpts from the FAA Safety Risk Management Guidance for System Acquisition (SRMGSA) dated March 2020 are provided below for reference.

4.1.2 Purpose of an FHA

The purpose of an FHA is to identify every expected function of a system and consider the hazards that may result when each function fails in every possible way. It does not determine causes of the hazards but rather focuses on the consequences and corresponding severities. As a predictive technique, the FHA attempts to explore the effects of functional failures of parts of a system. A guiding principle of the FHA is that if safety requirements are added at the functional level early in the system development process, the design of the system will be more stable from a safety perspective, and the cost of implementing safety mitigations will be reduced.

4.1.5 FHA Methodology

An FHA is a methodical approach for identifying credible operational safety effects through the analysis of system or sub-system functions and failure conditions. The FHA identifies and classifies the system functions and safety hazards associated with functional failure or malfunction. It identifies the relationships between functions and hazards, thereby identifying the safety-significant functions of the system as well as the hazards associated with that functionality. This identification provides a foundation for the safety program to scope additional safety analyses.

Requirements and design constraints are recommended for inclusion in the system specifications in order to eliminate or reduce the risk of the identified hazards once the system is successfully implemented.

4.1.5.2 FHA Process

Systematically, the FHA identifies:

- *The functions, purposes, and behaviors of a system.*
- *Considerations of how the system fails (e.g., when can the failure conditions occur? In what operational environment will these failures be present?). Consider the following hypothetical failure modes. (Note: Additional failure types may be identified through system reports and subject matter expertise.)*
    - *Fails to operate: Function does not occur/perform when given the appropriate input.*
    - *Operates early/late: Function performs earlier or later than it should.*
    - *Operates out of sequence: Function occurs before or after the wrong function; function occurs without receiving the appropriate inputs.*

    - *Unable to stop operation: Function continues even though the thread should move on to the next function.*
    - *Degraded function or malfunction: Function does not finish or only partially completes; function generates improper output.*
- *Impact or effects that failures may have (e.g., does the functional failure constitute hazard?).*

Table B-1. FHA-RVP-LoF-1

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of the capability to detect and identify aircraft, wildlife, vehicles, and pedestrians.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS		Define a reliability requirement for the RVP based on NAS equivalent equipment performance or based on a derived risk allocation for the Loss of RVP Function.	

Table B-2. FHA-RVP-LoF-2

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of capability to observe spatial relationships
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot		Define a reliability requirement for the RVP based on NAS equivalent equipment performance or based on a derived risk allocation for the Loss of RVP Function.	

- Airport Personnel - ATCT - Overlying Facility - NAS		

Table B-3. FHA-RVP-LoF-3

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of the capability to detect and identify non-cooperating traffic, wildlife, vehicles, or pedestrians.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: 1. Controller intervention. 2. Controller Input on Consolidating/Deconsolidating Controller Positions 3. SOPs for the provision of procedural spacing and sequencing services Pilot intervention 4. Pilot intervention 5. Pilot-reported positions 6. Published flight advisories	Equivalent effect/hazard identified in JYO SRM panels.	Define a reliability requirement for the RVP based on NAS equivalent equipment performance or based on a derived risk allocation for the Loss of RVP Function.	

7. Controller experience using PTZ and binoculars (when used) 8. Tracker boxes (when used)		

Table B-4. FHA-RVP-LoF-4

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of the capability to detection/identify FOD on the runway or taxiway.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: 1. Pilot intervention and FOD reporting 2. Airport Personnel Intervention and FOD Reporting. 3. Published flight advisories	Specific Controls listed are consistent with specific controls for similar JYO hazards. The equivalent JYO hazard (1b) was "bound out".		

Table B-5. FHA-RVP-LoF-5

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)

RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of the capability to detection/identify abnormal conditions (e.g., gear-up landing, baggage door open, smoke trailing from aircraft).
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: 1. Pilot intervention and FOD reporting 2. Airport Personnel Intervention	Specific Controls listed are consistent with specific controls for similar JYO hazards. The equivalent JYO hazard (1c) was "bounded out".		

Table B-6. FHA-RVP-LoF-6

(1) Function	**(2) Function Failure Type**	**(3) System State**	**(4) Function Failure Effect(s)**
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of the capability to detect and identify weather for situational awareness
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel	Equivalent effect/hazard identified in JYO SRM panels.	Define an installation/setup requirement to: 1) Identify (critical presentation areas) and 2) Define appropriate ATCS reaction to this failure.	

- ATCT - Overlying Facility - NAS		

Table B-7. FHA-RVP-LoF-7

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of the capability to detect and identify the need to manage airport lighting.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: 1. Controller intervention 2. Controller Input on Consolidating/Deconsolidating Controller Positions 3. SOPs for the provision of procedural spacing and sequencing services 4. Pilot intervention 5. Pilot-reported positions 6. Published flight advisories 7. Sunrise/sunset charts	Equivalent effect/hazard identified in JYO SRM panels.	Define an installation/setup requirement to: 1) Identify (critical presentation areas) and 2) Define appropriate ATCS reaction to this failure.	

8. Runway lighting status lights on lighting control panel in RTM (in new RTC location) 9. Ability to dim overlay on RT visual presentation (in new RTC location) 10. Standards on runway lighting in FAA Order JO 7110.65, Chapter 3, Section 4 11. Airport personnel intervention		

Table B-8. FHA-RVP-LoF-8

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of the capability to detect and identify airport runway conditions.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: 1. Controller intervention 2. Controller Input on Consolidating/Deconsolidating Controller Positions	Equivalent effect/hazard identified in JYO SRM panels.	Define an installation/setup requirement to: 1) Identify (critical presentation areas) and 2) Define appropriate ATCS reaction to this failure.	

3. SOPs for the provision of procedural spacing and sequencing services 4. Pilot intervention 5. Pilot-reported positions 6. Published flight advisories 7. Airport personnel intervention		

Table B-9. FHA-RVP-LoF-9

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of capability to visually observe the spatial relationships between aircraft and/or vehicles on the movement area.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: 1. Controller intervention 2. Controller Input on Consolidating/Deconsolidating Controller Positions 3. SOPs for the provision of procedural spacing and sequencing services 4. Pilot intervention 5. Pilot-reported positions	Equivalent effect/hazard identified in JYO SRM panels.		

6. Published flight advisories 7. Airport personnel intervention		

Table B-10. FHA-RVP-LoF-10

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of capability to visually observe the spatial relationships between arriving and departing traffic.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: 1. Controller intervention. 2. Controller Input on Consolidating/Deconsolidating Controller Positions 3. SOPs for the provision of procedural spacing and sequencing services Pilot intervention 4. Pilot intervention 5. Pilot-reported positions 6. Published flight advisories 7. Controller experience using PTZ and binoculars (when used)	Equivalent effect/hazard identified in JYO SRM panels.		

8. Tracker boxes (when used)		

Table B-11. FHA-RVP-LoF-11

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	Nominal (See Appendix C - System State)	Loss of the capability to observe spatial relationships when there is an aircraft that needs to avoid terrain or obstacles in the vicinity of the airport.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: 1. Controller intervention. 2. Pilot intervention 3. Pilot-reported positions 4. Published flight advisories	Specific Controls listed are consistent with specific controls for similar JYO hazards. The equivalent JYO hazard (2g) was "bounded out".		

Table B-12. FHA-RVP-LoF-12

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	non-Nominal: loss or failure of 2-way radio communications between at least one aircraft, vehicle, or personnel and ATC	Loss of the capability to detect and identify aircraft, wildlife, vehicles, and pedestrians.
(5)	**(6)**	**(7)**	

Existing Controls	Notes	Recommended Requirements and Design Constraints
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	Intended to address the severity of an RVP loss of function in a non-nominal system state. This case represents the possibility of two independent failure modes. The total effect needs to be considered. (i.e., Loss of RVP function AND loss of capability to establish 2-radio communicate with at least one aircraft, vehicle, and/or personnel.).	Define a reliability requirement for the RVP based on NAS equivalent equipment performance or based on a derived risk allocation for the Loss of RVP Function.

Table B-13. FHA-RVP-LoF-13

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Loss of Function: - Loss of all presentation - Partial Loss of active airfield/movement area presentation	non-Nominal: loss or failure of 2-way radio communications between at least one aircraft, vehicle, or personnel and ATC	Loss of capability to observe spatial relationships

(5) Existing Controls	(6) Notes	(7) Recommended Requirements and Design Constraints
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	Intended to address the severity of an RVP loss of function in a non-nominal system state. This case represents the possibility of two independent failure modes. The total effect needs to be considered. (i.e., Loss of RVP function AND loss of capability to establish 2-radio communicate with at least one aircraft, vehicle, and/or personnel.).	Define a reliability requirement for the RVP based on NAS equivalent equipment performance or based on a derived risk allocation for the Loss of RVP Function.

Table B-14. FHA-RVP-PLoF-1

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)

RVP	RVP Partial Loss of Function: - Partial loss of presentation (non-critical/non-essential area)	Nominal (See Appendix C - System State)	Partial Loss of RVP (non-essential/non-critical area)
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	Intended to capture a scenario of partial RVP loss (e.g., rooftop of an airport building)	Define an installation/setup requirement to: 1) Identify (non-critical presentation areas) and 2) Define appropriate ATCS reaction to this failure.	

Table B-15. FHA-RVP-MALF-1

(1) Function	**(2) Function Failure Type**	**(3) System State**	**(4) Function Failure Effect(s)**
RVP	RVP Malfunction: - Asynchronous presentations / displays (e.g., all monitors not synched in time, relative lag between some RT visual presentations, etc.)	Nominal (See Appendix C - System State)	HMI Provided to ATCT: Relative spatial relationship between objects on different physical presentations will be incorrect (i.e., misleading or hazardously misleading).
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS		Define synchronization monitoring requirement for all presentations: 1) Monitor all presentations against time standard (absolute time monitoring), and 2) Monitor for relative synchronization across all presentations (relative time monitoring).	

Table B-16. FHA-RVP-MALF-2

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Malfunction: - Consistent time lag in all monitors (e.g., RT visual presentation of stale or recorded visual information)	Nominal (See Appendix C - System State)	HMI Provided to ATCT: Presented visual information is incorrect (i.e., not real-time information, not consistent with reality, etc.).
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS		Define synchronization monitoring requirement for all presentations: 1) Monitor all presentations against time standard, and 2) Monitor for relative synchronization across all presentations.	

Table B-17. FHA-RVP-MALF-3

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
RVP	RVP Malfunction: - Presentation of frozen visual information	Nominal (See Appendix C - System State)	HMI Provided to ATCT: Presented visual information is incorrect (i.e., not real-time information, not consistent with reality, etc.).
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls)		Define synchronization monitoring requirement for all presentations: 1) Monitor all presentations against time standard (absolute time monitoring), AND/OR 2) Provide visual presentation of an external "truth" image.	

- Pilot - Airport Personnel - ATCT - Overlying Facility - NAS		

Table B-18. FHA-SLF-LoF-1

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
SLG	SLG Loss of Function	Nominal (See Appendix C - System State)	Inability to provide visual signals to aircraft, vehicles, and/or personnel.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	This may be considered a "No Effect" failure scenario in the OHA because SLGs aren't used in the Nominal system state; however, the scenario is captured here for completeness.		

Table B-19. FHA-SLF-LoF-2

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
SLG	SLG Loss of Function	non-Nominal: loss or failure of 2-way radio communications between at least one aircraft, vehicle, or personnel and ATC	Inability to provide visual signals to aircraft, vehicles, and/or personnel.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	

Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	Intended to capture the following scenarios: 1) No-Radio (NORDO) aircraft, aircraft tuned to the wrong communication frequency, aircraft with failed/inoperative radios 2) ground vehicles and/or personnel with failed/inoperative radios.	

Table B-20. FHA-SLF-MALF-1

(1) **Function**	**(2)** **Function Failure Type**	**(3)** **System State**	**(4)** **Function Failure Effect(s)**
SLG	SLG Malfunction: Unintended signal sent to aircraft, vehicle, and/or personnel.	Nominal (See Appendix C - System State)	Unintended visual signal provided to aircraft, vehicles, and/or personnel.
(5) **Existing Controls**	**(6)** **Notes**	**(7)** **Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	Intended to capture a 'rogue SLG' scenario.		

Table B-21. FHA-SLF-MALF-2

(1) **Function**	**(2)** **Function Failure Type**	**(3)** **System State**	**(4)** **Function Failure Effect(s)**
SLG	SLG Malfunction: Incorrect signal sent to aircraft, vehicle, and/or personnel.	non-Nominal: loss or failure of 2-way radio communications between at least	Incorrect visual signal provided to at least one aircraft, vehicle, or personnel.

		one aircraft, vehicle, or personnel and ATC	
(5) **Existing Controls**	**(6)** **Notes**	**(7)** **Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	Unintended ATC guidance provided to: 1) NORDO aircraft, aircraft tuned to the wrong communication frequency, aircraft with failed/inoperative radios, etc. 2) ground vehicles and/or personnel with failed/inoperative radios.		

Table B-22. FHA-SLF-MALF-3

(1) **Function**	**(2)** **Function Failure Type**	**(3)** **System State**	**(4)** **Function Failure Effect(s)**
SLG	SLG Malfunction: Visual signal is unusable due to pointing/tracking error.	non-Nominal: loss or failure of 2-way radio communications between at least one aircraft, vehicle, or personnel and ATC	Inability to provide visual signals to aircraft, vehicles, and/or personnel.
(5) **Existing Controls**	**(6)** **Notes**	**(7)** **Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	Inability to visually communicate with: 1. NORDO aircraft, aircraft tuned to the wrong communication frequency, aircraft with failed/inoperative radios, etc. 2. Ground vehicles and/or personnel with failed/inoperative radios.		

Table B-23. FHA-SLF-MALF-4

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
SLG	SLG Malfunction: Inadvertent visual signal sent to aircraft, vehicle, or personnel during system installation, setup, or checkout.	Installation, Setup, maintenance, and/or Checkout.	Unintended visual signal provided to aircraft, vehicles, and/or personnel.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
	3. Intended to address potential hazard in a NON-OPERATIONAL system state.		

Table B-24. FHA-AAA-LoF-1

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
Audio	Audio Loss of Function	Nominal (See Appendix C - System State)	Inability of ATCT to hear AAA
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls 1. RVP Visual Information			

Table B-25. FHA-AAA-PLoF-1

(1)	(2)	(3)	(4)

Function	Function Failure Type	System State	Function Failure Effect(s)
Audio	Audio Partial Loss of Function	Nominal (See Appendix C - System State)	Failure of individual audio microphone and/or speaker. This results in inability of ATCT to hear AAA from section of airfield.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls 1. RVP Visual Information			

Table B-26. FHA-AAA-MALF-1

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
Audio	Audio Malfunction	Nominal (See Appendix C - System State)	AAA isn't "near real time" (e.g. delayed, out of synchronization with correct visual information, etc.). This results in misleading information provided to ATCT.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel			

- ATCT - Overlying Facility - NAS Specific Controls 1. RVP Visual Information		

Table B-27. FHA-AAA-MALF-2

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
Audio	Audio Malfunction	Nominal (See Appendix C - System State)	AAA is not spatially representative of reality (e.g. engine noise from the south appears to be coming from the north). This results in misleading information provided to ATCT.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls 1. RVP Visual Information			

Table B-28. FHA-AAA-MALF-3

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)

Audio	Audio Malfunction	Nominal (See Appendix C - System State)	Ambient audio quality or volume creates a distraction (e.g. volume stuck high, excessive noise, etc.).
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls 1. RVP Visual Information			

Table B-29. FHA-MDT-LoF-1

(1) Function	**(2) Function Failure Type**	**(3) System State**	**(4) Function Failure Effect(s)**
MDT	MDT Loss of Function	Nominal (See Appendix C - System State)	Inability to view system status information or control system via the MDT interface.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
N/A	May require orderly shutdown for system maintenance to diagnose and repair (i.e., forced loss of availability).	Define a requirement that loss of the MDT function should have no impact on the RVP in operational mode.	

Table B-30. FHA-MDT-LoF-2

(1) Function	**(2) Function Failure Type**	**(3) System State**	**(4) Function Failure Effect(s)**

MDT	MDT Loss of Function	Installation, Setup, maintenance, and/or Checkout.	Loss of system availability: Inability to bring system back to an operational state.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	Intended to address potential hazard in a NON-OPERATIONAL system state.		

Table B-31. FHA-MDT-MALF-1

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
MDT	MDT Malfunction: Inadvertent and un-annunciated alteration of OPERATIONAL configuration or system status (e.g., monitor parameters/thresholds, configuration settings, turn system "off").	Nominal (See Appendix C - System State)	Loss of system availability and integrity.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS	Intended to capture an OPERATIONAL system state.	1. Define a requirement for defined system modes (e.g., Operational, non-Operational, Maintenance/Test, OFF). 2. Define a requirement to disable the MDT ability to alter system status and configuration parameters when the system is an OPERATIONAL state. 3. Define a requirement for fail-safe system status changes (e.g., Operational-to-Non-Operational, Non-Operational-to-Operational, Operational-to-Test, etc.). 4. DAL of MDT function should be equivalent to its most critical functional interface.	

Table B-32. FHA-MDT-MALF-2

(1) Function	(2) Function Failure Type	(3) System State	(4) Function Failure Effect(s)
MDT	MDT Malfunction: Inadvertent and un-annunciated alteration of OPERATIONAL configuration or system status data/information (e.g., monitor parameters/thresholds, configuration settings, turn system "off").	Installation, Setup, maintenance, and/or Checkout.	Loss of system availability and integrity.
(5) Existing Controls	**(6) Notes**	**(7) Recommended Requirements and Design Constraints**	
	Intended to address potential hazard in a NON-OPERATIONAL system state.	1. Define a procedural requirement to confirm configuration settings have been loaded into the system appropriately prior to the system being placed in an Operational state. 2. DAL of MDT function should be equivalent to its most critical functional interface.	

Appendix C - Nominal System State

1. RT System deployments will require airports to be designated Class D airspace, requiring aircraft to be equipped with radios and pilots to establish and maintain communication with the RT controller. [Ref 14 CFR Part 91]
2. "RT System" only refers to the baselined set of equipment reviewed under the non-Federal Type Certification process; it does not include other/existing equipment used in the NAS (e.g., other ATCT equipment listed in an FCT MEL).
3. In addition to the RT equipment, the RTM will include the same equipment from the MEL required at towers today.
    a. The required MEL is dependent on the type of tower implemented (e.g. NFCT, FCT). [Ref 7210.78 Appendix A for FCT] [Ref AC 90-93B for NFCT]
    b. It is assumed that the MEL equipment is functioning as intended
4. Controllers will have the appropriate training to properly use the implemented RT system configuration.
5. ATC staffing levels for Class D towers are as described in FAA Order 7210.3.
6. Controllers will have the appropriate training and certifications to provide Air Traffic services in accordance with FAA Order 3120.4, 8000.90, 7110.65, and 7210.3 and with 14 CFR Part 65.
7. Each RT System will have an approved local safety case.
8. An SOP will be developed and in place at each RTC to establish a predefined ATCS reaction to apparent malfunctions.
9. An LOA will exist between the ATCT and other stakeholders as required.
10. Physical security requirements will be addressed during local SRM and commissioning procedures.
11. Proper charting and NOTAMs are in place to ensure that pilots are aware that a tower is present and operational.
12. The RT system (i.e., the baselined equipment being reviewed under the non-Federal Type Certification Process) will be managed and administered as a non-Federal facility:
    a. FAA inspectors will be trained to oversee maintenance and conduct annual inspections
    b. Non-Federal technicians will be trained with approved material and will be procured/compensated by the system sponsor
    c. The system sponsor will sign the required OMM / MOA package with the FAA
    d. Appropriate physical and information security requirements will be levied on the facility
    e. System may be located in a Federal facility, FCT, or a NFCT
13. Airport markings, signage, lighting, and security at airports providing Class D services will meet or exceed FAA standards.
14. Airports providing ATCT services will continue to experience typical changes in aircraft operations.
15. The RT system is designed to allow system operation by one or more controllers in accordance with the FAA JO 7210.3 (in particular, Chapter 2, Section 6) for the consolidation of control positions and staffing levels.
16. Reference Condition: Airfield Lighting and Visibility

a. Lighting and visibility conditions always refer to Visual Meteorological Conditions (VMC).
b. Procedures defined in 7110.65 adequately mitigate other lighting and visibility conditions.

17. Approved non-Federal RT system are visual display only systems that are not dependent on, or integrated with, other forms of surveillance (e.g., RADAR, Automatic Dependent Surveillance-Broadcast (ADS-B), Multilateration, etc.).
18. Controllers are assumed to act/re-act in a fault-free manner with respect to their RTM and operations training and the information presented to them by the RT system.
19. Pilots are assumed to act/re-act in a fault-free manner with respect to piloting the aircraft and responding to controller information/guidance/direction.

Appendix D - Tables and Figures

RVP loss of function was discussed during the RT WG meeting. The following Swiss cheese model was presented describing the potential controls in the “transition to ATC-Zero” hazard scenario.

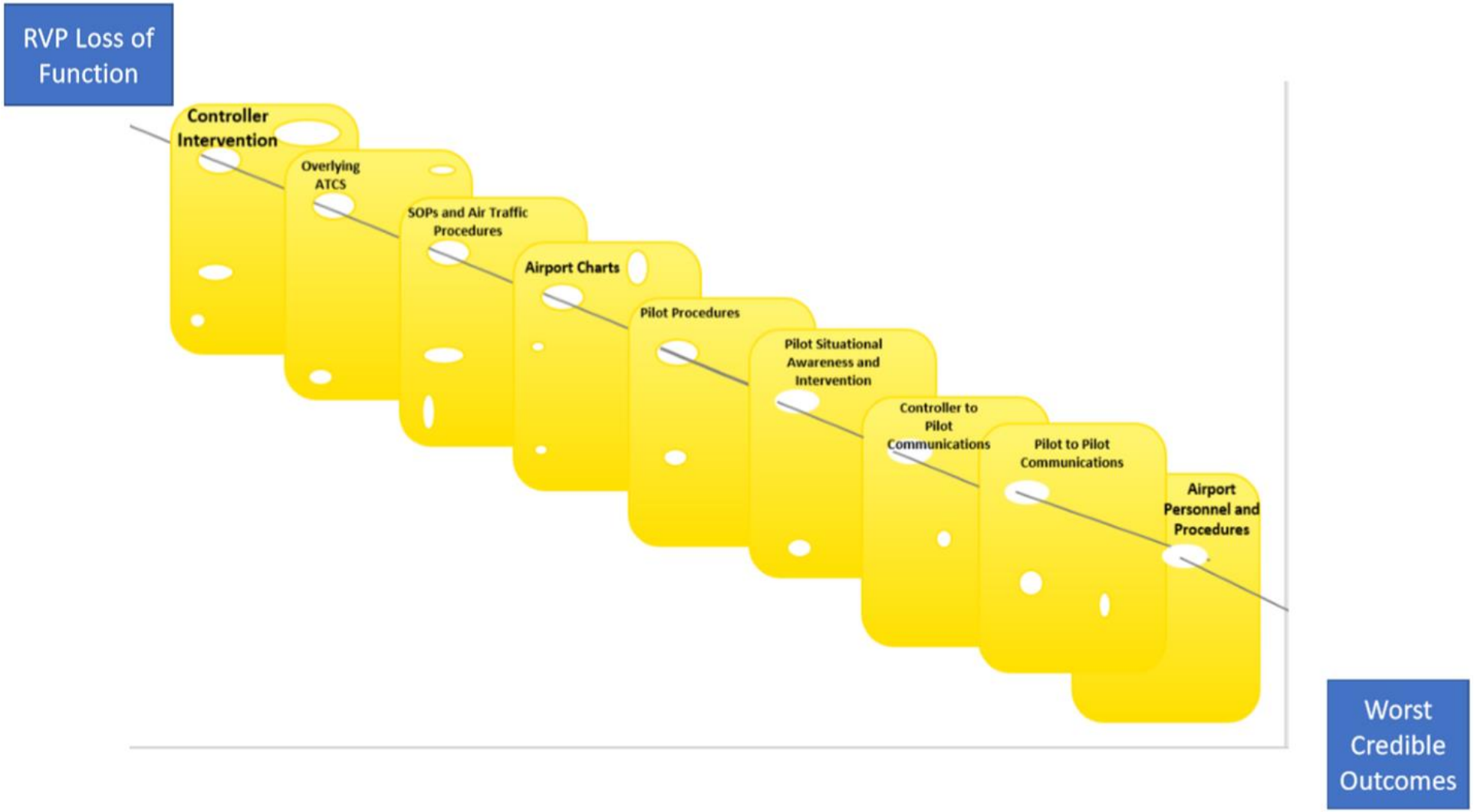

Figure D-1. RVP Swiss cheese Model

Figure D-2 was generated after a lengthy OSA WG discussion on June 3, 2020 regarding associated hazards resulting from a RVP LoF. The diagram was used as an aid to further the RVP LoF discussions during a June 8, 2020 OSA WG meeting.

An RVP LoF was associated with a simultaneous loss of the ability to detect and identify objects in the area of jurisdiction (e.g., runways, short finals, and base turns) and a loss of the ability to observe spatial relationships. The diagram attempts to capture several of the key points that SMEs raised during the discussion. The diagram was intended to support future discussions by depicting some of the potential system states and primary mitigations to be discussed/considered (i.e., to help identify the threat space). Several of these key points from the discussion are listed below:

- The idea of a primary exposure time associated with an RVP LoF hazard was expressed by multiple SMEs. The exposure time was identified to be the time from the self-annunciated RVP LoF (e.g., no usable visual information on the presented to the ATCS, screens go dark, etc.) until the ATCS can declare ATC-Zero over the tower communications system(s). The SMEs estimated that this time would be on the order of 60-120 seconds. The idea that ATCS would declare ATC-Zero immediately upon the RVP LoF event was rejected by multiple SMEs. (Note: At least one Subject Matter Expert (SME) thought that a delayed ATC-Zero declaration after an RVP LoF could result in a "snowball effect of hazards", but as this was not the majority opinion, the diagram depicts an exposure period perspective).

- No RVP LoF hazards were considered after ATC-Zero had been declared by the ATCS.

- The level of ATCS "stress" was assessed to be highest in the initial moments following an RVP Loss of Function. This increased stress was directly related to the loss of a primary source of information used to determine/maintain situational awareness.

- The level of ATCS stress was anticipated to decline over the 60-120 second period as increased ATCS-to-pilot communication helped to reestablish some ATCS situational awareness.

- The level of ATCS situational awareness was generally anticipated to decline after the loss of visual information from the RVP; although, it was noted that increased ATCS-to-pilot communication over time may help reestablish some level of situational awareness.

- The assessment of the hazard is dependent on the specific system states under consideration, the level of credit associated with existing mitigations (e.g., airport related controls, aircrew related controls, etc.), and the assessed credibility of several presumably independent events aligning in a hazardous way.

- The diagram does not depict all of the existing controls. For example, there is no attempt to depict the mitigation credit for airport controls for wildlife events (e.g., deer, birds, etc.) after an RVP LoF.

- After multiple hours of discussion over two different WG sessions, the SMEs were split between a minor and a major hazard severity classification for hazards associated with an RVP LoF.

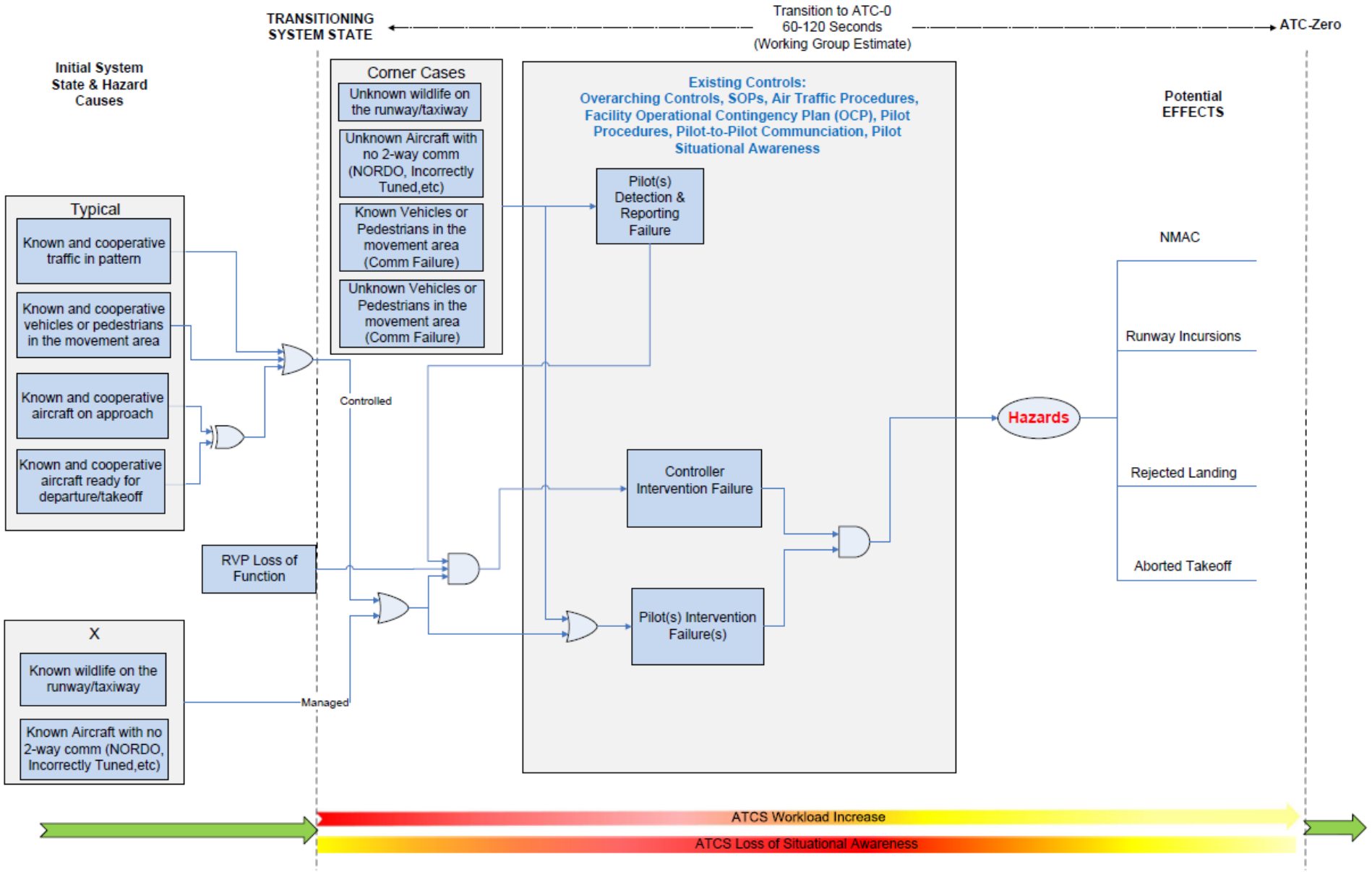

Figure D-2. Transition to ATC-Zero

Table D-1 is the severity table used by the ATO to assess the severity of a hazard when performing Safety Risk Management

Table D-1. Severity Table

	Hazard Severity Table *Note: Severities related to ground-based effects apply to movement areas only.*				
	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic[4] 1
	CONDITIONS RESULTING IN ANY ONE OF THE FOLLOWING:				
ATC Services	A minimal reduction in ATC services CAT D runway incursion[1] Proximity Event, Operational Deviation, or measure of compliance greater than or equal to 66 percent[2]	Low Risk Analysis Event severity,[3] two or fewer indicators fail CAT C runway incursion	Medium Risk Analysis Event severity, three indicators fail CAT B runway incursion	High Risk Analysis Event severity, four indicators fail CAT A runway incursion	Ground collision[5] Mid-air collision Controlled flight into terrain or obstacles
Flying Public	Minimal injury or discomfort to persons on board	Physical discomfort to passenger(s) (e.g., extreme braking action, clear air turbulence causing unexpected movement of aircraft resulting in injuries to one or two passengers out of their seats) Minor injury to less than or equal to 10 percent of persons on board[6]	Physical distress to passengers (e.g., abrupt evasive action, severe turbulence causing unexpected aircraft movements) Minor injury to greater than 10 percent of persons on board	Serious injury to persons on board[7]	Fatal injuries to persons on board[8]
NAS Equipment (with Table D-2)	Flight crew inconvenience	Increase in flight crew workload	Large increase in ATC workload	Large reduction in safety margin	Collision between aircraft and obstacles or terrain

	Slight increase in ATC workload	Significant increase in ATC workload Slight reduction in safety margin	Significant reduction in safety margin		
Flight Crew	Pilot is aware of traffic (identified by Traffic Collision Avoidance System traffic alert, issued by ATC, or observed by flight crew) in close enough proximity to require focused attention, but no action is required Pilot deviation[9] where loss of airborne separation falls within the same parameters of a Proximity Event or measure of compliance greater than or equal to 66 percent Circumstances requiring a flight crew to initiate a go-around	Pilot deviation where loss of airborne separation falls within the same parameters of a low Risk Analysis Event severity Reduction of functional capability of aircraft, but overall safety not affected (e.g., normal procedures as per Airplane Flight Manuals) Circumstances requiring a flight crew to abort takeoff (rejected takeoff); however, the act of aborting takeoff does not degrade the aircraft performance capability Near mid-air collision encounters with separation greater than 500 feet[10]	Pilot deviation where loss of airborne separation falls within the same parameters of a medium Risk Analysis Event severity Reduction in safety margin or functional capability of the aircraft, requiring crew to follow abnormal procedures as per Airplane Flight Manuals Circumstances requiring a flight crew to reject landing (i.e., balked landing) at or near the runway threshold Circumstances requiring a flight crew to abort takeoff (i.e., rejected takeoff); the act of aborting takeoff degrades the aircraft performance capability Near mid-air collision encounters with separation less than 500 feet[10]	Pilot deviation where loss of airborne separation falls within the same parameters of a high Risk Analysis Event severity Reduction in safety margin and functional capability of the aircraft requiring crew to follow emergency procedures as per Airplane Flight Manuals Near mid-air collision encounters with separation less than 100 feet[10]	Ground collision Mid-air collision Controlled flight into terrain or obstacles Hull loss to manned aircraft Failure conditions that would prevent continued safe flight and landing

1. Refer to the current version of FAA Order 7050.1, Runway Safety Program.
2. Proximity Events and Operational Deviations are no longer used to measure losses of separation, but they are applicable when validating old data. The minimal loss of standard separation is now represented as a measure of compliance of greater than or equal to 66percent.
3. Risk Analysis Event severity indicators are as follows:
    a. Proximity. Failure transition point of 50 percent of required separation or less.
    b. Rate of Closure. Failure transition point greater than 205 knots or 2,000 feet per minute (consider both aspects and utilize the higher of the two if only one lies above the transition point).
    c. ATC Mitigation. ATC able to implement separation actions in a timely manner.
    d. Pilot Mitigation. Pilot executed ATC mitigation in a timely manner.
4. An effect categorized as catastrophic is one that results in a fatality or fatal injury.
5. Ground Collision. An airplane on the ground collides with an object or person.
6. Minor Injury. Any injury that is neither fatal nor serious.
7. Serious Injury. Any injury that:
    a. Requires hospitalization for more than 48 hours, commencing within seven days from the date the injury was received;
    b. Results in a fracture of any bone (except simple fractures of fingers, toes, or nose);
    c. Causes severe hemorrhages, nerve, muscle, or tendon damage;
    d. Involves any internal organ; or
    e. Involves second- or third-degree burns, or any burns affecting more than five percent of the body's surface.
8. Fatal Injury. Any injury that results in death within 30 days of the accident.
9. Refer to *FAA Order JO 8020.11, Air Traffic Organization Aircraft Accident and Incident Notification, Investigation, and Reporting*, for more information about pilot deviations.
10. Near mid-air collision definitions are derived from *FAA Order 8900.1, Flight Standards Information Management System, Volume 7*, which defines the following categories: critical, potential, and low potential.

When assessing the severity of hazards related to NAS equipment, use the "NAS Equipment" row in Table D-1 in conjunction with Table D-2. Table D-2, the NAS Equipment Worst Credible Severity Table, is the starting point for severity assessments of NAS equipment. The severity of hazards that result from specific equipment changes may be lower or higher than the worst case presented in Table D-2 due to the possible controls that limit exposure or the interactions and dependencies that exist with other systems. Because effects of losses in equipment functionality and equipment malfunctions may not necessarily be traceable to a loss in separation, equipment safety effects may require separate assessment from operational effects (i.e., assess the severity of equipment loss or malfunction irrespective of operational severity).

The severity levels in Table D-2 are derived from the operational safety analyses and other documentation produced during initial safety assessments completed as part of the AMS processes that define severity based on the inherent functionality of systems. References to high or low traffic are relative indications during a period of time at any given facility [Ref: *FAA SMS]*.

Table D-2. NAS Equipment Worst Credible Severity Table[1]

Service	Functionality	Failure Condition / Hazard	Environment / System State	Effect	Worst Credible Severity / Rating
Surveillance	Aircraft/vehicle position	Loss of function	High Traffic	ATC loss of situational awareness	Major Significant reduction in safety margin
			Low Traffic		Minor Slight reduction in safety margin
		Malfunction	All	ATC makes decisions based on HMI	Major Significant reduction in safety margin
	Aircraft data	Loss of function	All	ATC loss of ability to differentiate among aircraft	Minor Significant increase in ATC workload
		Malfunction	All	ATC makes decisions based on incorrect aircraft identification information	Major Significant reduction in safety margin

[1] Risk should be assessed and determined with regard to its operational impact on the provision of air traffic management, communication, navigation, or surveillance services.

	Alerts	Loss of function	All	ATC not alerted when aircraft exceed established safety parameters	Major Significant reduction in safety margin
		Malfunction	All	False alarms	Minimal Slight increase in ATC workload
	Interfacility data	Loss of function	All	ATC transitions to manual methods	Minor Significant increase in ATC workload

Table D-3 was preserved from the initial draft of the Remote Towers OSA. NATCA and PASS both wrote informal dissenting opinions to the original minor severity, resulting in a follow up panel meeting on October 14, 2020. This allowed NATCA and PASS to further explain their rationales for believing the hazard severity to be major. The votes shifted to a five to four majority in favor of a major hazard severity. See section 3.4.1 for additional information.

Table D-3. RVP-LoF-1 OSA Version 1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
RVP-LoF-1	Partial or total loss of the capability to detect and identify objects / observe spatial relationships in the area of jurisdiction (i.e., runways, short finals, and base turns).	Equipment failure; Hardware design error; Software/Firmware design error; Installation, Setup/ Configuration Error	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS Specific Controls: - Controller intervention. - SOPs - Pilot training / intervention - Pilot-reported positions - Published flight advisories - Controller system experience. - Airport Personnel FOD prevention, detection, removal, evaluation, and reporting (Ref AC 150/5210-24). - Operational contingency plan (OCP) for transitioning to ATC-Zero
(6) Control Justification	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**

See Section 2.5 - Identified Controls	- Loss of all required ATC visual presentation
	  - ATC loss of situational awareness
	  - Significant increase in ATC workload
	  - Loss of ATC services requiring visual information
	- Transition to ATC-Zero in 60-120 seconds (estimate)
	- Aircraft under the direction of the RT will need to switch to uncontrolled tower procedures (e.g., Increase in flight crew workload)
	- Potential for CAT C runway incursion
		Minor	**Flight crew:**
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - Increase in flight crew workload
			- Two panel members dissented, stating that the severity should be defined as Major
			
			ATC:
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - CAT C runway incursion
			- One panel member dissented, stating the severity should be defined as Major
			
			NAS Equipment:
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
				SO1 - Define site-specific presentation areas that correspond to the area of jurisdiction. These critical areas need to be defined at each installation site.
				
				SO2 - Define appropriate site-specific ATCS reaction to this failure (i.e., transition to ATC-Zero) as required by FAA JO 1900.47.
				
				SO3 - Define a reliability requirement for the RVP based on NAS equivalent equipment performance or based on a derived risk allocation for the Loss of RVP Function.

			- Significant increase in ATC workload - Two panel members dissented, stating the severity should be defined as Major See Appendix E for Dissenting Opinions For more details see Section 3.4 Final Hazards and Deliberation Notes	

Table D-4 was preserved from the initial draft of the Remote Towers OSA. Since the panel previously determined that this malfunction case is of the same severity (Major) as the RVP LoF case, the severity of MDT-MALF-1 also became major.

Table D-4. MDT-MALF-1 OSA Version 1

(1) OHA Hazard ID	(2) Hazard Description	(3) Cause	(4) System State	(5) Controls
MDT-MALF-1	Loss of system availability during operations.	MDT Malfunction: Hardware failure, software design error, firmware failure, etc.	Nominal (See Appendix C - System State)	Overarching NAS Controls are active (See Section 2.5 - Identified Controls) - Pilot - Airport Personnel - ATCT - Overlying Facility - NAS
(6)	**(7) Effect**	**(8) Severity**	**(9) Severity Rationale**	**(10) Safety Objectives**

Control Justification				

See Section 2.5 - Identified Controls	- MDT Malfunction: inadvertent transition to non-operational state
	- Operational effect equivalent to RVP-LoF-1 (directly below)
	  - Loss of all required ATC visual presentation
	  o ATC loss of situational awareness
	  o Significant increase in ATC workload
	  o Loss of ATC services requiring visual information
	  - Transition to ATC-Zero in 60-120 seconds (estimate)
	  - Aircraft under the direction of the RT will need to switch to uncontrolled tower procedures (e.g., Increase in flight crew workload)
	  - Potential for CAT C runway incursion
	- Potential for additional functional losses (e.g., AAA, SLG, etc.)
		Minor	**Flight crew:**
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - Circumstances requiring a flight crew to reject landing (i.e., balked landing) at or near the runway threshold
			- Two panel members dissented, stating that the severity should be defined as Major
			
			ATC:
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - CAT C runway incursion
			- One panel member dissented, stating the severity should be defined as Major
			
			NAS Equipment:
			- Assessed effects are consistent with effects defined in SMS Table 3.3 for the stated severity classification
			  - Significant reduction in safety margin
				SO1 - Define a requirement for fail-safe system status changes (e.g., Operational-to-Non-Operational, Non-Operational-to-Operational, Operational-to-Test, etc.).
				
				SO2 - DAL of MDT function should be equivalent RVP loss of function severity.

			See Appendix E for Dissenting Opinions For more details see Section 3.4 Final Hazards and Deliberation Notes	

Appendix E - Dissenting Opinions

ANG-C5 Dissenting Opinion on RVP-MALF-3

Hazard: RVP-MALF-3 – Hazardous Misleading Information (HMI) provided to ATCT controller: Presented visual information is not real-time: presentation of frozen visual information.

Panel Severity Rating: Major

ANG-C5 Severity Rating: Minor

Severity Rating Rationale:

Example #1: Frozen screen(s) during an interaction between an approaching aircraft and a departing aircraft

The primary example brought up by the panel of how a frozen display could cause a hazardous situation was that there is an aircraft on final approach and an aircraft holding short that has been cleared for takeoff. The screen(s) displaying the departing aircraft freeze, making it appear as if the aircraft is still holding short. The controller becomes distracted and does not initially notice that the departing aircraft appears to still be holding short of the runway. The majority of the panel believed that by the time the situation is observed by the controller and the departing aircraft's takeoff clearance is cancelled, this could cause a Category B Runway Incursion, which is a major hazard.

ANG-C5 believes this event as described is not a credible scenario, and even if it were to occur, the severity would be minor at worst. Based on experience at the Leesburg and Fort Collins Remote Tower pilot projects, it is easy to notice a frozen screen quickly due to the lack of trees/flags blowing in the wind, cloud inactivity, frozen aircraft/vehicle movement, or general lack of any pixel movement whatsoever on the screen. In addition, the required visual presentation (360 degree view) of known systems includes views of both an arrival on final and traffic holding short of a runway on the same screen and it seems far-fetched to expect otherwise. Thirdly, given the time period of this scenario, the departing aircraft would progress to an adjacent and operational screen before a concern would arise. Consequently, we do not believe this scenario example is applicable to determining severity for this hazard and we believe the panel should reconsider.

ANG-C5 also believes there are strong controls inherently in place to avoid a major hazard and that a major severity is not a credible outcome. Controllers are trained to scan areas of jurisdiction, particularly when compliance to instructions is critical to safety (e.g., ensuring runway separation). Therefore it is not realistic to say that significant time would lapse before a controller took notice that a departure cleared for takeoff was not moving and took steps to address that situation. In addition to controller training, an overarching control in the NAS is pilot training to see and avoid other aircraft. Pilots are attentive in the vicinity of airports and are trained to scan a runway prior to landing. They are also trained to scan the final approach before taxiing onto a runway to avoid any significant potential for collision.

The specific example brought up by the panel assumes all of the following: 1) the frozen screen is not detected, 2) the aircraft holding short of the runway is on a separate screen than the aircraft on final, 3) that ATC will not quickly notice the aircraft cleared for takeoff is not moving, 4) that the departing aircraft will not soon appear on an adjacent operational screen, and 5) that the approaching aircraft is too far into the approach for the controller to issue alternative instructions to the arrival and/or contact the departing aircraft and be informed of the departing aircraft true status.

In the extremely unlikely event that all of these controls fail, there are three distinct potential outcomes:

1. The aircraft informs ATC it actually has departed already or the controller observes the departing aircraft progress to an adjacent operational screen (not a dangerous situation) and ATC becomes aware of the frozen display, resolving the hazard.
    - Hazard severity: **Minimal**
2. The aircraft did not follow instructions, has not yet departed, and is still holding short of the runway. ATC cancels the take-off clearance and tells the aircraft to hold short of the runway the same way as if the screen had not frozen.
    - Hazard severity: **Minimal**
3. ATC cancels the take-off clearance and tells the aircraft to hold short of the runway. The aircraft responds to ATC that it is already rolling or airborne. This is the most hazardous situation and the departing aircraft may already be in a critical phase of flight. Although it is a confusing situation and not ideal, the controller can resort to requesting pilot reports (departure airborne and turning) to ensure runway separation and/or issue alternative instructions to the arrival (e.g. 360 turn, go-around and fly parallel the runway report traffic in sight). This would likely resolve the situation and the departure would soon be observed on an adjacent operational screen.
    - Hazard severity: **Minor (Category C Runway Incursion)**

Example #2: Frozen screen(s) while there are no moving aircraft initially present
Alternatively, the screen freezes when there are no moving aircraft in the controller's area of jurisdiction. If an arriving aircraft enters the airspace or an aircraft wishes to depart, the pilot is required to contact ATC. In this situation, ATC would be able to identify that a screen is frozen prior to there being any hazardous interaction between two aircraft.

- Hazard severity: **Minimal**

Appendix F - References

1. DO-264, *Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications*, RTCA, December 14, 2000.
2. DO-278, *Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems*, December 13, 2011.
3. DO-254, *Design Assurance Guidance for Airborne Electronic Hardware*, April 19, 2000.
4. ED-240A, *Minimum Aviation System Performance Standards (MASPS) for Remote Tower Optical Systems*, EUROCAE, 12 November 2018.
5. *Safety Management System (SMS) Manual*, FAA Air Traffic Organization, April 2019.
6. *Remote Tower System: Generic Hazards, Version 1.0*, FAA Office of NextGen.
7. *Level 3 Concept of Operations Remote Tower Services at VFR Towers*, Version 3, May 2019.
8. *SRMGSA: Safety Risk Management for System Acquisition*, FAA Air Traffic Organization, March 2020.
9. Overarching Remote Tower System Research Operational Visual Requirements.
10. *National Runway Safety Plan*: 2015-2017, FAA.
11. *Order 8020.11D, Aircraft Accident and Incident Notification, Investigation, and Reporting*, FAA, 5/10/2018.
12. FAA Order 7110.65, *Air Traffic Control.*
13. FAA Order 7210.3, *Facility Operation and Administration.*
14. FAA Order 7210.78, *FAA Contract Tower (FCT) New Start and Replacement Tower Process.*
15. FAA Order 3120.4, *Air Traffic Technical Training.*
16. FAA Order 8000.90, *Air Traffic Safety Oversight Credentialing and Control Tower Operator Certification Programs*
17. FAA Order 1900.47, *Air Traffic Control Operational Contingency Plans*
18. FAA Guide to Ground Vehicle Operations: A Comprehensive Guide to Safe Driving on the Airport Surface.
19. *Visual Job Analysis of Airport Traffic Control Towers: Class D Airspace and Visual Flight Rules, Fort Hill Group, February 2016.*
20. 14 CFR Part 91, *General Operating and Flight Rules*.
21. FAA Advisory Circular 90-93B, *Operating Procedures for Airport Traffic Control Towers (ATCT) that are not Operated by, or Under Contract with, the United States (Non-Federal).*
22. FAA-G-2100G, *Electronic Equipment General Requirements*, May 9, 2005.
23. AC 150/5210-24, *Airport Foreign Object Debris (FOD) Management.*
24. National Airspace System (NAS) Voice Recorder (NVR) Preliminary Hazard Analysis (PHA), Version 1.1, June 14, 2019

Appendix G - Acronym List

AAA	Ambient Airfield Audio
AC	Advisory Circular
ADS-B	Automatic Dependent Surveillance-Broadcast
ASOR	Allocation of Safety Objectives and Requirements
ATC	Air Traffic Control
ATCS	Air Traffic Control Specialist
ATCT	Airport Traffic Control Tower
ATM	Air Traffic Management
CIC	Controller in Charge
CNS	Communication, Navigation, Surveillance
DAL	Design Assurance Levels
FA	Functional Analysis
FAA	Federal Aviation Administration
FCT	Federal Contract Tower
FFBD	Functional Flow Block Diagram
FOD	Foreign Object Debris
HMI	Hazardously Misleading Information
IFR	Instrument Flight Rules
LOA	Letter of Agreement
LoF	Loss of Function
MDT	Maintenance Data Terminal
MEL	Minimum Equipment List
MOA	Memorandum of Agreement
MSL	Mean Sea Level
MTBCF	Mean Time Between Critical Failure
NAS	National Airspace System
NFCT	non-Federal Federal Control Tower
NORDO	No-Radio
NOTAM	Notice to Airmen
OCP	Operational Contingency Plan
ODO	Opposite Direction Operations
OHA	Operational Hazard Assessment
OMM	Operations and Maintenance Manual
OSA	Operational Safety Assessment
OSED	Operational Services and Environment Description
OVR	Operational Visual Requirements
PLoF	Partial Loss of Function
PTZ	Pan-Tilt-Zoom
RI	Runway Incursion
RT	Remote Tower
RTC	Remote Tower Center
RTCA	Radio Technical Commission for Aeronautics
RTM	Remote Tower Module
RVP	Required Visual Presentation
SLG	Signal Light Gun
SME	Subject Matter Expert

SMS	Safety Management System
SOP	Standard Operating Procedure
SRMGSA	Safety Risk Management Guidance for System Acquisition
TR	Technical Requirement
VFR	Visual Flight Rules
VMC	Visual Meteorological Conditions