In-time Safety Management Capabilities for Wildland Fire Management Aircraft Operations - A Gap Assessment

Patricia Revolinsky*, Evan Dill†, Steve Young‡, Ersin Ancel§ and Samantha I. Infeld¶
NASA Langley Research Center, Hampton, VA, 23681, USA

This study assesses the in-time safety management services, functions, and capabilities (SFCs) being investigated by NASA's System Wide Safety (SWS) project to determine applicability to the project's planned safety demonstrator (SD-1) for wildland fire management. The purpose of this work is to evaluate how effectively existing SFCs address the different hazards presented by a safety demonstrator operating in a wildland fire management scenario. This will help inform decision makers which SFCs would provide the most cost-effective solutions to fill the hazard gaps for further research. Hazards for the safety demonstrator wildland fire management scenario were collated, and the SFCs were evaluated for each hazard based on how applicable and effective the unmodified SFCs are at addressing the hazard. The SFCs are also evaluated for the gap type that needs to be addressed to improve the SFC effectiveness for the given hazard. The key finding of this assessment is that all the existing SFCs require at least some research and development to adapt to the safety demonstrator. No single SFC fully addresses any of the safety demonstrator operation hazards. The result of this study will be used to determine the performance of current SFCs and suggest strategies to adapt existing SFCs or add new SFCs.

I. Background

In recent years, an In-time Aviation Safety Management System (IASMS) Concept of Operations (ConOps) has been defined and has matured to a consensus via industry workshops and outreach. An architecture and initial set of relevant information classes for monitoring has also been defined. The concept assumes a set of enabling Services, Functions, and Capabilities (SFCs) will perform the monitoring and support more timely safety risk assessment and mitigation. The IASMS concept is intended to be tailorable wherein the set of enabling SFCs may vary due to a use-case's mission, vehicle platform(s), operational environment, and safety risk tolerance. Because wildland fire management has been selected by the System-Wide Safety (SWS) project as the use-case for its first Safety Demonstrator (SD-1), the scope of such tailoring needs to be determined. As part of this process, this gap assessment identifies where additional SFC research and development may be needed beyond SFCs developed and tested at NASA to date. The current gap assessment did not look across industry developments to determine which commercial-off-the-shelf (COTS) products may provide the needed SFCs. Existing knowledge of COTS solutions informed the assessment, but a comprehensive state-of-the-commercial-industry study for each SFC is not in the scope of this work. This assessment is ongoing and further research into COTS solutions and efforts by other entities is in work for future reporting.

This section provides a background of the IASMS ConOps relevant to the SWS wildland fire management (WFM) safety demonstrator and describes the connection between the ConOps hazards and the SFCs for this gap assessment. The remainder of this paper shares the key assumptions, constraints, and derivation of the SFCs that inform the gap assessment; additionally, it shares the results of the gap assessment for SFC applicability, coverage, and implied need for addressing hazards. The paper then concludes with recommendations based on the results of the gap assessment.

A. ConOps for Wildland Fire Management Aircraft Operations (WFM-AO)

For SD-1, it is assumed that WFM flight operations are highly autonomous and include multiple aircraft (manned and unmanned) flying in defined airspace above active wildland fires. We consider operations that are in a mid-term context (i.e., 3-5 years from today) in a medium-density air traffic (i.e., 10-15 aircraft within the WFM-AO. In this context, WFM participants use aircraft assets similar to what exists today but which are difficult to acquire or are

*Aerospace Engineer, Aeronautics Systems Analysis Branch, MS 442, AIAA Member.
†Aerospace Engineer, Safety-Critical Avionics Systems Branch, MS 234, AIAA Member.
‡Aerospace Engineer, Safety-Critical Avionics Systems Branch, MS 234, AIAA Fellow.
§Assistant Branch Head, Aeronautics Systems Analysis Branch, MS 442, AIAA Member.
¶Aerospace Engineer, Engineering Integration Branch, MS 290, AIAA Associate Fellow.

underutilized due to constraints (e.g., procedural, policy, operational, technology limitations, and safety concerns). For example, all small Unmanned Aircraft System (sUAS) used in current WFM operations are flown strictly within Visual Line-of-Sight (VLOS); this is due to policy constraints as well as safety concerns. However, the vehicles may be safely flown without this constraint if appropriate risk mitigation steps are applied. Similarly, there is a desire to operate existing large Unmanned Aircraft System (UAS) above the WFM-reserved airspace and to coordinate this operation with operations occurring within the reserved airspace. Non-segregated operations are the desired future (e.g., sUAS, manned C-130s, and large UAS all safely operating different missions within the temporary flight restriction (TFR) airspace). For example, the UAS (small and large) would not have to stop performing their missions as a C-130 executes a fire-retardant mission. However, allowing aircraft to roam within the TFR (or even outside the TFR) in a self-managed, autonomous way is considered longer term and not in scope for this use case. For more details, see the WFM-AO ConOps found in Ref. [1].

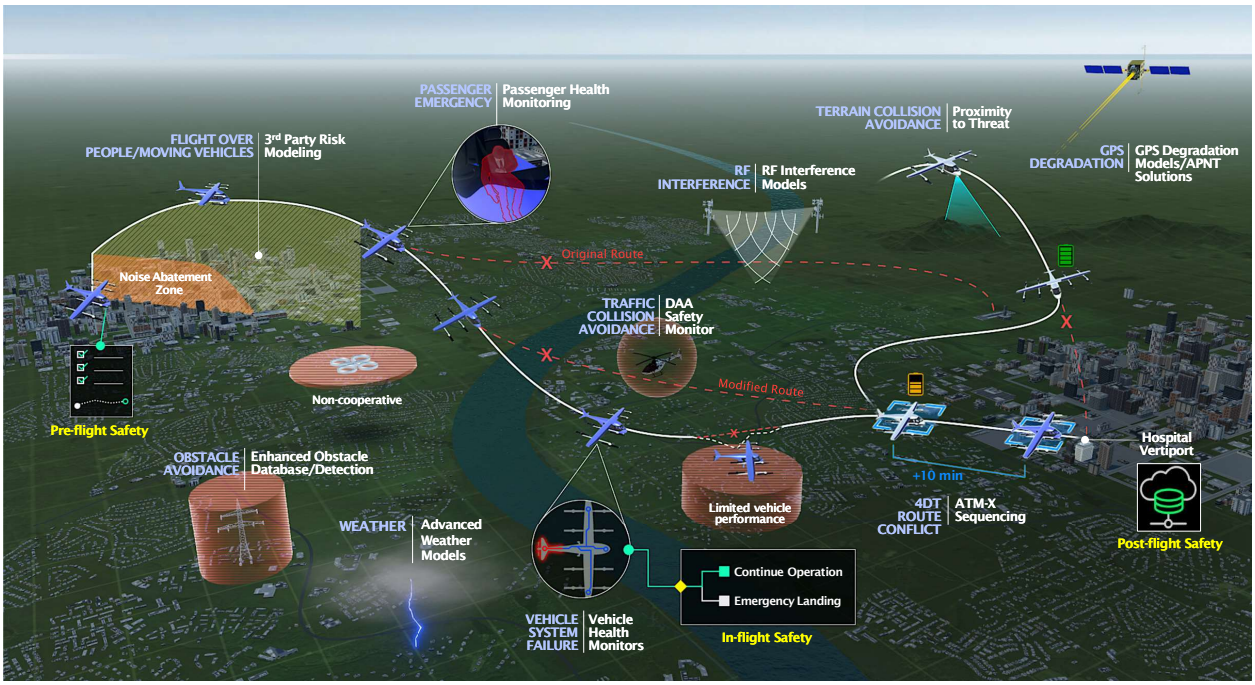

Fig. 1 IASMS operational view.

B. ConOps for In-Time Aviation Safety Management System (IASMS)

The IASMS ConOps assumes significant information sharing and a set of SFCs that work in concert to mitigate safety risk during flight operations. Operational mitigations occur during pre-flight (i.e., via advanced flight planning SFCs), in-flight (e.g., via supervisory and automated functions that may re-direct aircraft to reduce risk exposure), and post-flight (e.g., functions that monitor for precursors, anomalies, and trends when comparing with previous similar flights) [2, 3]. The types of information that may be shared to enable these SFCs are shown in Fig. 1 [2]. The hazards to be addressed and the SFCs needed to address them are envisioned to result from stakeholder efforts (e.g., manufacturers, operators, users, and government authorities). A model-based view of IASMS hazard management capabilities from the 2022 IASMS ConOps can be seen in Fig. 2. The starting point for a gap assessment is tracing service and function relevance to desired hazard management capabilities, as shown in Fig. 3.

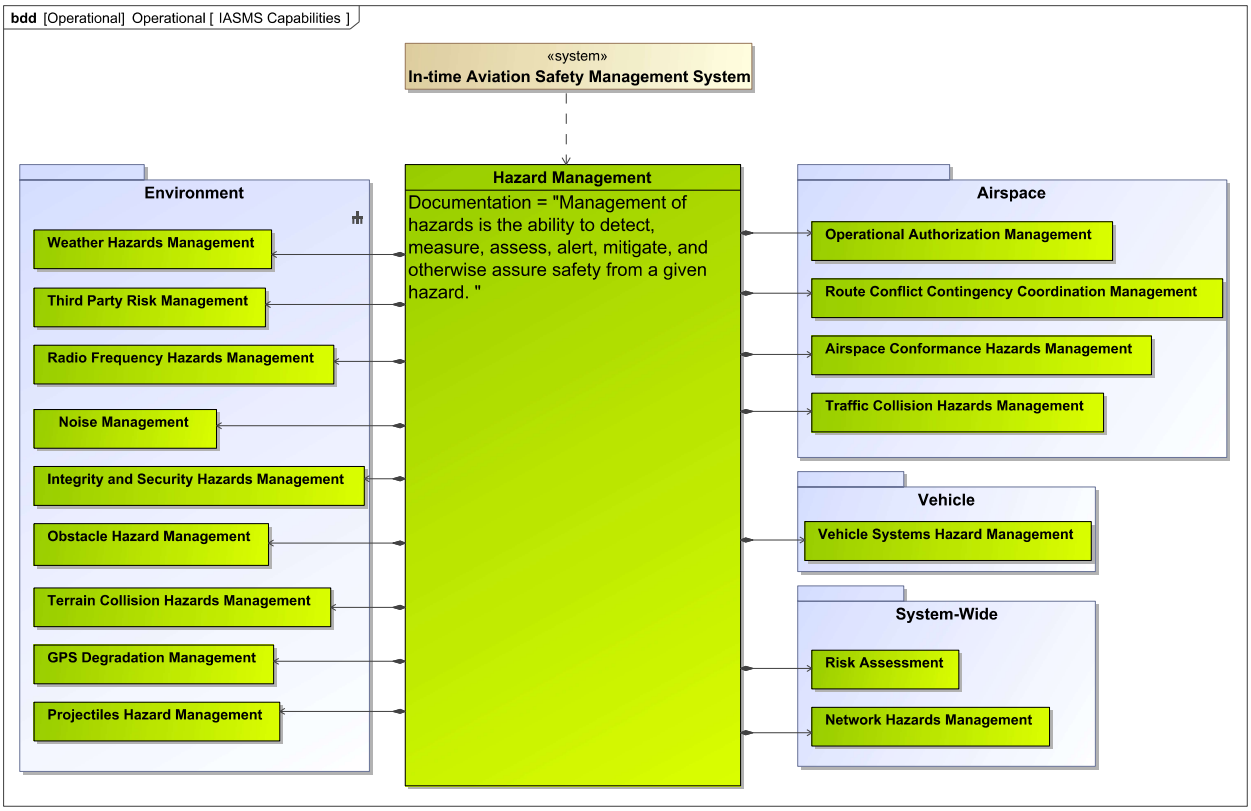

Fig. 2 Example IASMS hazard management capabilities.

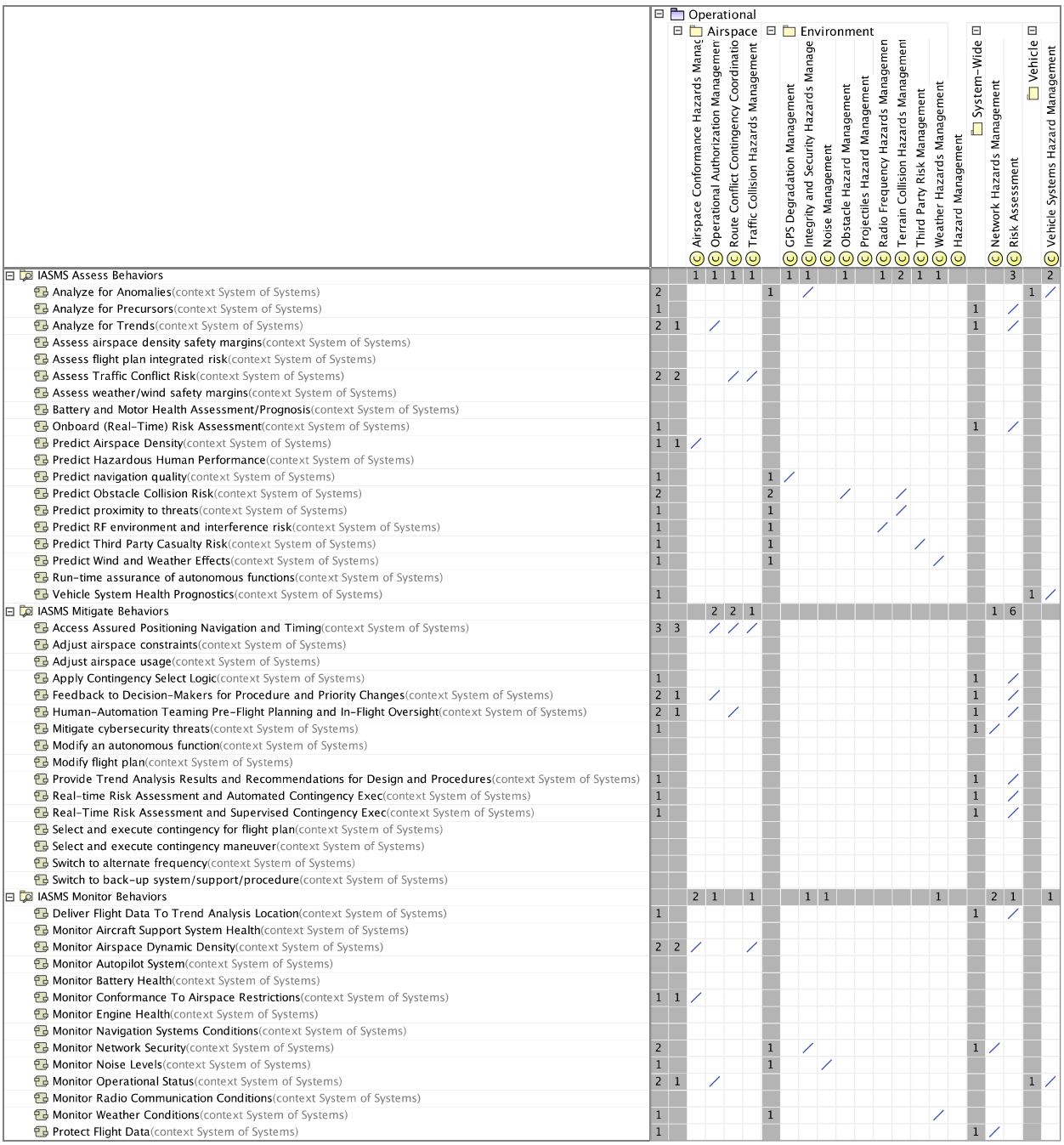

Fig. 3 Example IASMS services and functions mapped to hazard management capabilities.

II. Gap Assessment Setup

The hazards and SFCs in this work were derived from those identified in earlier efforts, including NASA partnerships with industry, workshops, and previous NASA SWS research [1, 3]. Both hazards and SFCs from these efforts were adjusted further for use in the WFM safety demonstrator.

A. Assumptions

1. Human Roles

We assume no significant changes to the roles of humans in WFM-AO when an IASMS has been implemented. The only change may be allowance for automated mitigation (by aircraft) if a safety metric threshold is exceeded and there is not sufficient time for the operator to either (a) intervene/takeover or (b) review/approve a mitigation suggested by automation. The level of oversight provided to automated systems may depend on the UAS platform and its mission. For example, for the small Unmanned Aircraft System (sUAS) it may be feasible to have a shifting locus of control that migrates some of the authority and responsibility from the remote pilot/operator to an automated function (e.g., onboard auto-pilot). However, for large UAS this may not be feasible as they may be interacting at the same altitudes as manned aircraft.

2. Top Priority Safety Risks

1) Risk of personal injury
    - *1st party risk:* Risk to individuals onboard a WFM-AO aircraft. Only applicable to manned aircraft participating in the operation.
    - *2nd party risk:* Risk to individuals on other aircraft (i.e., collision risk). May involve aircraft that are not part of the WFM-AO operation.
    - *3rd party risk:* Risk to individuals on the ground (and not in an aircraft); this includes non-participants.
2) Risk of property damage and/or hull loss
    - Property damage may be the aircraft as well as what it collides with (e.g., critical infrastructure)
    - Hull loss may not include any other damage (e.g., a crash into the ocean)

Note: In the context of this paper, risk is defined as the product of likelihood and severity. Personal injury and property damage may occur simultaneously.

B. Constraints

The IASMS ConOps assumes there are many operations generating a substantial amount of data. It also assumes safety benefits grow with time in service and operations. Until substantial operational data is available, research and development activities will be constrained to using historical data and/or data collected during testing.

It is difficult to baseline current WFM systems. This work uses only results from the SWS WFM workshop in 2022 [4] and would benefit from further information and partnerships with WFM practitioners and organizations.

C. Gap Assessment Objectives

Given the IASMS ConOps and a WFM ConOps, as well as the underlying aviation systems that are enabling these operations, the objectives of this analysis include the following:

a. Assessing the availability of IASMS information classes (pre-flight, in-flight, post-flight)
b. Assessing SFC coverage (monitor SFCs, assess SFCs, mitigate SFCs)
c. Assessing SFC R&D coverage
d. Identifying gaps in the prior three areas

D. Identifying Hazards

General hazard types for increasingly autonomous aviation operations were presented in the IASMS capabilities for hazard management as shown in Fig. 2. A subset of these applying to sUAS operations was previously derived and given in Refs. [5, 6]. For the gap analysis activity, precursors to these hazards specific to the wildfire environment were also considered. Engineering judgement, feedback from the SWS wildland firefighting workshop, and expert solicitation were utilized to collect hazards related to aviation in wildfire scenarios. These hazards are listed in Table 1.

The hazards are sorted by condition: hazards that can trigger other hazards (precursors), hazards that are caused by other hazards (undesirable outcomes), and hazards that encompass both precursors and undesirable outcomes (overarching).

Table 1 Wildfire scenario hazards for aviation operations

Precursors	
Loss of power (electrical)	Radio Frequency Interference (RFI)
Loss of propulsion	Fire related hazard (e.g., smoke, ash, heat, etc.)
Loss of C2/TM (command & control/telemetry) link	Hazardous weather (e.g., fire weather, weather caused by fire, such as pyrocumulonimbus, excessive wind, windshear, convection, lightning, etc.)
Loss of navigation	Weather (e.g., wind, turbulence, convection, etc.)
Loss of surveillance	Airspace non-conformance
Loss of control	Operator safety alerts (SA) and alerting
Flight path (or flight plan) deviations	Wildlife (e.g., birds)
Structural (e.g., damage)	Procedural error (e.g., omission/commission, in-flight vs pre-flight) [Human Factor]
Excessive vibration	Procedural error (e.g., technical, onboard, software, etc.)
Auto-pilot failure (software)	Operator issues (e.g., incapacitated, distracted, fatigued, etc.)
Overarching	
Insufficient information availability	Malicious interference (physical)
Insufficient data integrity (including inadequate information sharing)	Malicious interference (cyber)
Undesirable Outcome	
Loss of separation (terrain)	Loss of separation (3rd party)
Loss of separation (non-terrain obstacle)	Mission failure
Loss of separation (traffic)	

III. Evaluation of Services Functions, and Capabilities (SFCs)

A. SFCs

The applied SFCs are listed in Table 2. These SFCs were developed as part of NASA R&D for use in a related mission class (i.e., low altitude, highly autonomous urban flight operations) [6].

Table 2 NASA SWS SFCs

Offboard SFCs	Operator/User interface
	---Research Display Concept 1 (RD-1)
	---Research Display Concept 2 (RD-2)
	---Research Display Concept 3 (RD-3)
	Battery Prognostics (BP) service
	Proximity to Threat (PtT) service
	Airspace dynamic density service
	Obstacle collision risk service
	3rd party casualty risk service - Non-Participant Casualty Risk Assessment/Ground Risk Assessment Service Provider (NPCRA/GRASP) (pre-flight)
	3rd party casualty risk service - Non-Participant Casualty Risk Assessment/Real-Time Risk Assessment (NPCRA/RTRA) (in-flight)
	Radio frequency interference/radio frequency energy (RFI/RFE) service (pre-flight and in-flight)
	---Model-based service
	---Observations (via spectrum monitoring stations) service
	Navigation Quality 1 - NavQ - Corridor Assessment Prognostic Service (CAPS)
	Navigation Quality 2 - NavQ - Geometric Assessment Prognostic Service (GAPS)
	Wind service
Onboard SFCs	Risk Assessment 1 (Real-time Risk Assessment - RTRA-based) function
	Risk Assessment 2 (PtT-based) function
	Contingency Select & Trigger (CST) function
	Constraint Monitor (Safeguard) function
	Battery Health Monitor (BHM-1) (Electrochemical model) function
	Battery Health Monitor (BHM-2) (Electrolytic Capacitor - EC model) function
	Link Monitor function
	Auto-pilot Monitor (Co-pilot based) function
	Traffic and Run-Time Assurance (RTA) Monitor (Independent Configurable Architecture for Reliable Operations of Unmanned Systems - ICAROUS) function
	Diagnostic Reasoner/Anomaly Detector (DR-AD-1) function
	Diagnostic Reasoner/Anomaly Detector (DR-AD-2) function
	Aircraft and flight system state telemetry service (TMS)

The gap analysis here is analogous to the analysis at the IASMS ConOps level for SFCs to address identified hazards [2]. Here it was applied for the IASMS and its SFCs appropriate to the WFM-AO and the hazards more specific to that scenario. The SFCs and risks, hazards, and precursors are specialized versions of their equivalents at the IASMS ConOps level and the information learned through this application will in turn help refine the IASMS ConOps. Figure 4 shows the allocation of the IASMS general SFCs to the SWS R&D SFC implementations.

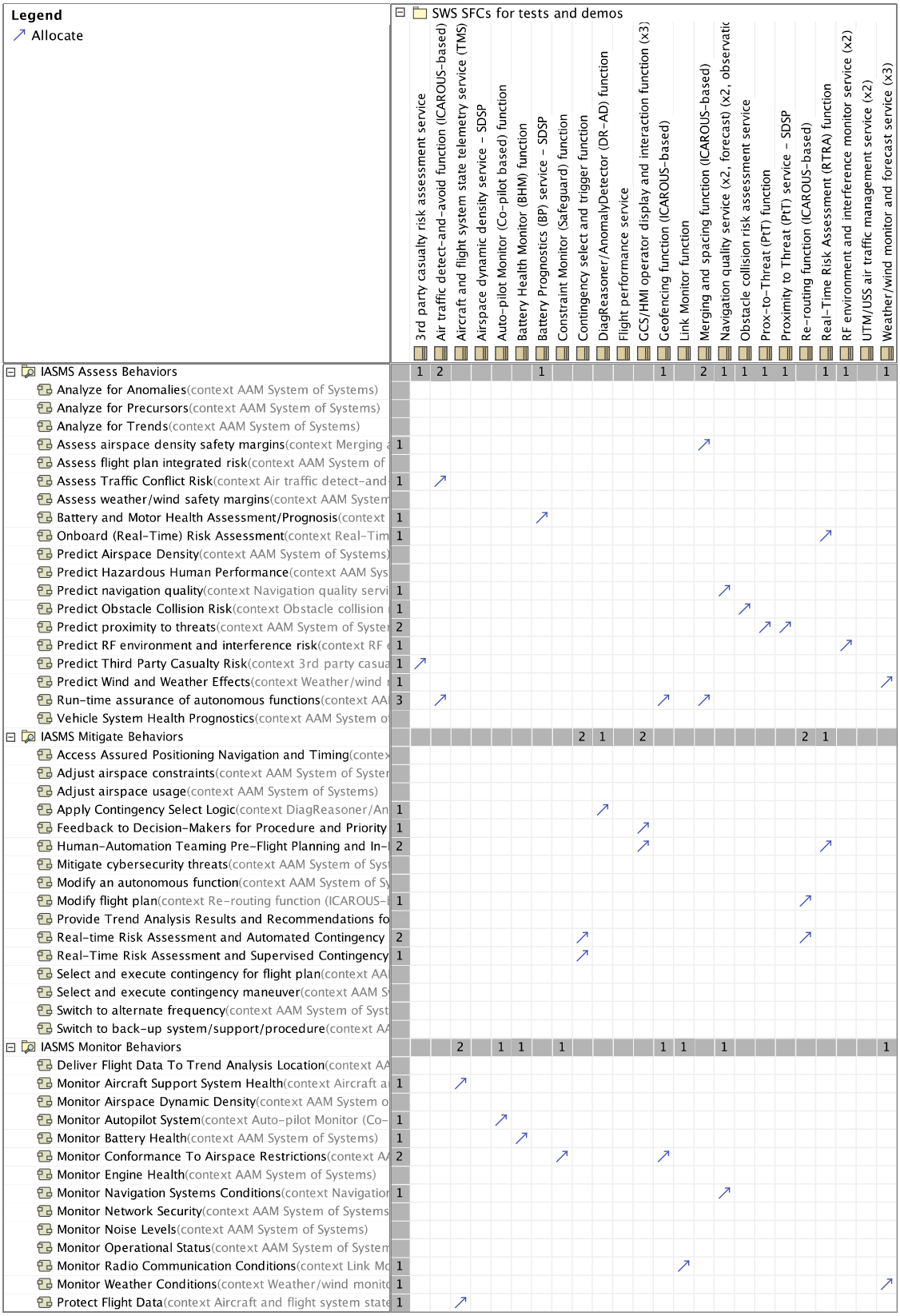

Fig. 4 IASMS SFCs allocated to low altitude urban flight SFCs.

B. Gap Assessment of SFCs

The existing SFCs were evaluated and adjusted for the needs of a WFM demonstration (i.e., SD-1). The set of SFCs used for the assessment consists of the SFCs listed in Table 2, SFCs developed from the WFM workshop, and additional SFCs suggested by specialists during reviews.

The list of SFCs given in Table 2 includes different methods to achieve the same functionality. For the gap assessment, SFCs with similar capabilities were combined into a single SFC for each capability, as listed in Table 3. These combinations were made to reduce the time dedicated to evaluating each hazard. For example, the SFCs for "Navigation Quality 1" and "Navigation Quality 2" are different approaches to provide similar functionality. "Navigation Quality 1" and "Navigation Quality 2" were combined into a single SFC category: "Navigation Quality (NavQ) (x2) service." The "(x2)" in the new SFC indicates that multiple related SFCs can be characterized by the listed moniker. Note that the functions are not identical, and this grouping is not intended to imply that some SFCs are unnecessary.

SFCs were divided by where the function is performed and given a corresponding alphanumeric identifier for ease of reference.* Offboard SFCs are capabilities performed by systems *not* on the sUAS, such as within a ground control station. Onboard SFCs are capabilities performed by systems on the sUAS, such as software collecting data from flight hardware all on board the sUAS.

Table 3 Finalized SFCs for gap assessment

OFfboard SFCs	F1	Ground control station/human-machine interface (GCS/HMI) Display Concepts (x3)
	F2	Battery Prognostics (BP) service – supplemental data service provider (SDSP)
	F3	Proximity to Threat (PtT) service - SDSP
	F4	Airspace dynamic density service - SDSP
	F5	Obstacle collision risk service - SDSP
	F6	3rd party casualty risk service – (NPCRA/GRASP)(in/pre-flight) – SDSP
	F7	RFI/RFE service (per-flight and in-flight) (x2) – SDSP
	F8	Navigation Quality (NavQ) (x2) service
	F9	Wind/Weather service (includes local and weather station observations)
	F10	Flight performance service
	F11	Unmanned Aircraft System (UAS) Traffic Management (UTM)/UAS Service Suppliers (USS)
ONboard SFCs	N1	Real-Time Risk Assessment (RTRA) function
	N2	Proximity to Threat (PtT) function
	N3	Constraint Monitor (Safeguard) function
	N4	Battery Health Monitor (BHM) function
	N5	Link Monitor function
	N6	Auto-pilot Monitor (Co-pilot based) function
	N7	Traffic and RTA Monitor (ICAROUS) functions
	N8	Diagnostic Reasoner/Anomaly Detector (DR-AD) function
	N9	Aircraft and flight system state telemetry service (TMS)
	N10	Contingency, Select, and Trigger (CST) function

C. Gap Types

Each hazard was evaluated for gap type. The gaps were separated into four types as shown in Table 4.

*The offboard and onboard SFCs were differentiated by the second letter of each category, enumerated by F# and N#, respectively

Table 4 Gap types

Gap Type	Definition
A	Changes needed to the approach or design. (SFC Modifications Needed)
B	The Technology Readiness Level (TRL) or the Application Readiness Level (ARL) may not be high enough yet for application to WFM. (Insufficient TRL/ARL)
C	The Design Assurance Level (DAL) may not be high enough yet for application to WFM. (Insufficient DAL)
D	There has been no NASA SWS R&D toward addressing this hazard. (No Coverage)

D. SFC Evaluation

1. Columns

The assessment results are given in tables where each hazard corresponds to a row. The evaluation of each hazard is broken into columns. Each column shares a different piece of information for the hazard. From left to right, the table indicates (1) which SFCs are applicable to that hazard, (2) the scoring for how effectively the combined SFCs provide coverage for that hazard for each stage of flight (pre-flight, in-flight, and post-flight), (3) the implied need to address the hazard for WFM safety demonstrator, and (4) the type of gaps the hazard has based on SFC coverage. Due to the different combinations of SFCs that apply to a given hazard, the evaluation of the hazards was divided by action: monitor, assess, and mitigate.

2. Scoring Definition

The scoring of how well an SFC addresses the hazard for a given IASMS functional category (monitor, assess, or mitigate) is based on the criteria given in Table 5. Values/scores were selected based on responses from a set of subject matter experts (SMEs). These scores are given in the column labeled "Coverage [pre-, in-, post-] (1-10)" and rate the applicable SFCs for the given hazard based on their maturity and coverage for each stage of flight operations (pre-, in-, and post-). Each flight stage score is based on the SFC that provides the highest level of coverage. As seen in Table 5, a score of 1 characterizes immature technology (i.e., low TRL) that provides very low hazard coverage, whereas a 10 indicates that a product exists that is sufficiently functional and can be packaged for commercialization with no changes.

The column titled "Implied as needed by WFM (1-10 rating); Solution Effectiveness (1-10)" in Tables 6 through 8 indicates (1) the WFM need for a solution to the hazard and (2) the effectiveness of current solutions (if one exists). For the first quantity, a score of 10 indicates the highest need for WFM and 1 is little to no need. For the second quantity, a score of 10 for the solution indicates that the hazard is thoroughly addressed, whereas a 1 indicates that current solutions are ineffective or non-existent.

Table 5 Estimating SFC coverage of hazard

Coverage	Definition
-	No Coverage
0	No Coverage, SFC planned/exists
1	Low Coverage
10	Full Coverage

IV. Gap Assessment Results

The gap assessment results are presented as tables. The results are divided by hazard response: monitoring the hazard, assessing the hazard, or mitigating the hazard. The information is shared in the order the hazard response occurs during operation: monitor, assess, and mitigate.

A. Monitor Table

The gap analysis results for hazard monitoring are tabulated in Table 6.[†]

Table 6 Gap analysis results for SFC applicability, coverage, and implied need for monitoring hazards

Hazard/Risk to Monitor	Applicable SFCs (#s)	Coverage [pre-, in-, post-] (1-10)	Implied as needed by WFM (1-10), Solution Effectiveness (1-10)	Gap Type
Undesirable Outcome				
Loss of separation (terrain)	F3, F5, N2	[4,4,1]	9,6	B, C
Loss of separation (non-terrain obstacle)	F3, F5, N2	[5,4,1]	9,5	B, C
Loss of separation (traffic)	F4, F11, N7	[7,4,2]	10,5	A, B, C
Loss of separation (3rd party)	F6, N1	[6,5,1]	5,8	A, B, C
Mission failure	ALL	-	10,5	A, B, C
Precursors				
Loss of power (electrical)	F2, N1, N4	[6,6,3]	10,10	B, C
Loss of propulsion	-	-	10,5	D
Loss of C2/TM link	N1, N5, N6, F7	[4,3,2]	9,5	B, C
Loss of navigation	N1, F8	[6,5,2]	8,9	C
Loss of surveillance	F1, N9, N3	[4,4,1]	10,5	A, B, C
Loss of control (e.g., control system failure)	N1	[1,5,1]	8,2	B, C
Flight Path/Plan Deviation	F10, N7, N3	[7,3,1]	9,6	B, C
Structural (e.g., damage)	-	-	8,4	D
Excessive vibration	-	-	5,10	D
Auto-pilot failure (s/w)	N6	[5,4,1]	10,2	A, B, C
RF Interference	F7	[6,3,1]	8,6	B, C
Fire related hazard (smoke, ash, heat)	-	-	10,4	D
Hazardous weather (e.g., fire weather, weather caused by fire, such as pyrocumulonimbus, excessive wind, windshear, convection, lightning, etc.)	-	-	10,3	D
Weather (e.g. wind, turb, convection)	F9	[6,3,1]	9,5	B, C
Airspace non-conformance	F4, F11, N7, N3	[9,9,1]	10,5	C
Operator SA and alerting	F1, N9	[7,5,1]	7,3	A, B, C
Wildlife (birds, etc.)	-	-	7,4	D
Procedural error (omission/commission) (in-flight vs pre-flight) [Human Factor]	F1	[3,2,1]	9,3	A, B, C
Procedural error [technical, onboard. i.e., software]	N8	[2,2,4]	9,3	A, B, C
Operator incapacitated, distracted, fatigued, etc.	-	-	10,2	D
Overarching				
Insufficient information availability	N5	-	9,3	D
Insufficient data integrity (including inadequate information sharing)	N9, F1	-	8,3	D
Malicious interference (physical)	-	-	3,5	D
Malicious interference (cyber)	-	-	?,?	D

[†]Note that the malicious interference from cyber attacks hazard has two question marks for implied need by wildfire management. These question marks indicate that the parties performing this evaluation were unable to provide a score for this entry. They reported that they did not have the expertise to provide an informed score for this entry. This entry requires input from experts in aerospace cyber security to provide further information for evaluating this hazard. This applies to all actions for addressing the hazard, as shown in the assess and mitigate tables in later sections.

Monitor Table Example Walkthrough

The following is a walkthrough of one row in the monitor table to demonstrate the meaning of each entry in the hazard row. This example walks through the "C2/Telemetry (TM) link" row in the monitor table.

Applicable SFCs: The loss of C2/Telemetry (TM) link in the monitor table has four applicable SFCs:

- N1: RTRA function
- N5: Link Monitor function
- N6: Auto-pilot Monitor (Co-Pilot based) function
- F7: RFI/RFE service (pre-flight and in-flight) (x2) – SDSP

The SFC that most directly applies to the loss of C2/TM hazard, and has the exclusive purpose to address it, is the "Link Monitor" function (N5). This function uses COTS autopilot messages to determine, at a high-level, the functionality of the C2 link using the Received Signal Strength Indicator (RSSI) values by comparing the received signal to selected minimum signal requirements. However, four SFCs are listed as applicable to monitoring "Loss of C2/TM link" because each can contribute to monitoring for C2/TM link loss.

Coverage: The monitoring of loss of C2/TM link scores as [4,3,2]. A score of 4 for WFM pre-flight indicates that the as-developed version for urban low altitude coverage is low-to-moderately mature for monitoring C2/TM link loss during WFM pre-flight use-case. The in-flight score, 3, is slightly lower than the pre-flight score because the link monitor function is required to respond to a dynamic environment, in contrast to the purely predictive data during pre-flight. During post-flight, the SFC rates as 2. The current link monitor function may have the capability to improve its functionality based on post flight data analysis, but this has been minimally investigated, and thus has very low maturity.

WFM Need and Solution Effectiveness: Loss of C2/TM link for WFM rates as a 9 (very high need) as loss of C2/TM link can result in mid-air collisions with other vehicles, loss of vehicle, loss of mission, etc. It is vitally important to address on behalf of the WFM community. The solution exists rating is a 5 because a solution for loss of C2 link exists and is moderately effective but has some significant shortcomings for WFM operations.

Gap Type: The loss of C2/TM link includes a gap type of (B): The Technology Readiness Level/Application Readiness Level (TRL/ARL) may not be high enough yet for application to WFM, and (C): the Design Assurance Level (DAL) may not be high enough for application to WFM. The COTS product utilized to monitor link loss for WFM provides the minimum support and thus has a low TRL and insufficient DAL.

B. Assess Table

The gap analysis results for hazard assessment are tabulated in Table 7.

Table 7 Gap analysis results for SFC applicability, coverage, and implied need for assessing hazards

Hazard/Risk to Assess	Applicable SFCs (#s)	Coverage [pre-, in-, post-] (1-10)	Implied as needed by WFM (1-10), Solution Effectiveness (1-10)	Gap Type
Undesirable Outcome				
Loss of separation (terrain)	F3, F5, N2	[4,4,1]	9,6	B, C
Loss of separation (non-terrain obstacle)	F3, F5, N2	[5,4,1]	9,4	B, C
Loss of separation (traffic)	F4, F11, N7	[7,3,2]	10,5	A, B, C
Loss of separation (3rd party)	F6, N1	[6,5,1]	5,7	A, B, C
Mission failure	ALL	-	10,4	A, B, C
Precursors				
Loss of power (electrical)	F2, N1, N4	[4,4,2]	10,6	B, C
Loss of propulsion	-	-	10,5	D
Loss of C2/TM link	N1, N5, N6, F7	[4,3,2]	9,6	A, B, C
Loss of navigation	N1, F8	[5,4,1]	8,9	B, C
Loss of surveillance	N3	[4,4,1]	10,3	A, B, C
Loss of control (e.g., control system failure)	N1	[1,5,1]	8,3	B, C
Flight Path/Plan Deviation	F10, N7	[7,3,1]	9,3	B, C
Structural (e.g., damage)	-	-	8,4	D
Excessive vibration	-	-	5,9	D
Auto-pilot failure (s/w)	N6	[3,2,1]	10,2	A, B, C
RF Interference	F7	[4,2,1]	8,6	A, B, C
Fire related hazard (smoke, ash, heat)	-	-	10,4	D
Hazardous weather (e.g., fire weather, weather caused by fire, such as pyrocumulonimbus, excessive wind, windshear, convection, lightning, etc.)	-	-	10,2	D
Weather (e.g. wind, turb, convection)	F9	[4,2,1]	9,3	A, B, C
Airspace non-conformance	F4, F11, N7, N3	[9,9,1]	10,5	C
Operator SA and alerting	-	-	7,3	D
Wildlife (birds, etc.)	-	-	7,4	D
Procedural error (omission/commission) (in-flight vs pre-flight) [Human Factor]	-	-	9,3	D
Procedural error [technical, onboard. i.e., software]	N8	[2,2,4]	9,3	A, B, C
Operator incapacitated, distracted, fatigued, etc.	-	-	10,2	D
Overarching				
Insufficient information availability	N5	-	9,2	D
Insufficient data integrity (including inadequate information sharing)	-	-	8,3	D
Malicious interference (physical)	-	-	2,4	D
Malicious interference (cyber)	-	-	?,?	D

Assess Table Example Walkthrough

The following is a walkthrough of one row in the assess table to demonstrate the meaning of each entry in the hazard row. This example walks through the "Hazardous Weather" row in the assess table.

Applicable SFCs: Hazardous weather has no applicable SFCs in the assess table.

Coverage: SFCs considered for this study are derived from those for SWS R&D. Other than wind, SWS SFC R&D has yet to address hazardous weather.

WFM Need and Solution Effectiveness: Hazardous weather for WFM rates as a 10 (critical need). WFM operations, by nature, take place in weather conditions caused by wildfires, particularly large wildfires: convective updraft columns from heat and ash that generate pyrocumulonimbus, high winds, and lightning. The solution exists rating is a 2 because the SWS SFC approach indirectly addresses hazardous weather and individuals interviewed for this study did not know

of a COTS solution. The wind service SFC (F9) addresses wind in more common settings such as day-to-day gusting and has potential application to sever winds generated by hazardous weather generated by wildland fires.

Gap Type: Hazardous weather has a gap type of (D): There has been no NASA R&D toward addressing this hazard.

C. Mitigate Table

The gap analysis results for hazard mitigation are tabulated in Table 8.

Note: All SFCs that help to Monitor and Assess vulnerability to hazards also produce data used by mitigation functions in the SFCs identified in the table below.

Table 8 Gap analysis results for SFC applicability, coverage, and implied need for mitigating hazards

Hazard/Risk to Mitigate	Applicable SFCs (#s)	Coverage [pre-, in-, post-] (1-10)	Implied as needed by WFM (1-10), Solution Effectiveness (1-10)	Gap Type
Undesirable Outcome				
Loss of separation (terrain)	N10 (F3, F5, N2)	[3,2,1]	9,1	A, B, C
Loss of separation (non-terrain obstacle)	N10 (F3, F5, N2)	[4,2,1]	9,1	A, B, C
Loss of separation (traffic)	N10, N7, F11 (F4)	[7,2,1]	10,2	A, B, C
Loss of separation (3rd party)	N10, N1 (F6)	[6,3,1]	5,2	A, B, C
Mission failure	ALL	-	10,1	A, B, C
Precursors				
Loss of power (electrical)	N10, N1 (F2, N4)	[4,2,2]	10,4	A, B, C
Loss of propulsion	-	-	10,3	D
Loss of C2/TM link	N10, N1 (N5, N6, F7)	[4,2,2]	8,2	A, B, C
Loss of navigation	N1 (F8)	[5,2,1]	8,9	A, B, C
Loss of surveillance	N10 (N3)	[4,2,1]	10,1	A, B, C
Loss of control (e.g., control system failure)	N1, N10	[1,2,1]	10,2	A, B, C
Flight Path/Plan Deviation	N7 (F10)	[7,2,1]	9,2	A, B, C
Structural (e.g., damage)	-	-	8,7	D
Excessive vibration	-	-	7,8	D
Auto-pilot failure (s/w)	N6	[3,1,1]	10,2	A, B, C
RF Interference	N10, N1 (F7)	[4,2,1]	8,7	A, B, C
Fire related hazard (smoke, ash, heat)	-	-	10,2	D
Hazardous weather (e.g., fire weather, weather caused by fire, such as pyrocumulonimbus, excessive wind, windshear, convection, lightning, etc.)	-	-	10,2	D
Weather (e.g. wind, turb, convection)	N10, N1 (F9)	[4,2,1]	10,2	A, B, C
Airspace non-conformance	N10, N7, N3, F11 (F4)	[9,9,1]	10,5	C
Operator SA and alerting	-	-	7,3	D
Wildlife (birds, etc.)	-	-	7,4	D
Procedural error (omission/commission) (in-flight vs pre-flight) [Human Factor]	-	-	9,3	D
Procedural error [technical, onboard. i.e., software]	-	-	9,3	D
Operator incapacitated, distracted, fatigued, etc.	-	-	10,1	D
Overarching				
Insufficient information availability	-	-	9,1	D
Insufficient data integrity (including inadequate information sharing)	-	-	8,1	D
Malicious interference (physical)	-	-	2,4	D
Malicious interference (cyber)	-	-	?,?	D

Mitigate Table Example Walkthrough The following is a walkthrough of one row in the mitigate table to demonstrate the meaning of each entry in the hazard row. This example walks through the "C2/Telemetry (TM) link" row in the mitigate table.

Applicable SFCs: The loss of C2/Telemetry (TM) link in the mitigate table has two directly applicable SFCs:

- N10: Contingency, Select, and Trigger (CST) function
- N1: Real-Time Risk Assessment (RTRA) function

The loss of C2/Telemetry (TM) link also has three indirectly applicable SFCs:

- N5: Link Monitor function
- N6: Auto-pilot Monitor (Co-Pilot based) function
- F7: RFI/RFE service (pre-flight and in-flight) (x2) – SDSP

Both the CST (N10) and RTRA (N1) functions serve to address mitigating loss of C2/TM link. The CST function commands an autopilot mode change (i.e., mitigation action) based on information from other functions. For example, it relies on the Autopilot Monitor (ApMon) function (N6) to verify that the CST autopilot change command does not attempt to change to an unsafe mode [7]. The RTRA function (N1) uses likelihood of events (LoE) estimates to generate recommended mitigation actions.

Coverage: The mitigation of loss of C2/TM link scores as [4,2,2]. The score of 4 for pre-flight remains unchanged from the monitor table. Mitigating loss of C2/TM link during pre-flight for WFM coverage is low-to-moderately mature. The in-flight score and post-flight scores, 2, are low because the current SFCs have very limited research into mitigating loss of C2/TM link during these flight phases.

WFM Need and Solution Effectiveness: Loss of C2/TM link for WFM rates as a 8 (high-to-very-high need). It is lower than the score of 9 from the monitor table. This is because monitoring loss of C2/TM link is considered a higher need for WFM than mitigating loss of C2/TM link. Mitigating loss of C2/TM link is dependent on monitoring whether that loss occurs. Weak monitoring functionality undermines the value of mitigation actions to address loss of C2/TM link, thus reducing the score for mitigating to a nominal, relatively lower 8 when compared to monitoring. The solution exists rating is a 2 because a solution for loss of C2 link is very limited in the context of SWS for WFM operations.

Gap Type: The loss of C2/TM link includes a gap type of (A): Changes needed to the approach taken by SWS SFC R&D so far, (B): The TRL/ARL may not be high enough yet for application to WFM, and (C): the DAL may not be high enough for application to WFM. There are no COTS products that can be utilized to mitigate link loss for WFM known to the individuals interviewed for this work. Therefore, combined with no development plans in work for WFM to mitigate loss of C2/TM link, this entry requires changes to the SWS R&D approach so far, has a low TRL, and insufficient DAL.

V. Concluding Remarks

A. Recommendations

The results of this assessment indicate that all of NASA's developmental SFCs considered for WFM operations would benefit from further development. No single SFC scores a 10 for satisfying solution effectiveness for WFM needs. However, some are close to an appropriate readiness level despite being developed for an alternate use case (i.e., low altitude, highly autonomous urban flights). Decision makers are advised to use these results to inform decisions regarding which SFCs to further develop for WFM operations. The assessment method may also be useful when evaluating SFCs developed outside the NASA SWS project.

B. Future Work

The authors intend to perform more extensive gap assessments for the SWS project, particularly regarding other types of use-cases that may be the subject of future demonstrations of the IASMS concept. The scope of this document is to share the results of an initial gap assessment and approach. The details of each score and why that score was given are of lower priority. A NASA technical memorandum (TM) is planned that expands on the scoring in this work.

C. Strategies for SFC Development

Possible strategies to adapt existing SFCs for the wildland fire management safety demonstrator include:

1. Strategy 1

Instead of modifying SFCs that require significant changes to respond to a hazard, a strategy is to fold these SFCs into broader SFCs that can increase the response of the initial SFC, thus requiring fewer changes. For example, significant modifications to the aircraft and flight system state telemetry service (SFC N9) could be made to increase the

effectiveness of monitoring the hazard for insufficient data integrity. Alternatively, the aircraft and flight system state telemetry service could be integrated with the link monitor function (SFC N5) to monitor for insufficient data integrity. This alternate approach could increase the effectiveness of the aircraft and flight system state telemetry service and require fewer modifications to achieve.

2. Strategy 2

Additionally, the creation of new SFCs can require significant investment. Instead, the new SFCs can be strategically developed to address multiple hazards in a single SFC. For example, the malicious interference hazards (physical and cyber), wildlife collision hazard, and procedural error hazard can all be addressed with a single SFC. Such an SFC could use incoming data (such as visual recognition and anomalies in data) to identify cyberattacks, identify physical hazards (both malicious and accidental wildlife collisions), and monitor for procedural error based on incoming commands from the ground control station or remote pilot.

3. Strategy 3

The scope of this work was focused on quantifying how effective unmodified SFCs are when applied to a different use case from their original design. Another strategy is to investigate existing COTS solutions that may address the hazards. Purchasing COTS solutions can reduce the cost of addressing hazards. This can allow decision makers to direct budget to developing other SFCs for hazards that do not have COTS solutions.

Acknowledgments

The authors of this work would like to thank the NASA SWS project under Aeronautics Research Mission Directorate's Airspace Operations and Safety Program for funding this research and enabling this work.

References

[1] Walsh, H. S., Spirakis, E., Andrade, S. R., Hulse, D. E., and Davis, M. D., "SMARt-STEReO: Preliminary Concept of Operations," NASA TM-2020-5007665, 2020.

[2] Ellis, K. K., Krois, P., Koelling, J. H., Prinzel, L. J., Davies, M. D., and Mah, R. W., "A Concept of Operations (ConOps) of an In-time Aviation Safety Management System (IASMS) for Advanced Air Mobility (AAM)," *AIAA Scitech 2021 Forum*, American Institute of Aeronautics and Astronautics, 2021. doi:10.2514/6.2021-1978.

[3] Kirkman, D., Mooberry, J., Reeser, R., Yang, M., Gould, K., Koelling, J., Davies, M., Ellis, K., Prinzel, L., Krois, P., Mah, R., and Infeld, S. I., "Informing New Concepts for UAS and Autonomous System Safety Management using Disaster Management and First Responder Scenarios," *IEEE/AIAA 40th Digital Avionics Systems Conference (DASC)*, San Antonio, TX, 2021. doi:10.1109/DASC52595.2021.9594356.

[4] Lehman, S. M., Slagel, J. T., Andrade, S., Walsh, H., Goodloe, A., Brandt, S. L., and Neogi, N., "NASA System-Wide Safety Wildland Firefighting Operations Workshop Report," NASA TM-2022-0014721, 2022.

[5] Young, S. D., Quach, C., Goebel, K., and Nowinski, J., "In-Time Safety Assurance Systems for Emerging Autonomous Flight Operations," *IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, London, UK, 2018.

[6] Young, S. D., Ancel, E., Moore, A. J., Dill, E. T., Quach, C. C., Foster, J. V., Darafsheh, K., Smalling, K. M., Vazquez, S. L., Evans, E. T., Okolo, W. A., Corbetta, M., Ossenfort, J. P., Watkins, J., Kulkarni, C. S., and Spirkovska, L., "Architecture and Information Requirements to Assess and Predict Flight Safety Risks During Highly Autonomous Urban Flight Operations," NASA TM-2020-220440, 2020.

[7] Ancel, E., Young, S. D., Quach, C. C., Haq, R., Darafsheh, K., Smalling, K. M., Vazquez, S., Dill, E. T., Condotta, R. C., Ethridge, B. E., Teska, L., and Johnson, T., "Design and Testing of an Approach to Automated In-Flight Safety Risk Management for sUAS Operations," *Aviation Forum 2022*, American Institute of Aeronautics and Astronautics, Chicago, IL, 2022. doi:10.2514/6.2022-3459.